GVT-070107-001-00 1.27

QX-S5600G Series Ethernet Switches

Command References

Revision History

Revision	Date	Reason for Change
1.0	2018/10	First Revision
1.1	2019/10	・The parity error monitor commands was added to “10 Device management commands” in “1.Fundamentals”. ・The resource-monitor commands was added to “10 Devaice management commands” in “1.Fundamentals”. ・The setting range of the link-delay command was changed of “1.Ethernet interface commands” in “3.Layer 2 – LAN Switching “. ・The auto option was added to combo enable command of “1 Ethernet interface commands” in “3.Layer 2 – LAN Switching”, and the default was changed to auto. ・The force option was added to port link-aggregation group command of “6. Ethernet link aggregation commands” in “3.Layer 2 – LAN Switching” ・The reauthentication server-select command was add to “1.AAA commands” in “8.Security”. ・The NetMeister commands was added to “12.NetMeister commands” in “11.Network Management and Monitoring”. ・Writing error correction
1.2	2020/02/24	Writing error correction
1.3	2020/03	・The packet-filter filter commands was added to “1 ACL commands” in “8.ACL and QoS”. ・Writing error correction
1.4	2020/06	・IMPORTAN has been added to the car command of “2. QoS Policy Commands” in “8.ACL and QoS”.
1.5	2020/07	・The restful https enable command was added to “3 Login management commands” in “1.Fundamentals”. ・The lldp management-address command was added to “15 LLDP commands” in “3.Layer 2 – LAN Switching”. ・The ip address unnumbered command was added to “ 5 IP addressing commands” in “4.Layer 3 – IP Services”. ・The arp route-direct advertise command was added to “ 14 ARP direct route advertisement commands” in “4.Layer 3 – IP Services”. ・The max-ecmp-num command was added to “ 1 Basic IP routing commands” in “5.Layer 3 – IP Routing”. ・The 1etconf ssh server enable command was added to “ 6 NETCONF commands” in “11.Network Management and Monitoring”. ・The OpenFlow commands was added to “12 OpenFlow” in “ 1. OpenFlow commands”. ・The OVSDB commands was added to “ 1 VXLAN commands” in “ 13.VXLAN”. ・The vtep access port command was added to “ 1 VXLAN commands” in “ 13.VXLAN”.

Revision	Date	Reason for Change
		・The vtep enable command was added to “ 1 VXLAN commands” in “ 13.VXLAN”.
1.6	2020/12/21	・Chapter 7 of 09-Security Password-control blacklist all-line command has been added to password management. ・Chapter 7 of 09-Security Password-control change-password first-login enable command has been added to password management. ・Chapter 7 of 09-Security Password-control change-password weak-password enable command has been added to password management. ・Chapter 09-Security Chapter 7 Changed the display example of the display password-control command of password management. ・Chapter 7 of 09-Security Changed the contents of password management display password-control blacklist. ・Chapter 7 of 09-Security Password-control { aging | command | history | length } enable has been changed. ・Chapter 09-Security Chapter 7 Password-control complex of password management has been changed. ・Chapter 09-Security Chapter 7 Password-control command content has been changed. ・Chapter 7 of 09-Security Password-control enable contents of password management have been changed. ・Chapter 09-Security Chapter 7 Password-control history has been changed. ・Chapter 09-Security Chapter 7 Password-control login-attempt has been changed. ・Chapter 09-Security Chapter 7 Password-control super command type-number has been changed. ・Chapter 09-Security Chapter 7 Added notes to password-control super length of password management. ・” 13 VCF fabric commands” in “ 11. Network Management and Monitoring” added. ・Added “1.4. Rate Limit Logging” to Chapter 1 System Maintenance and Debugging in “11-System Management”. ・The display arp suppression vsi command was changed of “ 1 VXLAN commands” in “ 13.VXLAN”. ・The display l2vpn mac-address command was changed of “ 1 VXLAN commands” in “ 13.VXLAN”. ・The display l2vpn service-instance command was changed of “ 1 VXLAN commands” in “ 13.VXLAN”. ・The display l2vpn vsi command was changed of “ 1 VXLAN commands” in “ 13.VXLAN”. ・The display vxlan tunnel command was changed of “ 1 VXLAN commands” in “ 13.VXLAN”. ・The vxlan command was changed of “ 1 VXLAN commands” in “ 13.VXLAN”. ・The display 2etconf2e vsi-interface command was changed of “ 1 VXLAN commands” in “ 13.VXLAN”. ・The ovsdb server ptcp command was changed of “ 1 VXLAN commands” in “ 13.VXLAN”.

Revision	Date	Reason for Change
		・The arp-advertising disable command was changed of “ 1 EVPN commands” in “ 14.EVPN”. ・The display bgp l2vpn evpn command was changed of “ 1 EVPN commands” in “ 14.EVPN”. ・The display evpn auto-discovery command was changed of “ 1 EVPN commands” in “ 14.EVPN”. ・The display evpn instance vxlan command was added to “ 1 EVPN commands” in “ 14.EVPN” ・The display evpn route arp command was changed of “ 1 EVPN commands” in “ 14.EVPN”. ・The display evpn route arp suppression command was changed of “ 1 EVPN commands” in “ 14.EVPN”. ・The display evpn route arp-mobility command was added to “ 1 EVPN commands” in “ 14.EVPN” ・The display evpn route mac command was changed of “ 1 EVPN commands” in “ 14.EVPN”. ・The display evpn route mac-mobility command was added to “ 1 EVPN commands” in “ 14.EVPN” ・The evpn encapsulation command was changed of “ 1 EVPN commands” in “ 14.EVPN”. ・The evpn route arp-mobility suppression command was added to “ 1 EVPN commands” in “ 14.EVPN” ・The evpn route mac-mobility suppression command was added to “ 1 EVPN commands” in “ 14.EVPN” ・The export route-policy command was added to “ 1 EVPN commands” in “ 14.EVPN” ・The import evpn mac-ip command was added to “ 1 EVPN commands” in “ 14.EVPN” ・The import route-policy command was added to “ 1 EVPN commands” in “ 14.EVPN” ・The ip-prefix-route generate disable command was added to “ 1 EVPN commands” in “ 14.EVPN” ・The ip public-instance command was deleted from “ 1 EVPN commands” in “ 14.EVPN” ・The l3-vni command was changed of “ 1 EVPN commands” in “ 14.EVPN”. ・The mac-advertising diable command was changed of “ 1 EVPN commands” in “ 14.EVPN”. ・The vpn-target command was changed of “ 1 EVPN commands” in “ 14.EVPN”.
1.7	2020/12/25	・ The option of the LAG interface has been added to “Chapter 16 L2PT” of “03-Access”. ・ NetMiester proxy has been added to “Chapter 13 NetMiester” in “11-System Management”. ・Writing error correction

Revision	Date	Reason for Change
1.8	2021/04	・Added NSR to the following chapters of “05-Routing”. “Capter 03 RIP”,” Capter 04 OSPF”,” Capter 05 BGP”, ”Capter 08 RIPng”,” Capter 09 OSPFv3” ・Writing error correction
1.9	2021/06	・Added notes to the restful https enable command in “3 Login management commands” in “ 1. Fundamentals” ・Added notes to the 4etconf ssh server enable command in “6 NETCONF commands commands” in “ 11. Network Management and Monitoring” ・Added notes to the vcf-fabric topology enable command in “13 VCF fabric commands” in “ 11. Network Management and Monitoring” ・Added notes to the vcf-fabric underlay autoconfigure command in “13 VCF fabric commands” in “ 11. Network Management and Monitoring” ・Added notes to the ovsdb server enable command in “1 VXLAN commands” in “ 13. VXLAN” ・Added notes to the ovsdb server ptcp command in “1 VXLAN commands” in “ 13. VXLAN” ・Added notes to the vtep access port command in “1 VXLAN commands” in “ 13. VXLAN” ・Added notes to the vtep enable command in “1 VXLAN commands” in “ 13. VXLAN”
1.10	2021/09	・The ssh2 algorithm commands was added to “9 SSH commands” in “9.Security”.
1.11	2021/09	・”control-plane protocol” and “control-plane protocol-group” option added to if-match command “ 2 QoS policy commands “ in “8.QoS/ACL”. ・The control-plane commands was added to “ 2 QoS policy commands “ in “8.QoS/ACL”.
1.12	2022/02	・Add the following commands to “6. Data buffer commands” in “8.ACL and QoS”. Buffer apply buffer shared display buffer
1.13	2022/08	・”lt “, “gt” and “range” option added to rule(Ipv4 advanced ACL view) command “ 1 ACL commands “ in “8.QoS/ACL”. ・Writing error correction
1.14	2022/10	・Added “17 M-LAG” to “03-Access”. ・Added “12 PIM Snooping” and “13 IGMP Proxy” to “06-Multicast”. ・Added “vrrp state-transition-delay” and “vrrp ipv6 state-transition-delay” to “Chapter 7 VRRP” of “10-High Availability”. ・Added “netmeister management ip”to 13 NetMeister in “11-Network Management and Monitorring”.

Revision	Date	Reason for Change
		・Correction of errors
1.15	2023/01	・Deleted “10.1.25 display transceiver diagnosis” from “10. Device management commands” in “1.Fundamentals”(correction of error). ・Modified “10.1.53. temperature-limit” of “10. Device management commands” in “1.Fundamentals”(correction of error). ・Added the following parameters to “03-DHCP commands” in “04-Layer 3 - IP Services” (correction of error). class public vpn-instance ・Added “security-enhanced level” command to “10-SSL” in “9-Security”. ・Deleted the delay parameter from “09-Track commands” in “10-High Availability”(correction of error). ・Added “fast-detection enable” and “fast-timer” to “Chapter 4 RRPP” of “10-High Availability”. ・Added “display evpn m-lag synchronized-mac”, “evpn m-lag group”, “evpn m-lag local”, “evpn global-mac”, “ip forwarding-conversational-learning”, “l2vpn m-lag peer-link ac-match-rule vxlan-mapping” and “l2vpn statistics vsi l3-vni” to “Chapter 1 EVPN” of “14-EVPN”. ・Added the System-view to “mac-address static source-check enable” in “Chapter 4 MAC address table” of ”03- Layer 2 - LAN Switching”. ・Added option to “xconnect vsi” in “Chapter 1 VXLAN” of ”13- VXLAN”.
1.16	2023/05	・An explanation has been added to the display of "display stp" in "Chapter 8 STP" of "03-Access." ・A gratuitous-arp mac-change retransmit command was added to “Chapter 2 Gratuitous ARP commands” of “04-Layer 3 - IP Services”. ・Added a processable broadcast condition to "rip version" in " Chapter 3 RIP commands" of "05- Layer 3 - IP Routing."
1.17	2023/07	・Fixed the default value of the "10.1.53 temperature-limit" command from "Chapter 10 Equipment Management" in "01 - Introduction." ・Added dropped packets to "bpdu-drop any" description in "Chapter 8 STP" of "03-Access." ・Added description of "dhcp relay server-address" in “Chapter 6 DHCP commands” of “04-Layer3-IP Services”.
1.18	2023/09	・Added support for the parent mode for "Chapter 12 NetMiester" in "10-System Management".
1.19	2024/05	・Added " Chapter 12 Automatic configuration commands " to "01- Fundamentals". ・Added "mac-address" to " Chapter 10 VLAN commands" of "03-Layer 2 - LAN Switching". ・Added "ospf peer sub-address enable" to " Chapter 4 OSPF commands" of "05-Layer 3 - IP Routing". ・Added " peer source-address" to " Chapter 5 BGP commands" of "05-Layer 3 - IP Routing".

Revision	Date	Reason for Change
		・Added “m-lag auto-recovery reload-delay”,” m-lag keepalive interval”,”m-lag mad exclude logical-interfaces”,”m-lag mad persistent”,”m-lag role priority”,”m-lag system-mac” , “m-lag system-priority” and "port m-lag virtual-ip" to Chapter 17 M-LAG commands" of “03-Layer2 -LAN Switching”.
1.20	2024/10	・Added notes to “Chapter 12 PIM snooping commnads” of ”06- IP Multicast”. ・Added notes to “Chapter 13 IGMP proxy commnads” of ”06- IP Multicast”.
1.21	2024/11	・The following commands have been added to “10. Device management commands” in “01-Fundamentals”: “10.1.27. dying-gasp host” and “10.1.28. dying-gasp source”.
1.22	2025/01	・Modified the parameters of the "1.2.11. mtu" command from "1. VXLAN commands" in "13 - VXLAN."
1.23	2025/02	Deleted the note of “port m-lag virtual-ip” command
1.24	2025/07	・Modified the Logo image on the Cover. ・The default for “set authentication password” has been changed. ・Added an explanation to "display mad" in " Chapter 1 IRF commands" of "02- IRF." ・Added a memo to "display igmp-snooping" in " Chapter 1 IGMP snooping commands" of "06- IP Multicast." ・Added an explanation to " igmp-snooping" and “igmp-snooping enable” in " Chapter 1 IGMP snooping commands" of "06- IP Multicast." ・The arp scan commands was added to “13 ARP attack protection commands “ in “9.Security”
1.25	2026/01	・Added an example of storm-constrain settings when specifying pps in "1.2.4 storm-constrain" in "03-Access." ・Corrected the lower limit of storm-constrain from 0 to 1 when specifying pps in "1.2.4 storm-constrain" in "03-Access." ・Added a note about interface view settings in "3.1.4 mac-authentication access-user log enable" in "09-Security." ・Added a note about interface view settings in "5.1.14 port-security timer autolearn aging" in "09-Security."
1.26	2026/09	・ Added "display transceiver alarm" to "10. Device management commands" in "01-Fundamentals". ・ Added "display transceiver diagnosis" to "10. Device management commands" in "01-Fundamentals". ・ Added a example and note of "display transceiver interface" in "10. Device management commands" of "01-Fundamentals". ・ Added "display transceiver manuinfo" to "10. Device management commands" in "01-Fundamentals". ・ Corrected an error in the description in "Table 10-6 Command output" of "10. Device management commands" in "01-Fundamentals". ・ Corrected an error in the description in "1.1.16. mad bfd enable" of "1. IRF commands" in "02-IRF".Corrected an error in the description in "1.1.17. mad enable" of "1. IRF commands" in "02-IRF". ・ Corrected an error in the description in "10.1.10. vlan" of "10. VLAN commands" in "03-Layer2".

Revision	Date	Reason for Change
		・ Added a description in "14.1.2. vlan mapping" of "14. VLAN mapping commands" in "03-Layer2". ・ Added "17.1.19. m-lag mad restore" to "17. M-LAG commands" in "03-Layer2". ・ Added "17.1.22. m-lag standalone enable" to "17. M-LAG commands" in "03-Layer2". ・ Deleted the note from "m-lag auto-recovery reload-delay" in "17. M-LAG commands" of "03-Layer2 - LAN Switching". ・ Deleted the note from "m-lag keepalive interval" in "17. M-LAG commands" of "03-Layer2 - LAN Switching". ・ Deleted the note from "m-lag mad exclude logical-interfaces" in "17. M-LAG commands" of "03-Layer2 - LAN Switching". ・ Deleted the note from "m-lag mad persistent" in "17. M-LAG commands" of "03-Layer2 - LAN Switching". ・ Deleted the note from "m-lag role priority" in "17. M-LAG commands" of "03-Layer2 - LAN Switching". ・ Corrected an error in the description in "13.1.1. http-redirect https-port" of "13. HTTPS redirect commands" in "04-Layer3-IP services". ・ Added "tunnel vpn-instance" to "12. Tunneling commands" in "04-Layer3 IP services". ・ Corrected an error in the description in "6.1.1. apply next-hop" of "6. Policy-based routing commands" in "05-Layer3 IP Routing". ・ Corrected an error in the description in "3.1.1. display qos map-table" of "3. Priority mapping commands" in "08-ACL and QoS". ・ Corrected an error in the description in "3.1.3. qos map-table" of "3. Priority mapping commands" in "08-ACL and QoS". ・ Corrected an error in the description in "1.2.4. display local-user" of "1. AAA commands" in "09-Security". ・ Corrected an error in the description in "1.2.7. local-user" of "1. AAA commands" in "09-Security".Corrected an error in the description in "1.2.10. service-type" of "1. AAA commands" in "09-Security". ・ Corrected an error in the description in "3.1.10. mac-authentication timer" of "3. MAC authentication commands" in "09-Security". ・ Added a description in "4.1.1. protected-vlan" of "4. RRPP commands" in "10-High Availability". ・ Corrected an error in the description in "8.1.3. bfd detect-multiplier" of "8. BFD commands" in "10-High Availability". ・ Corrected an error in the description in "8.1.11. bfd multi-hop detect-multiplier" of "8. BFD commands" in "10-High Availability".
1.27	2026/10	・ Added a description to the "1.1.12 repeat" command in "01 - Introduction ". ・ Deleted the note from “m-lag mad restore” in "17. M-LAG commands" of "03-Layer2 - LAN Switching". ・ Deleted the note from “m-lag standalone enable” in "17. M-LAG commands" of "03-Layer2 - LAN Switching". ・ Added a description of the default setting to "10.1.6 ssl version disable" in "08-Security". ・ Added the following commands to " 12 NetMeister" in "11-Network

Revision	Date	Reason for Change
		Management and Monitorring ". netmeister event log enable netmeister event syslog enable netmeister ngn enable

Copyright © NEC Corporation 2018-2026

All Rights Reserved

No part of this manual may be reproduced or transmitted in any form or by any means without prior written consent of NEC Corporation.

Trademarks

All other trademarks that may be mentioned in this manual are the property of their respective owners.

Notice

- Only the command indicated on *QX-S5600G Series Ethernet Switches Command References* can use this device. When using the command which isn't indicated on the *QX-S5600G Series Switch Command References*, operation of device isn't guaranteed.
- The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute the warranty of any kind, express or implied.

Preface

Version

This command reference corresponds after software version 7.1.X.

Documentation Set

The Documentation Set of QX-S5600G Series Ethernet Switches includes the following documentations.

Documentation Set	Description
QX-S5600G Series Ethernet Switches Installation Guide	This documentation describes installation.
QX-S5600G Series Ethernet Switches Configuration Guides	This documentation describes configuration.
QX-S5600G Series Ethernet Switches Command References	This documentation describes commands.

Sections

This command reference includes the following sections.

- **Fundamentals**

  The Fundamentals Command Reference describes commands for configuring command line interface (CLI), login management, FTP and TFTP, file system management, configuration file management, device management, etc.

- **IRF**

  The IRF Command Reference describes IRF configuration commands for creating an IRF fabric. It covers the commands for binding physical ports to an IRF port, configuring the member switch ID and priority, and detecting and maintaining the IRF link.

- **Layer 2 - LAN Switching**

  The Layer 2 - LAN Switching Command Reference describes the commands for configuring Layer 2 technologies and features in a LAN switched network, etc.

- **Layer 3 - IP Services**

  The Layer 3—IP Services Command Reference describes the commands for configuring IP addressing, IP performance optimization, ARP, IP forwarding basics and IPv6 basics, etc.

- **Layer 3 - IP Routing**

The Layer 3 – IP Routing Command Reference describes the routing configuration commands, etc.

- **IP Multicast**

  The IP Multicast Command Reference describes the commands for IGMP snooping, IGMP, Multicast routing and forwarding (IPv4, IPv6), PIM (IPv4, IPv6), MLD snooping, MLD, etc.

- **MCE**

  The MCE Command Reference describes the MCE configuration commands.

- **ACL and QoS**

  The ACL and QoS Command Reference describe ACL and QoS configuration commands. It covers the commands for creating ACLs, using ACLs for packet filtering, configuring QoS policies, and configuring common QoS techniques, such as traffic policing, congestion management, and congestion avoidance, etc.

- **Security**

  The Security Command Reference describes security configuration commands. It covers the commands for configuring identity authentication feature (AAA), secure management features (Public key management and SSH), and attack protection features (IP source guard and ARP attack protection), etc.

- **High Availability**

  The High Availability Command Reference describes high availability commands. It covers the commands for Ethernet OAM, Connectivity Fault Detection (CFD), Device Link Detection Protocol (DLDP), IPv4 and IPv6 VRRP, BFD, etc.

- **Network Management and Monitoring**

  The Network Management and Monitoring Command Reference describe network management and monitoring configuration commands. It covers the commands for viewing system information, synchronizing time for all devices with clocks in your network, and checking and debugging the current network connectivity with the ping, tracert, and debug commands.

- **OpenFlow**

  The OpenFlow Command Reference describes the OpenFlow configuration commands.

- **VXLAN**

  The VXLAN Command Reference describes the VXLAN configuration commands.

- **EVPN**

  The EVPN Command Reference describes the EVPN configuration commands.

Conventions

This section describes the conventions used in this documentation set.

I. Command conventions

Convention	Description
Boldface	**Bold** text represents commands and keywords that you enter literally as shown.
Italic	*Italic* text represents arguments that you replace with actual values.
[ ]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x | y | ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[x | y | ...]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x | y | ... } *	Asterisk marked braces enclose a set of required syntax choices separated by vertical bars, from which you select at least one.
[x | y | ...] *	Asterisk marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.

II. GUI conventions

Convention	Description
< >	Button names are inside angle brackets. For example, click <OK>.
[ ]	Window names, menu items, data table and field names are inside square brackets. For example, pop up the [New User] window.
/	Multi-level menus are separated by forward slashes. For example, [File/Create/Folder].

III. Keyboard Operations

Convention	Description
<KEY>	Push the KEY of keyboard. For example, <Enter> is push the Enter key.
<KEY1 + KEY2>	Push some KEYs of keyboard. For example, <Ctrl+Alt+A> is push the Ctrl key, the Alt key and the A key at the same time.
<KEY1, KEY2>	Push in turn some KEYs of keyboard. For example, <Alt,A> is push the Alt key then push the A key.

IV. Mouse Operations

Convention	Description
Click	Push the button of the mouse one time quickly. Usually, push the left button.
Double Click	Push the left button of the mouse two times quickly.
Drag	Move the mouse while holding down the left button of the mouse.

V. Symbols

Convention	Description
⚠ **WARNING**	An alert that calls attention to important information that if not understood or followed can result in personal injury.
⚠ **CAUTION**	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
⚠ **IMPORTANT**	An alert that calls attention to essential information.
🕮 **NOTE**	An alert that contains additional or supplementary information.
🕮 **TIP**	An alert that provides helpful information.

VI. Configuration Example

The configuration example of the command reference is an example. Interface Number or the information of the display command, etc. may differ from your device.

VII. Security consideration

To enhance security, configured plain password is converted to hash or cipher password.

This command reference includes the following sections.

01 - Fundamentals

02 - IRF

03 - Layer 2 - LAN Switching

04 - Layer 3 - IP Services

05 - Layer 3 - IP Routing

06 - IP Multicast

07 - MCE

08 - ACL and QoS

09 - Security

10 - High Availability

11 - Network Management and Monitoring

12 - OpenFlow

13 - VXLAN

14 - EVPN

QX-S5600G Series Ethernet Switches

Command References

1.Fundamentals

This manual is including the following chapters.

01-Basic CLI commands

02-RBAC commands

03-Login management commands

04-FTP commands

05-TFTP commands

06-File system management commands

07-Configuration file management commands

08-Software upgrade commands

09-ISSU commands

10-Device management commands

11-Python commands

Contents

A page of this section is **1-x-x**

1. Basic CLI commands 1-1
1.1. Basic CLI commands 1-1
1.1.1. alias 1-1
1.1.2. display | { begin | exclude | include } 1-3
1.1.3. display | by-linenum 1-3
1.1.4. display > 1-4
1.1.5. display >> 1-5
1.1.6. display alias 1-6
1.1.7. display history-command 1-7
1.1.8. display history-command all 1-8
1.1.9. display hotkey 1-9
1.1.10. hotkey 1-10
1.1.11. quit 1-12
1.1.12. repeat 1-13
1.1.13. return 1-14
1.1.14. screen-length disable 1-14
1.1.15. system-view 1-15

1. Basic CLI commands

1.1. Basic CLI commands

1.1.1. alias

Use **alias** to configure a command alias.

Use **undo alias** to delete a command alias.

Syntax

alias *alias command*

undo alias *alias*

Default

The device has a set of system-defined command aliases, as listed in Table 1-1 .

Table 1-1 System-defined command aliases

Command alias	Command or command keyword
access-list	**acl**
end	**return**
erase	**delete**
exit	**quit**
hostname	**sysname**
logging	**info-center**
no	**undo**
show	**display**
write	**save**

Views

System view

Predefined user roles

network-admin

Parameters

alias: Specifies an alias, a case-sensitive string of 1 to 20 characters. An alias cannot be **alias** or contain spaces.

command: Specifies a command string. Make sure the command string meets the syntax requirements.

Usage guidelines

System-defined command aliases cannot be deleted.

You can configure one or more aliases for a command or the starting keywords of commands. Then, you can use the aliases to execute the command or commands. If the command or commands have **undo** forms, you can also use the aliases to execute the **undo** command or commands.

For example, if you configure the alias **shiprt** for **display ip routing-table**, you can enter **shiprt** to execute the **display ip routing-table** command. If you configure the alias **ship** for **display ip**, you can use **ship** to execute all commands that start with **display ip**:

- Enter **ship routing-table** to execute the **display ip routing-table** command.
- Enter **ship interface** to execute the **display ip interface** command.

The command string can include up to nine parameters. Each parameter starts with the dollar sign ($) and a sequence number in the range of 1 to 9. For example, you can configure the alias **shinc** for the **display ip $1 | include $2** command. Then, to execute the **display ip routing-table | include Static** command, you only need to enter **shinc routing-table Static**. To execute the **display ip interface | include GigabitEthernet1/0/1** command, you only need to enter **shinc interface GigabitEthernet1/0/1**.

Examples

Configure **shiprt** as the alias for the **display ip routing-table** command and verify the configuration.

```
<Switch> system-view
[Switch] alias shiprt display ip routing-table
[Switch] shiprt
Destinations : 13        Routes : 13
Destination/Mask   Proto   Pre Cost        NextHop         Interface
0.0.0.0/32         Direct  0   0           127.0.0.1       InLoop0
3.3.3.3/32         Static  60  0           192.168.1.62    Vlan1
127.0.0.0/8        Direct  0   0           127.0.0.1       InLoop0
127.0.0.0/32       Direct  0   0           127.0.0.1       InLoop0
127.0.0.1/32       Direct  0   0           127.0.0.1       InLoop0
127.255.255.255/32 Direct  0   0           127.0.0.1       InLoop0
169.254.0.0/24     Direct  0   0           169.254.0.188   Vlan1
169.254.0.0/32     Direct  0   0           169.254.0.188   Vlan1
169.254.0.188/32   Direct  0   0           127.0.0.1       InLoop0
169.254.0.255/32   Direct  0   0           169.254.0.188   Vlan1
224.0.0.0/4        Direct  0   0           0.0.0.0         NULL0
224.0.0.0/24       Direct  0   0           0.0.0.0         NULL0
255.255.255.255/32 Direct  0   0           127.0.0.1       InLoop0
```

Configure **shinc** as the alias for **display ip $1 | include $2**.

```
[Switch] alias shinc display ip $1 | include $2
```

Use alias **shinc** to display all static routes.

```
[Switch] shinc routing-table Static
3.3.3.3/32         Static  60  0           192.168.1.62    Vlan1
```

Related commands

display alias

1.1.2. display | { begin | exclude | include }

Use **display |** { **begin** | **exclude** | **include** } to filter the output from a **display** command with a regular expression.

Syntax

display *command* **|** { **begin** | **exclude** | **include** } *regular-expression*

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

command: Specifies the keywords and arguments of a **display** command. To display available keywords and arguments, enter **display ?**.

begin: Displays the first line matching the specified regular expression and all subsequent lines.

exclude: Displays all lines not matching the specified regular expression.

include: Displays all lines matching the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Usage guidelines

Use the **|** { **begin** | **exclude** | **include** } *regular-expression* option with a **display** command to filter the command output. For more information about regular expressions, see *Fundamentals Configuration Guide*.

Examples

Display the lines that contain **vlan** in the running configuration.

```
<Switch> display current-configuration | include vlan
vlan 1
vlan 999
 port access vlan 999
```

1.1.3. display | by-linenum

Use **display | by-linenum** to number each output line for a **display** command.

Syntax

display *command* **| by-linenum**

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

command: Specifies the keywords and arguments of a **display** command. To display available keywords and arguments, enter **display ?**.

Usage guidelines

By numbering each output line from a **display** command, you can easily identify the lines of interest.

Each line number is displayed as a 5-character string and might be followed by a colon (:) or hyphen (-). If you specify both **| by-linenum** and **| begin** *regular-expression* for a **display** command, a hyphen is displayed for all lines that do not match the regular expression.

Examples

Display VLAN 999 settings, with each output line identified by a number.

```
<Switch> display vlan 999 | by-linenum
    1:  VLAN ID: 999
    2:  VLAN type: Static
    3:  Route interface: Configured
    4:  IPv4 address: 192.168.2.1
    5:  IPv4 subnet mask: 255.255.255.0
    6:  Description: For LAN Access
    7:  Name: VLAN 0999
    8:  Tagged ports:   None
    9:  Untagged ports:
   10:     GigabitEthernet1/0/1
```

Display the first line that begins with **user-group** in the running configuration and all of the following lines.

```
<Switch> display current-configuration | by-linenum begin user-group
  114:  user-group system
  115-  #
  116-  return
```

1.1.4. display >

Use **display >** to save the output from a **display** command to a separate file.

Syntax

display *command* **>** *filename*

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

command: Specifies the keywords and arguments of a **display** command. To display available keywords and arguments, enter **display ?**.

filename: Specifies the name of the file that is used to save the output, a string of 1 to 63 characters.

Usage guidelines

The **display** commands show the configuration, statistics, and states of the device. You can use the **display >** command to save the output to a file.

If the specified file does not exist, the system creates the file and saves the output to the file. If the file already exists, the system overwrites the file.

Examples

Save VLAN 1 settings to a separate file named **vlan.txt**.

```
<Switch> display vlan 1 > vlan.txt
```

Check the content of the **vlan.txt** file.

```
<Switch> more vlan.txt
VLAN ID: 1
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0001
 Name: VLAN 0001
 Tagged ports:   None
 Untagged ports:
    GigabitEthernet1/0/2
```

1.1.5. display >>

Use **display >>** to append the output from a **display** command to the end of a file.

Syntax

display *command* **>>** *filename*

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

command: Specifies the keywords and arguments of a **display** command. To display available keywords and arguments, enter **display ?**.

filename: Specifies the name of the file that is used to save the output, a string of 1 to 63 characters.

Usage guidelines

The **display** commands show the configuration, statistics, and states of the device. You can use **display >>** to save the output to a file.

If the specified file does not exist, the system creates the file and saves the output to the file. If the file already exists, the system appends the output to the end of the file.

Examples

Append the VLAN 999 settings to the end of the **vlan.txt** file.

```
<Switch> display vlan 999 >> vlan.txt
<Switch>
```

Check the content of the **vlan.txt** file.

```
<Switch> more vlan.txt
VLAN ID: 1
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0001
 Name: VLAN 0001
 Tagged ports:   None
 Untagged ports:
    GigabitEthernet1/0/2

 VLAN ID: 999
 VLAN type: Static
 Route interface: Configured
 IPv4 address: 192.168.2.1
 IPv4 subnet mask: 255.255.255.0
 Description: For LAN Access
 Name: VLAN 0999
 Tagged ports:   None
 Untagged ports:
    GigabitEthernet1/0/2
```

1.1.6. display alias

Use **display alias** to display command aliases.

Syntax

display alias [*alias*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

alias: Specifies a command alias. If you do not specify this argument, the command displays all command aliases.

Examples

Display all command aliases.

```
<Switch> display alias
Index     Alias               Command key
1         access-list         acl
2         end                 return
3         erase               delete
4         exit                quit
5         hostname            sysname
6         logging             info-center
```

```
7          no                    undo
8          shinc                 display $1 | include $2
9          show                  display
10         sirt                  display ip routing-table
11         write                 save
```

Display the command alias **shinc**.

```
<Switch> display alias shinc
Alias                Command key
shinc                display ip $1 | include $2
```

Related commands

alias

1.1.7. display history-command

Use **display history-command** to display all commands that are saved in the command history buffer for the current CLI session.

Syntax

display history-command

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

The system automatically saves commands you have successfully executed to the command history buffer for the current CLI session. You can view them and execute them again.

By default, the system can save up to 10 commands in the buffer. You can use the **history-command max-size** command to change the buffer size. To buffer a new command when the buffer is full, the system deletes the oldest command entry in the buffer.

All commands in the command history buffer for the current CLI session will be cleared when you log out.

Examples

Display all commands saved in the command history buffer for the current CLI session.

```
<Switch> display history-command
  system-view
  vlan 2
  quit
```

Related commands

history-command max-size

1.1.8. display history-command all

Use **display history-command all** to display all commands that are saved in the command history buffer for all CLI sessions.

Syntax

display history-command all

Views

Any view

Predefined user roles

network-admin

Usage guidelines

The system automatically saves commands successfully executed by users to the command history buffer for all CLI sessions. Users can view them but cannot recall them from the buffer.

Up to 1024 commands can be saved in the command history buffer. To buffer a new command when the buffer is full, the system deletes the oldest command entry in the buffer.

A user logout does not cause the system to delete commands from the history buffer for all CLI sessions.

Examples

Display all commands saved in the command history buffer for all CLI sessions.

```
<Switch> display history-command all
  Date       Time     Terminal   Ip              User
  03/16/2017 20:03:33 vty0       192.168.1.26    **
  Cmd:dis his all

  03/16/2017 20:03:29 vty0       192.168.1.26    **
  Cmd:sys
```

Table 1-2 Command output

Field	Description
Date	Date when the command was executed.
Time	Time when the command was executed.
Terminal	User line used by the user.
Ip	IP address of the terminal used by the user.
User	Username used by the user if the user login authentication mode is **scheme**. If the login authentication mode is **none** or **password**, this field displays ******.
Cmd	Command string entered by the user.

Related commands

display history-command

1.1.9. display hotkey

Use **display hotkey** to display hotkey information.

Syntax

display hotkey

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display hotkey information.

```
<Switch> display hotkey
----------------- Hotkeys -----------------
           -Defined function hotkeys-
CTRL_A  Move the cursor to the beginning of the line.
CTRL_B  Move the cursor one character to the left.
CTRL_C  Stop the current command.
CTRL_D  Erase the character at the cursor.
CTRL_E  Move the cursor to the end of the line.
CTRL_F  Move the cursor one character to the right.
CTRL_H  Erase the character to the left of the cursor.
CTRL_K  Abort the connection request.
CTRL_N  Display the next command in the history buffer.
CTRL_P  Display the previous command in the history buffer.
CTRL_R  Redisplay the current line.
CTRL_V  Paste text from the clipboard.
CTRL_W  Delete the word to the left of the cursor.
CTRL_X  Delete all characters from the beginning of the line to the cursor.
CTRL_Y  Delete all characters from the cursor to the end of the line.
CTRL_Z  Return to the User View.
CTRL_]  Kill incoming connection or redirect connection.
ESC_B   Move the cursor back one word.
ESC_D   Delete all characters from the cursor to the end of the word.
ESC_F   Move the cursor forward one word.
ESC_N   Move the cursor down a line.
ESC_P   Move the cursor up a line.
ESC_<   Move the cursor to the beginning of the clipboard.
ESC_>   Move the cursor to the end of the clipboard.

           -Defined command hotkeys-
CTRL_G display current-configuration
CTRL_L display ip routing-table
CTRL_O undo debugging all
```

```
            -Undefined hotkeys-
CTRL_T NULL
CTRL_U NULL
```

Related commands

hotkey

1.1.10. hotkey

Use **hotkey** to configure a hotkey.

Use **undo hotkey** to restore the default.

Syntax

hotkey *hotkey* { *command* | **function** *function* | **none** }

undo hotkey *hotkey*

Default

Table 1-3 shows the default definitions for hotkeys.

Table 1-3 Default definitions for hotkeys

Hotkey	Function or command
Ctrl+A	**move_the_cursor_to_the_beginning_of_the_line**: Moves the cursor to the beginning of a line.
Ctrl+B	**move_the_cursor_one_character_to_the_left**: Moves the cursor one character to the left.
Ctrl+C	**stop_the_current_command**: Stops the current command.
Ctrl+D	**erase_the_character_at_the_cursor**: Deletes the character at the cursor.
Ctrl+E	**move_the_cursor_to_the_end_of_the_line**: Moves the cursor to the end of a line.
Ctrl+F	**move_the_cursor_one_character_to_the_right**: Moves the cursor one character to the right.
Ctrl+G	**display current-configuration**: Displays the running configuration.
Ctrl+H	**erase_the_character_to_the_left_of_the_cursor**: Deletes the character to the left of the cursor.
Ctrl+K	**abort_the_connection_request**: Aborts the connection request.
Ctrl+L	**display ip routing-table**: Displays the IPv4 routing table information.
Ctrl+N	**display_the_next_command_in_the_history_buffer**: Displays the next command in the history buffer.
Ctrl+O	**undo debugging all**: Displays all debugging functions.
Ctrl+P	**display_the_previous_command_in_the_history_buffer**: Displays the previous command in the history buffer.
Ctrl+R	**redisplay_the_current_line**: Redisplays the current line.
Ctrl+T	N/A

Hotkey	Function or command
Ctrl+U	N/A
Ctrl+V	**paste_text_from_the_clipboard**: Pastes text from the clipboard. This hotkey is not supported in the current software version.
Ctrl+W	**delete_the_word_to_the_left_of_the_cursor**: Deletes the word to the left of the cursor.
Ctrl+X	**delete_all_characters_from_the_beginning_of_the_line_to_the_cursor**: Deletes all characters to the left of the cursor.
Ctrl+Y	**delete_all_characters_from_the_cursor_to_the_end_of_the_line** : Deletes all characters from the cursor to the end of the line.
Ctrl+Z	**return_to_the_User_View**: Returns to user view.
Ctrl+]	**kill_incoming_connection_or_redirect_connection**: Terminates the current connection.
Esc+B	**move_the_cursor_back_one_word**: Moves the cursor back one word.
Esc+D	**delete_all_characters_from_the_cursor_to_the_end_of_the_word**: Deletes all characters from the cursor to the end of the word.
Esc+F	**move_the_cursor_forward_one_word**: Moves the cursor forward one word.
Esc+N	**move_the_cursor_down_a_line**: Moves the cursor down one line. You can use this hotkey before pressing **Enter**. This hotkey is not supported in the current software version.
Esc+P	**move_the_cursor_up_a_line**: Moves the cursor up one line. You can use this hotkey before pressing **Enter**. This hotkey is not supported in the current software version.
Esc+<	**move_the_cursor_to_the_beginning_of_the_clipboard**: Moves the cursor to the beginning of the clipboard. This hotkey is not supported in the current software version.
Esc+>	**move_the_cursor_to_the_end_of_the_clipboard**: Moves the cursor to the end of the clipboard. This hotkey is not supported in the current software version.

Views

System view

Predefined user roles

network-admin

Parameters

hotkey: Specifies a hotkey. To display the supported hotkeys, enter **hotkey ?** or see Table 1-3 .

command: Specifies the command to be assigned to the hotkey.

function *function*: Specifies the function to be assigned to the hotkey. To display the supported functions, enter **hotkey** *hotkey* **function ?** or see Table 1-3 .

none: Removes the command or function assignment for the hotkey. After you remove the assignment for a hotkey, pressing the hotkey does not execute any command or function.

Usage guidelines

The device supports a set of hotkeys. Pressing a hotkey executes the command or function assigned to the hotkey.

A hotkey can correspond to only one command or function. If you assign multiple commands or functions to the same hotkey, the most recently assigned command or function takes effect.

A command or function can be assigned to multiple hotkeys. You can use any of those hotkeys to execute the command or function.

If a hotkey is also defined by the terminal software you are using to interact with the device, the terminal software definition takes effect.

Examples

Assign the **display tcp statistics** command to hotkey **Ctrl+T**.

```
<Switch> system-view
[Switch] hotkey ctrl_t display tcp statistics
```

Assign move_the_cursor_to_the_beginning_of_the_line function to hotkey **Ctrl+U**.

```
<Switch> system-view
[Switch] hotkey ctrl_u function move_the_cursor_to_the_beginning_of_the_line
```

Disable the configurable command or function assigned to hotkey **Ctrl+A**.

```
<Switch> system-view
[Switch] hotkey ctrl_a none
```

Related commands

display hotkey

1.1.11. quit

Use **quit** to return to the upper-level view.

Syntax

quit

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

Executing this command in user view disconnects you from the device.

Examples

Return from GigabitEthernet 1/0/1 interface view to system view and then to user view.

```
[Switch-GigabitEthernet1/0/1] quit
[Switch] quit
<Switch>
```

1.1.12. repeat

Use **repeat** to repeat commands in the command history buffer for the current CLI session.

Syntax

repeat [*number*] [**count** *times*] [**delay** *seconds*]

Views

Any view

Predefined user roles

network-admin

Parameters

number: Specifies the number of the most recently executed commands in the command history buffer for the current CLI session that you want to execute. The value range is 1 to 256. The default is 1.

count *times*: Specifies the number of times that you want to execute the commands. The value range is 0 to 4294967295. The default is 0. If you do not specify this option, the system keeps executing the commands until you press the escape key to terminate the execution.

delay *seconds*: Specifies the time (in seconds) for the system to wait before executing the commands again. The value range is 0 to 4294967295. The default is 1.

Usage guidelines

To repeat a command, first enter the view for the command. To repeat multiple commands, first enter the view for the first command.

The **repeat** command executes commands in the order they were executed.

The system starts a timer and waits for your interaction when it repeats an interactive command. If you do not provide the required information at prompt before the timer expires, the system skips the interactive command.

The system skips all password configuration commands.Examples

Configure the system to execute the two most recently executed commands (**display cpu-usage** and **display clock**) three times at an interval of 10 seconds.

```
<Sysname> repeat 2 count 3 delay 10
<Sysname> display cpu
Slot 1 CPU 0 CPU usage:
      33% in last 5 seconds
      32% in last 1 minute
      33% in last 5 minutes
<Sysname> display clock
07:02:18.230 UTC Thu 06/19/2017
<Sysname> display cpu-usage
Slot 1 CPU 0 CPU usage:
      33% in last 5 seconds
      32% in last 1 minute
      33% in last 5 minutes
<Sysname> display clock
07:02:28.263 UTC Thu 06/19/2017
<Sysname> display cpu-usage
```

```
Slot 1 CPU 0 CPU usage:
      33% in last 5 seconds
      32% in last 1 minute
      33% in last 5 minutes
<Sysname> display clock
07:02:38.293 UTC Thu 06/19/2017
```

1.1.13. return

Use **return** to return to user view from any other view.

Syntax

return

Views

Any view except user view

Predefined user roles

network-admin

network-operator

Usage guidelines

Pressing **Ctrl+Z** has the same effect as the **return** command.

Examples

Return to user view from GigabitEthernet 1/0/1 interface view.

```
[Switch-GigabitEthernet1/0/1] return
<Switch>
```

1.1.14. screen-length disable

Use **screen-length disable** to disable pausing between screens of output for the current CLI session.

Use **undo screen-length disable** to enable pausing between screens of output for the current CLI session.

Syntax

screen-length disable

undo screen-length disable

Default

The default depends on the configuration of the **screen-length** command in user line view.

The following are the default settings for the **screen-length** command:

- Pausing between screens of output.
- Displaying up to 24 lines on a screen.

Views

User view

Predefined user roles

network-admin

Usage guidelines

If you disable pausing between screens of output, all output is displayed. The screen is refreshed continuously until the final screen is displayed.

This command takes effect only for the current CLI session. When you are logged out, the default is restored.

Examples

Disable pausing between screens of output for the current CLI session.

```
<Switch> screen-length disable
```

Related commands

screen-length

1.1.15. system-view

Use **system-view** to enter system view from user view.

Syntax

system-view

Views

User view

Predefined user roles

network-admin

network-operator

Examples

Enter system view from user view.

```
<Switch> system-view
System View: return to User View with Ctrl+Z.
[Switch]
```

Contents

A page of this section is **1-x-x**

2. RBAC commands ····· 2-1
2.1. RBAC commands ····· 2-1
2.1.1. description ····· 2-1
2.1.2. display role ····· 2-1
2.1.3. display role feature ····· 2-8
2.1.4. display role feature-group ····· 2-11
2.1.5. feature ····· 2-14
2.1.6. interface policy deny ····· 2-14
2.1.7. permit interface ····· 2-15
2.1.8. permit vlan ····· 2-17
2.1.9. permit vpn-instance ····· 2-18
2.1.10. role ····· 2-20
2.1.11. role default-role enable ····· 2-21
2.1.12. role feature-group ····· 2-21
2.1.13. rule ····· 2-22
2.1.14. super ····· 2-26
2.1.15. super authentication-mode ····· 2-27
2.1.16. super default role ····· 2-28
2.1.17. super password ····· 2-29
2.1.18. vlan policy deny ····· 2-30
2.1.19. vpn-instance policy deny ····· 2-31

2. RBAC commands

2.1. RBAC commands

2.1.1. description

Use **description** to configure a description for a user role for easy identification.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

A user role does not have a description.

Views

User role view

Predefined user roles

network-admin

Parameters

text: Specifies a description, a case-sensitive string of 1 to 128 characters.

Examples

Configure the description as **labVIP** for user role **role1**.

```
<Switch> system-view
[Switch] role name role1
[Switch-role-role1] description labVIP
```

Related commands

display role

role

2.1.2. display role

Use **display role** to display user role information.

Syntax

display role [**name** *role-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

name *role-name*: Specifies a user role name, a case-sensitive string of 1 to 63 characters. If you do not specify a user role name, the command displays information about all user roles, including the predefined user roles.

Examples

Display information about user role **123**.

```
<Switch> display role name 123
Role: 123
  Description: new role
  VLAN policy: deny
  Permitted VLANs: 1 to 5, 7 to 8
  Interface policy: deny
  Permitted interfaces: GigabitEthernet1/0/1 to GigabitEthernet1/0/3, Vlan-interface1 to
Vlan-interface20
  VPN instance policy: permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ----------------------------------------------------------------------
  1       permit RWX   feature-group abc
  2       deny   -W-   feature       ldap
  3       permit       command       system ; radius sc *
  4       permit R--   xml-element   -
  5       permit RW-   oid           1.2.1
  R:Read W:Write X:Execute
```

Display information about all user roles.

```
<Switch> display role
Role: network-admin
  Description: Predefined network admin role has access to all commands on the
  device
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ----------------------------------------------------------------------
  sys-1   permit       command       *
  sys-2   permit RWX   web-menu      -
  sys-3   permit RWX   xml-element   -
  sys-4   deny         command       display security-logfile summary
  sys-5   deny         command       system-view ; info-center
                                     security-logfile directory *
  sys-6   deny         command       security-logfile save
  sys-7   permit RW-   oid           1
  R:Read W:Write X:Execute

Role: network-operator
  Description: Predefined network operator role has access to all read commands
```

```
on the device
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ----------------------------------------------------------------------
  sys-1   permit       command       display *
  sys-2   permit       command       xml
  sys-3   permit       command       system-view ; probe ; display *
  sys-4   deny         command       display history-command all
  sys-5   deny         command       display exception *
  sys-6   deny         command       display cpu-usage configuration *
  sys-7   deny         command       display kernel exception *
  sys-8   deny         command       display kernel deadloop *
  sys-9   deny         command       display kernel starvation *
  sys-10  deny         command       display kernel reboot *
  sys-13  permit       command       system-view ; local-user *
  sys-15  permit R--   web-menu      -
  sys-16  permit R--   xml-element   -
  sys-17  deny         command       display security-logfile summary
  sys-18  deny         command       system-view ; info-center
                                     security-logfile directory *
  sys-19  deny         command       security-logfile save
  sys-20  deny         command       system-view ; local-user-import *
  sys-21  deny         command       system-view ; local-user-export *
  sys-22  permit R--   oid           1
  R:Read W:Write X:Execute

Role: level-0
  Description: Predefined level-0 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ----------------------------------------------------------------------
  sys-1   permit       command       tracert *
  sys-2   permit       command       telnet *
  sys-3   permit       command       ping *
  sys-4   permit       command       ssh2 *
  sys-5   permit       command       super *
  sys-6   permit       command       mtrace *
  R:Read W:Write X:Execute

Role: level-1
  Description: Predefined level-1 role
  VLAN policy: permit (default)
```

```
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ----------------------------------------------------------------------
  sys-1   permit       command       tracert *
  sys-2   permit       command       telnet *
  sys-3   permit       command       ping *
  sys-4   permit       command       ssh2 *
  sys-5   permit       command       display *
  sys-6   permit       command       super *
  sys-7   deny         command       display history-command all
  sys-8   permit       command       mtrace *
  R:Read W:Write X:Execute

Role: level-2
  Description: Predefined level-2 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)

Role: level-3
  Description: Predefined level-3 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)

Role: level-4
  Description: Predefined level-4 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)

Role: level-5
  Description: Predefined level-5 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)

Role: level-6
  Description: Predefined level-6 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)

Role: level-7
  Description: Predefined level-7 role
  VLAN policy: permit (default)
```

```
  Interface policy: permit (default)
  VPN instance policy: permit (default)

Role: level-8
  Description: Predefined level-8 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)

Role: level-9
  Description: Predefined level-9 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ----------------------------------------------------------------------
  sys-1   permit RWX   feature       -
  sys-2   deny   RWX   feature       device
  sys-3   deny   RWX   feature       filesystem
  sys-4   permit       command       display *
  sys-5   deny         command       display history-command all
  R:Read W:Write X:Execute

Role: level-10
  Description: Predefined level-10 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)

Role: level-11
  Description: Predefined level-11 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)

Role: level-12
  Description: Predefined level-12 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)

Role: level-13
  Description: Predefined level-13 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
```

```
Role: level-14
  Description: Predefined level-14 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)

Role: level-15
  Description: Predefined level-15 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  ------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ------------------------------------------------------------------
  sys-1   permit       command       *
  sys-2   permit RWX   web-menu      -
  sys-3   permit RWX   xml-element   -
  sys-4   deny         command       display security-logfile summary
  sys-5   deny         command       system-view ; info-center
                                     security-logfile directory *
  sys-6   deny         command       security-logfile save
  sys-7   permit RW-   oid           1
  R:Read W:Write X:Execute

Role: security-audit
  Description: Predefined security audit role only has access to commands for
the security log administrator
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  ------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ------------------------------------------------------------------
  sys-1   deny         command       *
  sys-2   permit       command       display security-logfile summary
  sys-3   permit       command       system-view ; info-center
                                     security-logfile directory *
  sys-4   permit       command       security-logfile save
  sys-5   permit       command       cd *
  sys-6   permit       command       copy *
  sys-7   permit       command       delete *
  sys-8   permit       command       dir *
  sys-9   permit       command       mkdir *
  sys-10  permit       command       more *
  sys-11  permit       command       move *
  sys-12  permit       command       rmdir *
  sys-13  permit       command       pwd
  sys-14  permit       command       rename *
```

```
  sys-15  permit       command       undelete *
  sys-16  permit       command       ftp *
  sys-17  permit       command       sftp *
  R:Read W:Write X:Execute

Role: guest-manager
  Description: Predefined guest manager role can't access to commands
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ----------------------------------------------------------------------
  sys-1   permit RWX   xml-element   useraccounts/approveguest/
  sys-2   permit RWX   xml-element   useraccounts/exportguestaccount/
  sys-3   permit RWX   xml-element   useraccounts/generateguestaccount/
  sys-4   permit RWX   xml-element   useraccounts/guest/
  sys-5   permit RWX   xml-element   useraccounts/guestconfigure/
  sys-6   permit RWX   xml-element   useraccounts/importguestaccount/
  sys-7   permit RWX   xml-element   useraccounts/exportguesttemplet/
  sys-8   permit RWX   xml-element   rpc/
  sys-9   deny         command       *
  R:Read W:Write X:Execute
```

Table 2-1 Command output

Field	Description
Role	User role name. Predefined user role names: • network-admin. • network-operator. • level-*n* (where *n* represents an integer in the range of 0 to 15). • security-audit. • guest-manager. This user role is not supported in the current software version.
Description	User role description.
VLAN policy	VLAN policy of the user role: • **deny**—Denies access to any VLANs except for permitted VLANs. • **permit (default)**—Default VLAN policy, which enables the user role to access all VLANs.
Permitted VLANs	VLANs accessible to the user role.
Interface policy	Interface policy of the user role: • **deny**—Denies access to any interfaces except for permitted interfaces. • **permit (default)**—Default interface policy, which enables the user role to access all interfaces.
Permitted interfaces	Interfaces accessible to the user role.

Field	Description
VPN instance policy	VPN instance policy of the user role: • **deny**—Denies access to any VPN instances except for permitted VPN instances. • **permit (default)**—Default VPN instance policy, which enables the user role to access all VPN instances.
Permitted VPN instances	VPN instances accessible to the user role.
Rule	User role rule number. Predefined user role rules are identified by sys-*n*, where *n* represents an integer.
Perm	Access control type: • **permit**—User role has access to the items in the **Entity** field. • **deny**—User role does not have access to the items in the **Entity** field.
Type	Controlled type: • **R**—Read-only. • **W**—Write. • **X**—Execute.
Scope	Rule control scope: • **command**—Controls access to the command or commands, as specified in the **Entity** field. • **feature**—Controls access to the commands of the feature, as specified in the **Entity** field. • **feature-group**—Controls access to the commands of the features in the feature group, as specified in the **Entity** field. • **web-menu**—Controls access to Web menus. This rule control scope is not supported in the current software version. • **xml-element**—Controls access to XML elements. • **oid**—Controls access to MIB nodes.
Entity	Command string, feature name, feature group, XML element, or OID specified in the user role rule: • An en dash (–) represents any feature. • An asterisk (*) represents zero or more characters.

Related commands

role

2.1.3. display role feature

Use **display role feature** to display features available in the system.

Syntax

display role feature [**name** *feature-name* | **verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

name *feature-name*: Specifies a feature by feature name. The *feature-name* argument represents the feature name, and all letters must be in lower case.

verbose: Displays the commands of each feature.

Usage guidelines

If you do not specify any parameters, the command displays only the list of features available in the system.

Examples

Display the list of feature names.

```
<Switch> display role feature
Feature: device           (Device configuration related commands)
Feature: interface        (Interface related commands)
Feature: syslog           (Syslog related commands)
…
```

Display the commands of each feature.

```
<Switch> display role feature verbose
Feature: device           (Device configuration related commands)
  display clock    (R)
  debugging dev    (W)
  display debugging dev    (R)
  display device *    (R)
  display diagnostic-information *    (R)
  display environment *    (R)
  display fan *    (R)
  display power *    (R)
  display current-configuration *    (R)
  display saved-configuration *    (R)
  display default-configuration *    (R)
  display startup    (R)
  display this *    (R)
…
```

Display the commands of feature **aaa**.

```
<Switch> display role feature name aaa
Feature: aaa              (AAA related commands)
  system-view ; domain *    (W)
  system-view ; header *    (W)
  system-view ; aaa *    (W)
  display domain *    (R)
  display aaa *    (R)
  system-view ; user-group *    (W)
  system-view ; local-user *    (W)
  display local-user *    (R)
```

```
display user-group *    (R)
display debugging local-server    (R)
debugging local-server *    (W)
super *    (X)
display password-control *    (R)
reset password-control *    (W)
system-view ; password-control *    (W)
```

…

Table 2-2 Command output (display role feature name aaa)

Field	Description
Feature	Displays the name and brief function description of the feature.
system-view ; domain *	All commands that start with the **domain** keyword in system view, and all commands in ISP domain view.
system-view ; header *	All commands that start with the **header** keyword in system view.
system-view ; aaa *	All commands that start with the **aaa** keyword in system view.
display domain *	All commands that start with the **display domain** keywords in user view.
system-view ; user-group *	All commands that start with the **user-group** keyword in system view, and all commands in user group view.
system-view ; local-user *	All commands that start with the **local-user** keyword in system view, and all commands in local user view.
display local-user *	All commands that start with the **display local-user** keywords in user view.
display user-group *	All commands that start with the **display user-group** keywords in user view.
display debugging local-server	All commands that start with the **display debugging local-server** keywords in user view.
debugging local-server *	All commands that start with the **debugging local-server** keywords in user view.
super *	All commands that start with the **super** keyword in user view.
display password-control *	All commands that start with the **display password-control** keywords in user view.
reset password-control *	All commands that start with the **reset password-control** keywords in user view.
system-view ; password-control *	All commands that start with the **password-control** keyword in system view.
(W)	Command type is Write. A write command configures the system.
(R)	Command type is Read. A read command displays configuration or maintenance information.

Field	Description
(X)	Command type is Execute. An execute command executes a specific function.

Related commands

feature

2.1.4. display role feature-group

Use **display role feature-group** to display feature group information.

Syntax

display role feature-group [**name** *feature-group-name*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

name *feature-group-name*: Specifies a feature group. The *feature-group-name* argument represents the feature group name, a case-sensitive string of 1 to 31 characters. If you do not specify a feature group, the command displays information about all feature groups.

verbose: Displays the commands of each feature in feature groups. If you do not specify this keyword, the command displays only the feature lists of feature groups.

Usage guidelines

Feature groups **L2** and **L3** are predefined feature groups.

Examples

Display the feature lists of feature groups.

```
<Switch> display role feature-group
Feature group: L2
Feature: igmp-snooping    (IGMP-Snooping related commands)
Feature: mld-snooping     (MLD-Snooping related commands)
Feature: lacp             (LACP related commands)
Feature: stp              (STP related commands)
Feature: lldp             (LLDP related commands)
Feature: dldp             (DLDP related commands)
Feature: cfm              (CFM related commands)
Feature: eoam             (EOAM related commands)
Feature: smart-link       (Smart-link related commands)
Feature: monitor-link     (Monitor-link related commands)
Feature: loopbk-detect    (Loopback-detection related commands)
Feature: vlan             (Virtual LAN related commands)
Feature: evb              (EVB related commands)
Feature: mvrp             (MVRP related commands )
Feature: rrpp             (RRPP related commands)
```

```
Feature: erps             (ERPS related commands)
Feature: ofp              (OFP related commands)
Feature: port-security    (Port-security related commands)
Feature: l2pt             (L2PT related commands)

Feature group: L3
Feature: route            (Route management related commands)
Feature: staticrt         (Unicast static route related commands)
Feature: ospf             (Open Shortest Path First protocol related commands)
Feature: rip              (Routing Information Protocol related commands)
Feature: isis             (ISIS protocol related commands)
Feature: lisp             (LISP protocol related commands)
Feature: bgp              (Border Gateway Protocol related commands)
Feature: l3vpn            (Layer 3 Virtual Private Network related commands)
Feature: route-policy     (Routing Policy related commands)
Feature: multicast        (Multicast related commands)
Feature: pim              (Protocol Independent Multicast related commands)
Feature: igmp             (Internet Group Management Protocol related commands)
Feature: mld              (Multicast Listener Discovery related commands)
Feature: mcast-domain     (Multicast Domain related commands)
Feature: msdp             (Multicast Source Discovery Protocol related commands)
```

Display the commands in each feature group. For more information about the wildcards and marks used in the command list, see Table 2-2 .

```
<Switch> display role feature-group verbose
Feature group: L2
Feature: igmp-snooping    (IGMP-Snooping related commands)
  system-view ; igmp-snooping *     (W)
  system-view ; multicast-vlan *     (W)
  system-view ; vlan * ; igmp-snooping *     (W)
  system-view ; vlan * ; pim-snooping *     (W)
  system-view ; vsi * ; igmp-snooping *     (W)
  system-view ; vsi * ; pim-snooping *     (W)
  system-view ; interface * ; igmp-snooping *     (W)
  system-view ; interface * ; port multicast-vlan *     (W)
  display igmp-snooping *     (R)
  display pim-snooping *     (R)
  display multicast-vlan *     (R)
  display l2-multicast *     (R)
  system-view ; probe ; display system internal l2-multicast *     (R)
  system-view ; probe ; display system internal multicast-vlan *     (R)
  reset igmp-snooping *     (W)
  reset pim-snooping *     (W)
  reset multicast-vlan *     (W)
  reset l2-multicast *     (W)
  debugging igmp-snooping *     (W)
  display debugging igmp-snooping *     (R)
  system-view ; probe ; debugging system internal igmp-snooping *     (W)
```

```
Feature: mld-snooping    (MLD-Snooping related commands)
  system-view ; mld-snooping *    (W)
  system-view ; ipv6 multicast-vlan *    (W)
  system-view ; vlan * ; mld-snooping *    (W)
  system-view ; vlan * ; ipv6 pim-snooping *    (W)
  system-view ; vsi * ; mld-snooping *    (W)
  system-view ; vsi * ; ipv6 pim-snooping *    (W)
  system-view ; interface * ; mld-snooping *    (W)
  system-view ; interface * ; ipv6 port multicast-vlan *    (W)
  display mld-snooping *    (R)
  display ipv6 pim-snooping *    (R)
  display ipv6 multicast-vlan *    (R)
  display ipv6 l2-multicast *    (R)
  system-view ; probe ; display system internal ipv6 l2-multicast *    (R)
  system-view ; probe ; display system internal ipv6 multicast-vlan *    (R)
  reset mld-snooping *    (W)
  reset ipv6 pim-snooping *    (W)
  reset ipv6 multicast-vlan *    (W)
  reset ipv6 l2-multicast *    (W)
  debugging mld-snooping *    (W)
  display debugging mld-snooping *    (R)
  system-view ; probe ; debugging system internal mld-snooping *    (W)
…
```

Display the feature list of the **L3** feature group.

```
<Switch> display role feature-group name L3
Feature group: L3
Feature: route           (Route management related commands)
Feature: staticrt        (Unicast static route related commands)
Feature: ospf            (Open Shortest Path First protocol related commands)
Feature: rip             (Routing Information Protocol related commands)
Feature: isis            (ISIS protocol related commands)
Feature: lisp            (LISP protocol related commands)
Feature: bgp             (Border Gateway Protocol related commands)
Feature: l3vpn           (Layer 3 Virtual Private Network related commands)
Feature: route-policy    (Routing Policy related commands)
Feature: multicast       (Multicast related commands)
Feature: pim             (Protocol Independent Multicast related commands)
Feature: igmp            (Internet Group Management Protocol related commands)
Feature: mld             (Multicast Listener Discovery related commands)
Feature: mcast-domain    (Multicast Domain related commands)
Feature: msdp            (Multicast Source Discovery Protocol related commands)
```

Related commands

feature

role feature-group

2.1.5. feature

Use **feature** to add a feature to a feature group.

Use **undo feature** to remove a feature from a feature group.

Syntax

feature *feature-name*

undo feature *feature-name*

Default

A user-defined feature group does not have any features.

Views

Feature group view

Predefined user roles

network-admin

Parameters

feature-name: Specifies a feature name. You must enter the feature name in lower case.

Usage guidelines

Repeat the **feature** command to add multiple features to a feature group.

Examples

Add the AAA and ACL features to feature group **security-features**.

```
<Switch> system-view
[Switch] role feature-group name security-features
[Switch-featuregrp-security-features] feature aaa
[Switch-featuregrp-security-features] feature acl
```

Related commands

display role feature

display role feature-group

role feature-group

2.1.6. interface policy deny

Use **interface policy deny** to enter user role interface policy view.

Use **undo interface policy deny** to restore the default.

Syntax

interface policy deny

undo interface policy deny

Default

A user role has access to all interfaces.

Views

User role view

Predefined user roles

network-admin

Usage guidelines

To restrict the interface access of a user role to a set of interfaces, perform the following tasks:

1. Use **interface policy deny** to enter user role interface policy view.
2. Use **permit interface** to specify accessible interfaces.

NOTE:

The **interface policy deny** command denies the access of the user role to any interfaces if the **permit interface** command is not configured.

To configure an interface, make sure the interface is permitted by the user role interface policy in use. You can perform the following tasks on an accessible interface:

- Create, remove, or configure the interface.
- Enter interface view.
- Specify the interface in feature commands.

The create and remove operations are available only for logical interfaces.

Any change to a user role interface policy takes effect only on users who log in with the user role after the change.

Examples

Enter user role interface policy view of **role1**, and deny **role1** to access any interfaces.

```
<Switch> system-view
[Switch] role name role1
[Switch-role-role1] interface policy deny
[Switch-role-role1-ifpolicy] quit
```

Enter user role interface policy view of **role1**, and deny **role1** to access any interfaces except for GigabitEthernet 1/0/1 to GigabitEthernet 1/0/4.

```
<Switch> system-view
[Switch] role name role1
[Switch-role-role1] interface policy deny
[Switch-role-role1-ifpolicy] permit interface gigabitethernet 1/0/1 to gigabitethernet
1/0/4
```

Related commands

display role

permit interface

role

2.1.7. permit interface

Use **permit interface** to configure a list of interfaces accessible to a user role.

Use **undo permit interface** to disable the access of a user role to specific interfaces.

Syntax

permit interface *interface-list*

undo permit interface [*interface-list*]

Default

No permitted interfaces are configured in user role interface policy view.

Views

User role interface policy view

Predefined user roles

network-admin

Parameters

interface-list: Specifies a space-separated list of up to 10 interface items. Each interface item specifies one interface in the *interface-type interface-number* form or a range of interfaces in the *interface-type interface-number* **to** *interface-type interface-number* form. If you specify an interface range, the end interface must meet the following requirements:

- Be the same type as the start interface.
- Have a higher interface number than the start interface.

Usage guidelines

To permit a user role to access an interface after you configure the **interface policy deny** command, you must add the interface to the permitted interface list of the policy. With the user role, you can perform the following tasks to the interfaces in the permitted interface list:

- Create, remove, or configure the interfaces.
- Enter the interface views.
- Specify the interfaces in feature commands.

The create and remove operations are available only for logical interfaces.

You can repeat the **permit interface** command to add multiple permitted interfaces to a user role interface policy.

The **undo permit interface** command removes the entire list of permitted interfaces if you do not specify an interface.

Any change to a user role interface policy takes effect only on users who log in with the user role after the change.

Examples

1. Configure user role **role1**:

   # Permit user role **role1** to execute all commands available in interface view and VLAN view.

```
<Switch> system-view
[Switch] role name role1
[Switch-role-role1] rule 1 permit command system-view ; interface *
[Switch-role-role1] rule 2 permit command system-view ; vlan *
```

   # Permit the user role to access GigabitEthernet 1/0/1, and GigabitEthernet 1/0/3 to GigabitEthernet 1/0/5.

```
[Switch-role-role1] interface policy deny
[Switch-role-role1-ifpolicy] permit interface gigabitethernet 1/0/1 gigabitethernet
1/0/3 to gigabitethernet 1/0/5
[Switch-role-role1-ifpolicy] quit
[Switch-role-role1] quit
```

2. Verify that you cannot use user role **role1** to work on all interfaces except for GigabitEthernet 1/0/1 and GigabitEthernet 1/0/3 to GigabitEthernet 1/0/5:

   # Verify that you can enter GigabitEthernet 1/0/1 interface view.

   ```
   [Switch] interface gigabitethernet 1/0/1
   [Switch-GigabitEthernet1/0/1] quit
   ```

   # Verify that you can assign GigabitEthernet 1/0/5 to VLAN 10. In this example, the user role can access all VLANs because the default VLAN policy of the user role is used.

   ```
   [Switch] vlan 10
   [Switch-vlan10] port gigabitethernet 1/0/5
   [Switch-vlan10] quit
   ```

   # Verify that you cannot enter interface view of GigabitEthernet 1/0/2.

   ```
   [Switch] interface gigabitethernet 1/0/2
   Permission denied.
   ```

Related commands

display role

interface policy deny

role

2.1.8. permit vlan

Use **permit vlan** to configure a list of VLANs accessible to a user role.

Use **undo permit vlan** to remove the permission for a user role to access specific VLANs.

Syntax

permit vlan *vlan-id-list*

undo permit vlan [*vlan-id-list*]

Default

No permitted VLANs are configured in user role VLAN policy view.

Views

User role VLAN policy view

Predefined user roles

network-admin

Parameters

vlan-id-list: Specifies a space-separated list of up to 10 VLAN items. Each VLAN item specifies a VLAN by VLAN ID or specifies a range of VLANs in the form of *vlan-id1* **to** *vlan-id2*. The value range for the VLAN IDs is 1 to 4094. If you specify a VLAN range, the value for the *vlan-id2* argument must be greater than the value for the *vlan-id1* argument.

Usage guidelines

To permit a user role to access a VLAN after you configure the **vlan policy deny** command, you must add the VLAN to the permitted VLAN list of the policy. With the user role, you can perform the following tasks on the VLANs in the permitted VLAN list:

- Create, remove, or configure the VLANs.
- Enter the VLAN views.
- Specify the VLANs in feature commands.

You can repeat the **permit vlan** command to add multiple permitted VLANs to a user role VLAN policy.

The **undo permit vlan** command removes the entire list of permitted VLANs if you do not specify a VLAN.

Any change to a user role VLAN policy takes effect only on users who log in with the user role after the change.

Examples

1. Configure user role **role1**:

   # Permit user role **role1** to execute all commands available in interface view and VLAN view.

   ```
   <Switch> system-view
   [Switch] role name role1
   [Switch-role-role1] rule 1 permit command system-view ; interface *
   [Switch-role-role1] rule 2 permit command system-view ; vlan *
   ```

   # Permit user role **role1** to access VLANs 2, 4, and 50 to 100.

   ```
   [Switch-role-role1] vlan policy deny
   [Switch-role-role1-vlanpolicy] permit vlan 2 4 50 to 100
   [Switch-role-role1-vlanpolicy] quit
   [Switch-role-role1] quit
   ```

2. Verify that you cannot use user role **role1** to work on all VLANs except for VLANs 2, 4, and 50 to 100:

   # Verify that you can create VLAN 100 and enter VLAN view.

   ```
   [Switch] vlan 100
   [Switch-vlan100] quit
   ```

   # Verify that you can add GigabitEthernet 1/0/1 to VLAN 100 as an access port.

   ```
   [Switch] interface gigabitethernet 1/0/1
   [Switch-GigabitEthernet1/0/1] port access vlan 100
   [Switch-GigabitEthernet1/0/1] quit
   ```

   # Verify that you cannot create VLAN 101 or enter VLAN view.

   ```
   [Switch] vlan 101
   Permission denied.
   ```

Related commands

display role

role

vlan policy deny

2.1.9. permit vpn-instance

Use **permit vpn-instance** to configure a list of VPN instances accessible to a user role.

Use **undo permit vpn-instance** to disable the access of a user role to specific VPN instances.

Syntax

permit vpn-instance *vpn-instance-name*&<1-10>

undo permit vpn-instance [*vpn-instance-name*&<1-10>]

Default

No permitted VPN instances are configured in user role VPN instance policy.

Views

User role VPN instance policy view

Predefined user roles

network-admin

Parameters

vpn-instance-name&<1-10>: Specifies a space-separated list of up to 10 VPN instance names. Each name is a case-sensitive string of 1 to 31 characters.

Usage guidelines

To permit a user role to access a VPN instance after you configure the **vpn-instance policy deny** command, you must add the VPN instance to the permitted VPN instance list of the policy. With the user role, you can perform the following tasks on the VPN instances in the permitted VPN instance list:

- Create, remove, or configure the VPN instances.
- Enter the VPN instance views.
- Specify the VPN instances in feature commands.

You can repeat the **permit vpn-instance** command to add multiple permitted VPN instances to a user role VPN instance policy.

The **undo permit vpn-instance** command removes the entire list of permitted VPN instances if you do not specify a VPN instance.

Any change to a user role VPN instance policy takes effect only on users who log in with the user role after the change.

Examples

1. Configure user role **role1**:

   # Permit the user role to execute all commands available in system view and in the child views of system view.

   ```
   <Switch> system-view
   [Switch] role name role1
   [Switch-role-role1] rule 1 permit command system-view ; *
   ```

   # Permit the user role to access VPN instance **vpn1**.

   ```
   [Switch-role-role1] vpn policy deny
   [Switch-role-role1-vpnpolicy] permit vpn-instance vpn1
   [Switch-role-role1-vpnpolicy] quit
   [Switch-role-role1] quit
   ```

2. Verify that you cannot use user role **role1** to work on all VPN instances except for **vpn1**:

   # Verify that you can enter the view of **vpn1**.

   ```
   [Switch] ip vpn-instance vpn1
   [Switch-vpn-instance-vpn1] quit
   ```

   # Verify that you can specify the primary accounting server at 10.110.1.2 in VPN instance **vpn1** for RADIUS scheme **radius1**.

   ```
   [Switch] radius scheme radius1
   [Switch-radius-radius1] primary accounting 10.110.1.2 vpn-instance vpn1
   [Switch-radius-radius1] quit
   ```

   # Verify that you cannot create VPN instance **vpn2** or enter VPN instance view.

   ```
   [Switch] ip vpn-instance vpn2
   Permission denied.
   ```

Related commands

display role

role

vpn-instance policy deny

2.1.10. role

Use **role** to create a user role and enter its view, or enter the view of an existing user role.

Use **undo role** to delete a user role.

Syntax

role name *role-name*

undo role name *role-name*

Default

The system has the following predefined user roles: network-admin, network-operator, level-*n* (where *n* represents an integer in the range of 0 to 15), and security-audit.

Views

System view

Predefined user roles

network-admin

Parameters

name *role-name*: Specifies a username. The *role-name* argument is a case-sensitive string of 1 to 63 characters.

Usage guidelines

You can create a maximum of 64 user roles in addition to the predefined user roles.

You cannot delete the predefined user roles or change the permissions assigned to network-admin, network-operator, level-15, or security-audit.

You cannot assign the security-audit user role to non-AAA authentication users.

The access permissions of the level-0 to level-14 user roles can be modified through user role rules and resource access policies. However, you cannot make changes on the predefined access permissions of these user roles. For example, you cannot change the access permission of these user roles to the **display history-command all** command.

Examples

Create user role **role1** and enter its view.

```
<Switch> system-view
[Switch] role name role1
[Switch-role-role1]
```

Related commands

display role

interface policy deny

rule

vlan policy deny

vpn-instance policy deny

2.1.11. role default-role enable

Use **role default-role enable** to enable the default user role feature for remote AAA users.

Use **undo role default-role enable** to restore the default.

Syntax

role default-role enable [*role-name*]

undo role default-role enable

Default

The default user role feature is disabled. AAA users who do not have a user role cannot log in to the device.

Views

System view

Predefined user roles

network-admin

Parameters

role-name: Specifies a user role by its name for the default user role. The user role must already exist. The argument is a case-sensitive string of 1 to 63 characters.

Usage guidelines

The default user role feature assigns the default user role to AAA-authenticated users if the authentication server (local or remote) does not assign any user roles to the users. These users are allowed to access the system with the default user role.

For local authorization, this command is required if you do not use the **authorization-attribute user role** command to assign user roles to local users.

If AAA users have been assigned user roles, they log in with the user roles.

If you do not specify the *role-name* argument, the default user role is network-operator.

Examples

Enable the default user role feature.

```
<Switch> system-view
[Switch] role default-role enable
```

Related commands

role

2.1.12. role feature-group

Use **role feature-group** to create a user role feature group and enter its view, or enter the view of an existing user role feature group.

Use **undo role feature-group** to delete a user role feature group.

Syntax

role feature-group name *feature-group-name*

undo role feature-group name *feature-group-name*

Default

Two user role feature groups **L2** and **L3** exist.

Views

System view

Predefined user roles

network-admin

Parameters

name *feature-group-name*: Specifies a feature group name. The *feature-group-name* argument is a case-sensitive string of 1 to 31 characters.

Usage guidelines

The **L2** feature group includes all Layer 2 feature commands, and the **L3** feature group includes all Layer 3 feature commands. These predefined feature groups are not user configurable.

In addition to the predefined feature groups **L2** and **L3**, you can create a maximum of 64 user role feature groups.

Examples

Create feature group **security-features** and enter its view.

```
<Switch> system-view
[Switch] role feature-group name security-features
[Switch-featuregrp-security-features]
```

Related commands

display role feature

display role feature-group

feature

2.1.13. rule

Use **rule** to create or change a user role rule.

Use **undo rule** to delete user role rules.

Syntax

rule *number* { **deny** | **permit** } { **command** *command-string* | { **execute** | **read** | **write** } * { **feature** [*feature-name*] | **feature-group** *feature-group-name* | **oid** *oid-string*} }

undo rule { *number* | **all** }

Default

A user-defined user role does not have any rules and cannot access any resources.

Views

User role view

Predefined user roles

network-admin

Parameters

number: Specifies a rule number in the range of 1 to 256.

deny: Denies access to the specified commands, XML elements, or MIB nodes.

permit: Permits access to the specified commands, XML elements, or MIB nodes.

command *command-string*: Specifies a command string. The command string can represent a command or a group of commands. The *command-string* argument is a case-sensitive string of 1 to 128 characters, including the following characters:

- The wildcard asterisk (*).
- The delimiters space and tab.
- All printable characters.

execute: Specifies the execute commands, XML elements, or MIB nodes to execute a specific function or program. The **ping** command is an example of execute commands.

read: Specifies the read commands, XML elements, or MIB nodes to display configuration or maintenance information. The **display**, **dir**, **more**, and **pwd** commands are examples of read commands.

write: Specifies the write commands, XML elements, or MIB nodes to configure the system. The **ssh server enable** command is an example of write commands.

feature [*feature-name*]: Specifies one or all features. The *feature-name* argument is a case-sensitive character string. If you do not specify a feature name, you specify all the features in the system.

feature-group *feature-group-name*: Specifies a user-defined or predefined feature group. The *feature-group-name* argument represents the feature group name, a case-sensitive string of 1 to 31 characters. If the feature group has not been created, the rule takes effect after the group is created. To display the feature groups that have been created, use the **display role feature-group** command.

oid *oid-string*: Specifies an OID of a MIB node. The *oid-string* argument represents the OID, a case-insensitive string of 1 to 255 characters. The OID is a dotted numeric string that uniquely identifies the path from the root node to this node. For example, 1.3.6.1.4.1.25506.8.35.14.19.1.1.

all: Specifies all the user role rules.

Usage guidelines

You can define the following types of rules for different access control granularities:

- **Command rule**—Controls access to a command or a set of commands that match a regular expression.
- **Feature rule**—Controls access to the commands of a feature by command type.
- **Feature group rule**—Controls access to the commands of a group of features by command type.
- **OID rule**—Controls access to the specified MIB node and its child nodes by node type.

A user role can access the set of permitted resources specified in the user role rules. User role rules include predefined (identified by sys-n) and user-defined user role rules.

You can configure a maximum of 256 user-defined rules for a user role. The total number of user-defined user role rules cannot exceed 1024.

Any rule modification, addition, or removal for a user role takes effect only on the users who log in with the user role after the change.

Access to the file system commands is controlled by both the file system command rules and the file system feature rule.

A command with output redirection to the file system is permitted only when the command type write is assigned to the file system feature.

The following guidelines apply to non-OID rules:

- If two user-defined rules of the same type conflict, the rule with the higher ID takes effect. For example, a user role can use the **tracert** command but not the **ping** command if the user role contains rules configured by using the following commands:
  - **rule** *1* **permit command** *ping*
  - **rule** *2* **permit command** *tracert*
  - **rule** *3* **deny command** *ping*
- If a predefined user role rule and a user-defined user role rule conflict, the user-defined user role rule takes effect.

The following guidelines apply to OID rules:

- The system compares an OID with the OIDs specified in rules, and it uses the longest match principle to select a rule for the OID. For example, a user role cannot access the MIB node with OID 1.3.6.1.4.1.25506.141.3.0.1 if the user role contains rules configured by using the following commands:
  - **rule** *1* **permit read write oid** *1.3.6*
  - **rule** *2* **deny read write oid** *1.3.6.1.4.1*
  - **rule** *3* **permit read write oid** *1.3.6.1.4*
- If the same OID is specified in multiple rules, the rule with the higher ID takes effect. For example, a user role can access the MIB node with OID 1.3.6.1.4.1.25506.141.3.0.1 if the user role contains rules configured by using the following commands:
  - **rule** *1* **permit read write oid** *1.3.6*
  - **rule** *2* **deny read write oid** *1.3.6.1.4.1*
  - **rule** *3* **permit read write oid** *1.3.6.1.4.1*

When you specify a command string, follow the guidelines in Table 2-3 .

Table 2-3 Command string configuration rules

Rule	Guidelines
Semicolon (;) is the delimiter.	Use a semicolon to separate the command of each view that you must enter before you access a command or a set of commands. However, do not use a semicolon to separate commands available in user view or any view, for example, **display** and **dir**. Each semicolon-separated segment must have a minimum of one printable character. To specify the commands in a view but not the commands in the view's subviews, use a semicolon as the last printable character in the last segment. To specify the commands in a view and the view's subviews, the last printable character in the last segment must not be a semicolon. For example, you must enter system view before you enter interface view. To specify all commands starting with the **ip** keyword in any interface view, you must use the "system ; interface * ; ip * ;" command string. For another example, the "system ; radius scheme * ;" command string represents all commands that start with the

Rule	Guidelines
	radius scheme keywords in system view. The "system ; radius scheme *" command string represents all commands that start with the **radius scheme** keywords in system view and all commands in RADIUS scheme view.
Asterisk (*) is the wildcard.	An asterisk represents zero or multiple characters. In a non-last segment, you can use an asterisk only at the end of the segment. In the last segment, you can use an asterisk in any position of the segment. If the asterisk appears at the beginning, you cannot specify a printable character behind the asterisk. For example, the "system ; *" command string represents all commands available in system view and all subviews of the system view. The "debugging * event" command string represents all event debugging commands available in user view.
Keyword abbreviation is allowed.	You can specify a keyword by entering the first few characters of the keyword. Any command that starts with this character string matches the rule. For example, "rule 1 deny command dis arp source *" denies access to the commands **display arp source-mac interface** and **display arp source-suppression**.
To control the access to a command, you must specify the command immediately after the view that has the command.	To control access to a command, you must specify the command immediately behind the view to which the command is assigned. The rules that control command access for any subview do not apply to the command. For example, the "rule 1 deny command system ; interface * ; *" command string disables access to any command that is assigned to interface view. However, you can still execute the **acl advanced** command in interface view, because this command is assigned to system view rather than interface view. To disable access to this command, use "rule 1 deny command system ; acl *;".
Do not include the vertical bar (|), greater-than sign (>), or double greater-than sign (>>) when you specify **display** commands in a user role command rule.	The system does not treat the redirect signs and the parameters that follow the signs as part of command lines. However, in user role command rules, these redirect signs and parameters are handled as part of command lines. As a result, no rule that includes any of these signs can find a match. For example, "rule 1 permit command display debugging > log" can never find a match. This is because the system has a **display debugging** command but not a **display debugging > log** command.

Examples

Permit user role **role1** to execute the **display acl** command.

```
<Switch> system-view
[Switch] role name role1
[Switch-role-role1] rule 1 permit command display acl
```

Permit user role **role1** to execute all commands that start with the **display** keyword.

```
[Switch-role-role1] rule 2 permit command display *
```

Permit user role **role1** to execute the **radius scheme aaa** command in system view and use all commands assigned to RADIUS scheme view.

```
[Switch-role-role1] rule 3 permit command system ; radius scheme aaa
```

Deny the access of **role1** to the read or write commands of any features.

```
[Switch-role-role1] rule 4 deny read write feature
```

Deny the access of **role1** to the read commands of the **aaa** feature.

```
[Switch-role-role1] rule 5 deny read feature aaa
```

Permit **role1** to access all read, write, and execute commands of feature group **security-features**.

```
[Switch-role-role1] rule 6 permit read write execute feature-group security-features
```

Permit **role1** to access all read and write MIB nodes starting from the node with OID 1.1.2.

```
[Switch-role-role1] rule 7 permit read write oid 1.1.2
```

Related commands

display role

display role feature

display role feature-group

role

2.1.14. super

Use **super** to obtain another user role without reconnecting to the device.

Syntax

super [*role-name*]

Views

User view

Predefined user roles

network-admin

Parameters

role-name: Specifies a user role, a case-sensitive string of 1 to 63 characters. The user role must exist in the system and cannot be security-audit. If you do not specify a user role, you obtain the default target user role which is set by using the **super default role** command.

Usage guidelines

The obtained user role is a temporary user role, because this command is effective only on the current login. The next time you are logged in with the user account, the original user role settings take effect.

To enable a user to obtain another user role without reconnecting to the device, you must configure user role authentication.

- If no local password is configured in the local password authentication (**local**), an AUX user can obtain the user role by either entering a string or not entering anything.
- If no local password is configured in the local-then-remote authentication (**local scheme**), the following rules apply:
  - A VTY user performs remote authentication.
  - An AUX user can obtain user role authorization by either entering a string or not entering anything.

Examples

Obtain the user role network-operator.

```
<Switch> super network-operator
Password:
User privilege role is network-operator, and only those commands that authorized to the role can be used.
```

Related commands

authentication super (*Security Command Reference*)

super authentication-mode

super password

2.1.15. super authentication-mode

Use **super authentication-mode** to set an authentication mode for temporary user role authorization.

Use **undo super authentication-mode** to restore the default.

Syntax

super authentication-mode { **local** | **scheme** } *

undo super authentication-mode

Default

Local password authentication applies.

Views

System view

Predefined user roles

network-admin

Parameters

local: Enables local password authentication.

scheme: Enables remote AAA authentication.

Usage guidelines

For local password authentication, use the **super password** command to set a password.

For remote AAA authentication, set the username and password on the RADIUS server.

If you specify both **local** and **scheme** keywords, the keyword first entered in the command takes precedence.

- **scheme local**—Enables remote-then-local authentication mode. The device first performs AAA authentication to obtain a temporary user role. Local password authentication is performed if the remote RADIUS server does not respond, or if the AAA configuration on the device is invalid.
- **local scheme**—Enables local-then-remote authentication mode. The device first performs local password authentication. If no password is configured for the user role, the device performs remote authentication for VTY users. An AUX user can obtain another user role by either entering a string or not entering anything.

For more information about AAA, see *Security Configuration Guide*.

Examples

Enable local-only authentication for temporary user role authorization.

```
<Switch> system-view
[Switch] super authentication-mode local
```

Enable remote-then-local authentication for temporary user role authorization.

```
<Switch> system-view
[Switch] super authentication-mode scheme local
```

Related commands

authentication super (*Security Command Reference*)

super password

2.1.16. super default role

Use **super default role** to specify the default target user role for temporary user role authorization.

Use **undo super default role** to restore the default.

Syntax

super default role *role-name*

undo super default role

Default

The default target user role is network-admin.

Views

System view

Predefined user roles

network-admin

Parameters

role-name: Specifies the name of the default target user role, a case-sensitive string of 1 to 63 characters. The user role must exist in the system and cannot be security-audit.

Usage guidelines

The default target user role is applied to the **super** or **super password** command when you do not specify a user role for the command.

Examples

Specify **network-operator** as the default target user role for temporary user role authorization.

```
<Switch> system-view
[Switch] super default role network-operator
```

Related commands

super

super password

2.1.17. super password

Use **super password** to set a password for a user role.

Use **undo super password** to delete the password for a user role.

Syntax

super password [**role** *role-name*] [{ **hash** | **simple** } *string*]

undo super password [**role** *role-name*]

Default

No password is set for a user role.

Views

System view

Predefined user roles

network-admin

Parameters

role *role-name*: Specifies a user role, a case-sensitive string of 1 to 63 characters. The user role must exist in the system and cannot be security-audit. If you do not specify a user role, the command sets a password for the default target user role which is set by using the **super default role** command.

hash: Specifies a password in hashed form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in hashed form.

string: Specifies the password. The plaintext form of the password is a case-sensitive string of 1 to 63 characters. The hashed form of the password is a case-sensitive string of 1 to 110 characters.

Usage guidelines

If you do not specify any parameters, you specify a plaintext password in the interactive mode.

Set a password if you configure local password authentication for temporary user role authorization.

It is a good practice to specify different passwords for different user roles.

Examples

Set the password to **123456TESTplat&!** in plaintext form for user role network-operator.

```
<Switch> system-view
[Switch] super password role network-operator simple 123456TESTplat&!
```

Set the password to **123456TESTplat&!** in the interactive mode for user role network-operator.

```
<Switch> system-view
[Switch] super password role network-operator
Password:
Confirm :
Updating user information. Please wait... ...
```

Related commands

super authentication-mode

super default role

2.1.18. vlan policy deny

Use **vlan policy deny** to enter user role VLAN policy view.

Use **undo vlan policy deny** to restore the default.

Syntax

vlan policy deny

undo vlan policy deny

Default

A user role has access to all VLANs.

Views

User role view

Predefined user roles

network-admin

Usage guidelines

To restrict the VLAN access of a user role to a set of VLANs, perform the following tasks:

1. Use **vlan policy deny** to enter user role VLAN policy view.
2. Use **permit vlan** to specify accessible VLANs.

NOTE:

The **vlan policy deny** command denies the access of the user role to any VLANs if the **permit vlan** command is not configured.

To configure a VLAN, make sure the VLAN is permitted by the user role VLAN policy in use. You can perform the following tasks on an accessible VLAN:

- Create, remove, or configure the VLAN.
- Enter VLAN view.
- Specify the VLAN in feature commands.

Any change to a user role VLAN policy takes effect only on users who log in with the user role after the change.

Examples

Enter user role VLAN policy view of **role1**, and deny the access of **role1** to any VLANs.

```
<Switch> system-view
[Switch] role name role1
[Switch-role-role1] vlan policy deny
[Switch-role-role1-vlanpolicy] quit
```

Enter user role VLAN policy view of **role1**, and deny the access of **role1** to any VLANs except for VLANs 50 to 100.

```
<Switch> system-view
[Switch] role name role1
[Switch-role-role1] vlan policy deny
[Switch-role-role1-vlanpolicy] permit vlan 50 to 100
```

Related commands

display role

permit vlan

role

2.1.19. vpn-instance policy deny

Use **vpn-instance policy deny** to enter user role VPN instance policy view.

Use **undo vpn-instance policy deny** to restore the default.

Syntax

vpn-instance policy deny

undo vpn-instance policy deny

Default

A user role has access to all VPN instances.

Views

User role view

Predefined user roles

network-admin

Usage guidelines

To restrict the VPN instance access of a user role to a set of VPN instances, perform the following tasks:

1. Use **vpn-instance policy deny** to enter user role VPN instance policy view.
2. Use **permit vpn-instance** to specify accessible VPN instances.

NOTE:

The **vpn-instance policy deny** command denies the access of the user role to any VPN instances if the **permit vpn-instance** command is not configured.

To configure a VPN instance, make sure the VPN instance is permitted by the user role VPN instance policy in use. You can perform the following tasks on an accessible VPN instance:

- Create, remove, or configure the VPN instance.
- Enter VPN instance view.
- Specify the VPN instance in feature commands.

Any change to a user role VPN instance policy takes effect only on users who log in with the user role after the change.

Examples

Enter user role VPN instance policy view of **role1**, and deny the access of **role1** to any VPN instances.

```
<Switch> system-view
[Switch] role name role1
[Switch-role-role1] vpn-instance policy deny
[Switch-role-role1-vpnpolicy] quit
```

Enter user role VPN instance policy view of **role1**, and deny the access of **role1** to any VPN instances except for **vpn2**.

```
<Switch> system-view
[Switch] role name role1
[Switch-role-role1] vpn-instance policy deny
[Switch-role-role1-vpnpolicy] permit vpn-instance vpn2
```

Related commands

display role

permit vpn-instance

role

Contents

A page of this section is **1-x-x**

3. Login management commands ····· 3-1
3.1. Login management commands ····· 3-1
3.1.1. authentication-mode ····· 3-1
3.1.2. auto-execute command ····· 3-2
3.1.3. databits ····· 3-3
3.1.4. display line ····· 3-4
3.1.5. display telnet client ····· 3-6
3.1.6. display users ····· 3-6
3.1.7. escape-key ····· 3-7
3.1.8. free line ····· 3-9
3.1.9. history-command max-size ····· 3-9
3.1.10. idle-timeout ····· 3-10
3.1.11. line ····· 3-11
3.1.12. line class ····· 3-12
3.1.13. lock ····· 3-13
3.1.14. parity ····· 3-13
3.1.15. protocol inbound ····· 3-14
3.1.16. restful https enable ····· 3-16
3.1.17. screen-length ····· 3-16
3.1.18. send ····· 3-17
3.1.19. set authentication password ····· 3-18
3.1.20. shell ····· 3-19
3.1.21. speed ····· 3-20
3.1.22. stopbits ····· 3-21
3.1.23. telnet ····· 3-21
3.1.24. telnet client source ····· 3-22
3.1.25. telnet ipv6 ····· 3-23
3.1.26. telnet server acl ····· 3-24
3.1.27. telnet server dscp ····· 3-25
3.1.28. telnet server enable ····· 3-25
3.1.29. telnet server ipv6 acl ····· 3-26
3.1.30. telnet server ipv6 dscp ····· 3-27
3.1.31. terminal type ····· 3-27
3.1.32. user-role ····· 3-28

3. Login management commands

3.1. Login management commands

Some login management commands are available in both user line view and user line class view. For these commands, the device uses the following rules to determine the settings to be activated:

- A setting in user line view applies only to the user line. A setting in user line class view applies to all user lines of the class.
- A non-default setting in either view takes precedence over a default setting in the other view. A non-default setting in user line view takes precedence over a non-default setting in user line class view.
- A setting in user line class view takes effect for login sessions that are established after the setting is configured.

3.1.1. authentication-mode

Use **authentication-mode** to set the authentication mode for a user line.

Use **undo authentication-mode** to restore the default.

Syntax

authentication-mode { **none** | **password** | **scheme** }

undo authentication-mode

Default

none

Views

User line view

User line class view

Predefined user roles

network-admin

Parameters

none: Disables authentication.

password: Performs local password authentication.

scheme: Performs AAA authentication. For more information about AAA, see *Security Configuration Guide*.

Usage guidelines

Only users assigned the network-admin, or level-15 user role can execute this command. Other users cannot execute this command, even if they are granted the right to execute this command.

When the authentication mode is **none**, a user can log in without authentication. To improve device security, use the password or scheme authentication mode.

In VTY line view, this command is associated with the **protocol inbound** command.

- If the settings of the two commands in VTY line view are both the default settings, the settings for the commands in VTY line class view take effect.

- If the settings of the two commands in VTY line view are both non-default settings, the non-default settings in VTY line view take effect.
- If only one command has a non-default setting in VTY line view, the other command uses the default setting, regardless of the setting in VTY line class view.

An authentication mode change does not take effect for the current session. It takes effect for subsequent login sessions.

Examples

Enable the **none** authentication mode for VTY line 0.

```
<Switch> system-view
[Switch] line vty 0
[Switch-line-vty0] authentication-mode none
```

Enable password authentication for VTY line 0 and set the password to **321**.

```
<Switch> system-view
[Switch] line vty 0
[Switch-line-vty0] authentication-mode password
[Switch-line-vty0] set authentication password simple 321
```

Enable scheme authentication for VTY line 0. Configure the local user **123** and set the password to **321**. Assign the Telnet service and the user role network-admin to the user.

```
<Switch> system-view
[Switch] line vty 0
[Switch-line-vty0] authentication-mode scheme
[Switch-line-vty0] quit
[Switch] local-user 123
[Switch-luser-manage-123] password simple 321
[Switch-luser-manage-123] service-type telnet
[Switch-luser-manage-123] authorization-attribute user-role network-admin
```

Related commands

set authentication password

3.1.2. auto-execute command

Use **auto-execute command** to specify the command to be automatically executed for a login user.

Use **undo auto-execute command** to restore the default.

Syntax

auto-execute command *command*

undo auto-execute command

Default

No command is specified to be automatically executed for a login user.

Views

User line view

User line class view

Predefined user roles

network-admin

Parameters

command: Specifies the command to be automatically executed.

Usage guidelines

CAUTION:

After configuring this command for a user line, you might be unable to access the CLI through the user line. Make sure you can access the CLI through a different user line before you configure this command and save the configuration.

The device will automatically execute the specified command when a user logs in through the user line, and close the user connection after the command is executed.

This command is not supported in AUX line view or AUX line class view.

This command is available in both user line view and user line class view. A non-default setting in either view takes precedence over a default setting in the other view. A non-default setting in user line view takes precedence over a non-default setting in user line class view.

A configuration change made by this command does not take effect for the current session. It takes effect for subsequent login sessions.

Examples

Configure the device to automatically execute the **telnet 192.168.1.41** command when a user logs in through VTY line 0.

```
<Switch> system-view
[Switch] line vty 0
[Switch-line-vty0] auto-execute command telnet 192.168.1.41
This action will lead to configuration failure through line-vty0. Are you sure?
[Y/N]:y
[Switch-line-vty0]
```

To verify the configuration, Telnet to the device (192.168.1.40).

The device automatically Telnets to 192.168.1.41. The following output is displayed on the configuration terminal:

```
C:\> telnet 192.168.1.40


<Switch>
Trying 192.168.1.41 ...
Press CTRL+K to abort
Connected to 192.168.1.41 ...
<Switch.41>
```

This operation is the same as directly logging in to the device at 192.168.1.41 through Telnet. When you close the Telnet connection to 192.168.1.41, the Telnet connection to 192.168.1.40 is closed at the same time.

3.1.3. databits

Use **databits** to specify the number of data bits for a character.

Use **undo databits** to restore the default.

Syntax

databits { **7** | **8** }

undo databits

Default

Eight data bits are used for a character.

Views

User line view

Predefined user roles

network-admin

Parameters

7: Uses seven data bits for a character.

8: Uses eight data bits for a character.

Usage guidelines

This command is not supported in VTY line class view.

This setting must be the same as the setting on the configuration terminal.

Examples

Configure AUX 0 to use seven data bits for a character.

```
<Switch> system-view
[Switch] line aux 0
[Switch-line-aux0] databits 7
```

3.1.4. display line

Use **display line** to display user line information.

Syntax

display line [*number1* | { **aux** | **vty** } *number2*] [**summary**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

number1: Specifies the absolute number of a user line. The value range is 0 to 83.

aux: Specifies the AUX line.

vty: Specifies the VTY line.

number2: Specifies the relative number of a user line. The value range is 0 to 9 for AUX line, and 0 to 63 for VTY lines.

summary: Displays summary information about user lines. If you do not specify this keyword, the command displays detailed information.

Examples

Display information about line 0.

```
<Switch> display line 0
  Idx  Type     Tx/Rx      Modem Auth  Int         Location
F 0    AUX 0    9600       -     N     -           1/0

  +    : Line is active.
  F    : Line is active and in async mode.
  Idx  : Absolute index of line.
  Type : Type and relative index of line.
  Auth : Login authentication mode.
  Int  : Physical port of the line.
  A    : Authentication use AAA.
  N    : No authentication is required.
  P    : Password authentication.
```

Table 3-1 Command output

Field	Description
Modem	Whether the modem allows calling in or out. By default, this attribute is not configured and this field displays a hyphen (-). This field is not supported in the current software version.
Int	Physical port for the line. If there is no physical port for the line or the port is a console port, this field displays a hyphen (-).
Location	Physical position of the line, in the form of *slot number*/*CPU number*.

Display summary information about all user lines.

```
<Switch> display line summary
  Line type : [AUX]
            0:XXXX XXXX XX
  Line type : [VTY]
           10:UXXX XXXX XXXX XXXX
           26:XXXX XXXX XXXX XXXX
           42:XXXX XXXX XXXX XXXX
           58:XXXX XXXX XXXX XXXX
  Line type : [USB]
           74:XXXX XXXX XX

   1 lines used.       (U)
  83 lines not used.   (X)
```

Table 3-2 Command output

Fields	Description
Line type	Type of the user line: • **AUX**–AUX line. • **VTY**–VTY line.
number:*status*	*number*: Absolute number of the first user line in the user line class.

Fields	Description
	status: User line status. **X** is for unused and **U** is for used.

3.1.5. display telnet client

Use **display telnet client** to display the packet source setting for the Telnet client.

Syntax

display telnet client

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

This command displays the source IPv4 address or source interface specified for the Telnet client to use in outgoing Telnet packets, depending on the **telnet client source** command.

Examples

Display the packet source setting for the Telnet client.

```
<Switch> display telnet client
 The source IP address is 1.1.1.1.
```

Related commands

telnet client source

3.1.6. display users

Use **display users** to display online CLI users.

Syntax

display users [**all**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

all: Displays all user lines supported by the device.

Examples

Display online user information.

```
<Switch> display users
  Idx  Line      Idle        Time               Pid     Type
+ 10   VTY 0     00:00:00    Jan 01 00:33:10    484     TEL
```

```
  12   VTY 2    00:06:22   Jan 01 00:33:22   495     TEL

Following are more details.
VTY 0   :
        Location: 192.168.1.107
VTY 2   :
        Location: 192.168.1.134
 +    : Current operation user.
 F    : Current operation user works in async mode.
```

Table 3-3 Command output

Field	Description
Idx	Absolute number of the user line.
Line	Type and relative number of the user line.
Idle	Time elapsed after the user's most recent input, in the *hh*:*mm*:*ss* format.
Time	Login time of the user.
Pid	Process ID of the user session.
Type	User type: • **TEL**–Telnet user. • **SSH**–SSH user. • For a user who logged in through the console, USB port, this field does not display anything.
+	User line you are using.
Location	IP address of the user.

3.1.7. escape-key

Use **escape-key** to set the escape key.

Use **undo escape-key** to disable the escape key.

Syntax

escape-key { *key-string* | **default** }

undo escape-key

Default

The escape key is **Ctrl+C**.

Views

User line view

User line class view

Predefined user roles

network-admin

Parameters

key-string: Specifies a shortcut key. It can be a character (case sensitive, except for **d** and **D**), or an ASCII code value in the range of 0 to 127. For example, if you configure **escape-key 1**, the

shortcut key is **Ctrl+A**. If you configure **escape-key a**, the shortcut key is **a**. If you specify the character **d** or **D** for this argument, the actual shortcut key is **Ctrl+C**. To use **d** or **D** as the shortcut key, you must specify the ASCII code value of the character for this argument. For information about ASCII code values of individual characters, see the standard ASCII code chart. For information about ASCII code values of combined keys that use the **Ctrl** key, see authentication-mode.

default: Restores the default escape key **Ctrl+C**.

Usage guidelines

You can press the escape key to abort a command that is being executed, for example, a **ping** or **tracert** command. Whether a command can be aborted by **Ctrl+C** by default depends on the software implementation of the command. For more information, see the usage guidelines for the command.

As a best practice, use a key sequence as the escape key. If you define a single character as the escape key, pressing the key while a command is being executed stops the command. If no command is being executed, pressing the key enters the character as a common character. If you Telnet from the device to a remote device, pressing the key enters the character as a common character on the remote device. The key acts as the escape key on the remote device only when the following conditions are met:

- You define the same character as the escape key on the remote device.
- You press the key while a command is being executed on the remote device.

The **undo escape-key** command disables the current escape key. After you execute this **undo** command, no escape key is available.

This command is available in both user line view and user line class view. A non-default setting in either view takes precedence over a default setting in the other view. A non-default setting in user line view takes precedence over a non-default setting in user line class view.

The setting in user line view takes effect immediately for the current session. The setting in user line class view takes effect for login sessions that are established after the setting is configured.

To display the current escape key, use the **display current-configuration | include escape-key** command.

Examples

Configure character **a** as the escape key for VTY line 0.

```
<Switch> system-view
[Switch] line vty 0
[Switch-line-vty0] escape-key a
```

To verify the configuration:

1. Ping IP address 192.168.1.49, specifying the **-c** keyword to set the number of ICMP echo request packets to 20.

```
<Switch> ping -c 20 192.168.1.49
  PING 192.168.1.49: 56  data bytes, press a to break
    Reply from 192.168.1.49: bytes=56 Sequence=1 ttl=255 time=3 ms
    Reply from 192.168.1.49: bytes=56 Sequence=2 ttl=255 time=3 ms
```

2. Press **a**.

   The system aborts the command and returns to user view.

```
  --- 192.168.1.49 ping statistics ---
    2 packet(s) transmitted
    2 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 3/3/3 ms
```

```
<Switch>
```

3.1.8. free line

Use **free line** to release a user line.

Syntax

free line { *number1* | { **aux** | **vty** } *number2* }

Views

User view

Predefined user roles

network-admin

Parameters

number1: Specifies the absolute number of a user line. The value range is 0 to 83.

aux: Specifies the AUX line.

vty: Specifies the VTY line.

number2: Specifies the relative number of a user line. The value range is 0 to 9 for AUX line, and 0 to 63 for VTY lines.

Usage guidelines

This command does not release the line you are using.

Examples

Release VTY line 1.

```
<Switch> free line vty 1
Are you sure to free line vty1? [Y/N]:y
 [OK]
```

3.1.9. history-command max-size

Use **history-command max-size** to set the size of the command history buffer for a user line.

Use **undo history-command max-size** to restore the default.

Syntax

history-command max-size *size-value*

undo history-command max-size

Default

The command history buffer for a user line stores up to 10 history commands.

Views

User line view

User line class view

Predefined user roles

network-admin

Parameters

size-value: Specifies the maximum number of history commands the buffer can store, in the range of 0 to 256.

Usage guidelines

Each user line uses a separate command history buffer to store commands successfully executed by its user. The buffer size determines how many history commands the buffer can store.

To display history commands in the buffer for your session, press the up or down arrow key, or execute the **display history-command** command. For more information about the command history buffer, see *Fundamentals Configuration Guide*.

Terminating a CLI session clears the commands in the command history buffer.

The setting in user line view takes effect immediately for the current session. The setting in user line class view takes effect for login sessions that are established after the setting is configured.

Examples

Set the command history buffer size to 20 for VTY line 0.

```
<Switch> system-view
[Switch] line vty 0
[Switch-line-vty0] history-command max-size 20
```

3.1.10. idle-timeout

Use **idle-timeout** to set the CLI connection idle-timeout timer.

Use **undo idle-timeout** to restore the default.

Syntax

idle-timeout *minutes* [*seconds*]

undo idle-timeout

Default

The CLI connection idle-timeout timer is 10 minutes.

Views

User line view

User line class view

Predefined user roles

network-admin

Parameters

minutes: Specifies the number of minutes, in the range of 0 to 35791.

seconds: Specifies the number of seconds, in the range of 0 to 59. The default is 0 seconds.

Usage guidelines

The system automatically terminates a user connection if no information interaction occurs on the connection within the idle-timeout interval.

To disable the idle-timeout feature, execute the **idle-timeout 0** command.

This command is available in both user line view and user line class view. A non-default setting in either view takes precedence over a default setting in the other view. A non-default setting in user line view takes precedence over a non-default setting in user line class view.

The setting in user line view takes effect immediately for the current session. The setting in user line class view takes effect for login sessions that are established after the setting is configured.

Examples

Set the CLI connection idle-timeout timer to 1 minute and 30 seconds for VTY line 0.

```
<Switch> system-view
[Switch] line vty 0
[Switch-line-vty0] idle-timeout 1 30
```

3.1.11. line

Use **line** to enter one or multiple user line views.

Syntax

line { *first-number1* [*last-number1*] | { **aux** | **vty** } *first-number2* [*last-number2*] }

Views

System view

Predefined user roles

network-admin

Parameters

first-number1: Specifies the absolute number of the first user line. The value range is 0 to 83.

last-number1: Specifies the absolute number of the last user line. The value range is 1 to 83. This number must be greater than *first-number1*.

aux: Specifies the AUX line.

vty: Specifies the VTY line.

first-number2: Specifies the relative number of the first user line. The value range is 0 to 9 for AUX line, and 0 to 63 for VTY lines.

last-number2: Specifies the relative number of the last user line. The value range is 1 to 9 for AUX line, and 1 to 63 for VTY lines. This number must be greater than *first-number2*.

Examples

Enter the view of VTY line 0.

```
<Switch> system-view
[Switch] line vty 0
[Switch-line-vty0]
```

Enter the views of VTY lines 0 to 63.

```
<Switch> system-view
[Switch] line vty 0 63
[Switch-line-vty0-63]
```

Related commands

line class

3.1.12. line class

Use **line class** to enter user line class view.

Syntax

line class { **aux** | **vty** }

Views

System view

Predefined user roles

network-admin

Parameters

aux: Specifies the AUX line class view.

vty: Specifies the VTY line class view.

Usage guidelines

To configure the same settings for all user lines of a line class, use this command to enter the user line class view.

In user line class view, you can execute the following commands:

- **auto-execute command**
- **authentication-mode**
- **escape-key**
- **history-command max-size**
- **idle-timeout**
- **protocol inbound**
- **screen-length**
- **set authentication password**
- **shell**
- **terminal type**
- **user-role**

For commands that are available in both user line view and user line class view, the device uses the following rules to determine the settings to use:

- A setting in user line view applies only to the user line. A setting in user line class view applies to all user lines of the class.
- A non-default setting in either view takes precedence over a default setting in the other view. A non-default setting in user line view takes precedence over a non-default setting in user line class view.
- A setting in user line class view does not take effect for current online users. It takes effect only for new login users.

Examples

Set the CLI connection idle-timeout timer to 15 minutes in VTY line class view.

```
<Switch> system-view
[Switch] line class vty
[Switch-line-class-vty] idle-timeout 15
```

Related commands

line

3.1.13. lock

Use **lock** to lock the current user line and set the password for unlocking the line.

Syntax

lock

Default

The system does not lock any user lines.

Views

User view

Predefined user roles

network-admin

Usage guidelines

This command locks the current user line to prevent unauthorized users from using the line. You must set the password for unlocking the line as prompted. The user line is locked after you enter the password and confirm the password.

To unlock the user line, press **Enter** and enter the password you set.

Examples

Lock the current user line and set the password for unlocking the line.

```
<Switch> lock
Please input password<1 to 16> to lock current line:
Password:
Again:

                    locked !
```

// The user line is locked. To unlock it, press **Enter** and enter the password:

```
Password:
<Switch>
```

3.1.14. parity

Use **parity** to specify the parity.

Use **undo parity** to restore the default.

Syntax

parity { **even** | **mark** | **none** | **odd** | **space** }

undo parity

Default

The setting is **none**. No parity is used.

Views

User line view

Predefined user roles

network-admin

Parameters

even: Uses even parity.

mark: Uses mark parity.

none: Uses no parity.

odd: Uses odd parity.

space: Uses space parity.

Usage guidelines

This command is not supported in VTY line view.

The configuration terminal and the device must use the same parity.

Examples

Configure AUX line 0 to use odd parity.

```
<Switch> system-view
[Switch] line aux 0
[Switch-line-aux0] parity odd
```

3.1.15. protocol inbound

Use **protocol inbound** to specify the supported protocols.

Use **undo protocol inbound** to restore the default.

Syntax

protocol inbound { **all** | **ssh** | **telnet** }

undo protocol inbound

Default

All protocols are supported.

Views

VTY line view

VTY line class view

Predefined user roles

network-admin

Parameters

all: Supports all protocols, including SSH and Telnet.

ssh: Supports SSH only.

telnet: Supports Telnet only.

Usage guidelines

Only users assigned the network-admin, or level-15 user role can execute this command. Other users cannot execute this command, even if they are granted the right to execute this command.

A configuration change in user line view does not take effect for the current session. It takes effect for subsequent login sessions.

Before configuring a user line to support SSH, set the authentication mode to **scheme** for the user line.

In VTY line view, this command is associated with the **authentication-mode** command. If you specify a non-default value for one of the two commands, the other command uses the default setting, regardless of the setting in VTY line class view.

- If the settings of the two commands in VTY line view are both the default settings, the settings for the commands in VTY line class view take effect.
- If the settings of the two commands in VTY line view are both non-default settings, the non-default settings in VTY line view take effect.
- If only one command has a non-default setting in VTY line view, the other command uses the default setting, regardless of the setting in VTY line class view.

Examples

Enable user lines VTY 0 through VTY 4 to support only SSH.

```
<Switch> system-view
[Switch] line vty 0 4
[Switch-line-vty0-4] authentication-mode scheme
[Switch-line-vty0-4] protocol inbound ssh
```

Enable SSH support and set the authentication mode to scheme in VTY line class view. Enable user lines VTY 0 through VTY 4 to support all protocols and disable authentication for the user lines.

```
<Switch> system-view
[Switch] line class vty
[Switch-line-class-vty] authentication-mode scheme
[Switch-line-class-vty] protocol inbound ssh
[Switch-line-class-vty] line vty 0 4
[Switch-line-vty0-4] authentication-mode none
```

To verify the configuration:

1. Telnet to the device.

```
<Client> telnet 192.168.1.241
Trying 192.168.1.241 ...
Press CTRL+K to abort
Connected to 192.168.1.241 ...


<Server>
```

You are logged in without authentication.

2. Display online CLI user information.

```
<Server> display users
  Idx  Line      Idle        Time               Pid      Type
+ 50   VTY 0     00:00:00    Jan 17 15:29:27    189      TEL

Following are more details.
```

```
VTY 0    :
         Location: 192.168.1.186
 +       : Current operation user.
 F       : Current operation user works in async mode.
```

The output shows that you are using VTY 0. The configuration in user line view is effective.

Related commands

authentication-mode

3.1.16. restful https enable

Use **restful https enable** to enable RESTful access over HTTPS.

Use **undo restful https enable** to disable RESTful access over HTTPS.

Syntax

restful https enable

undo restful https enable

Default

RESTful access over HTTPS is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

For users to access the device through the HTTPS-based RESTful API, you must enable RESTful access over HTTPS.

Examples

Enable RESTful access over HTTPS.

```
<Switch> system-view
[Switch] restful https enable
```

NOTE:

The **restful https enable** command are only supported when used in combination with UNIVERGE Network Operation Engine Overlay Network Extension.

3.1.17. screen-length

Use **screen-length** to set the maximum number of lines of command output to send to the terminal at a time when the screen pausing feature is enabled.

Use **undo screen-length** to restore the default.

Syntax

screen-length *screen-length*

undo screen-length

Default

A maximum of 24 lines are sent.

Views

User line view

User line class view

Predefined user roles

network-admin

Parameters

screen-length: Specifies the maximum number of lines to send, in the range of 0 to 512. To send command output without pausing, set the number to 0 or execute the **screen-length disable** command.

Usage guidelines

The number of lines that can be displayed on the terminal screen is restricted by both this setting and the display specification of the terminal. For example, if this setting is 40, the device sends 40 lines to the terminal at a time. If the terminal display specification is 24 lines, only the last 24 lines are displayed on the terminal screen. To view the previous 16 lines, you must press **PgUp**.

To continue to display command output after a pause, press the space bar.

By default, pausing between screens of output is enabled.

This command is available in both user line view and user line class view. A non-default setting in either view takes precedence over a default setting in the other view. A non-default setting in user line view takes precedence over a non-default setting in user line class view.

The setting in user line view takes effect immediately for the current session. The setting in user line class view takes effect for login sessions that are established after the setting is configured.

Examples

Set the maximum number of lines to send at a time to 30 for VTY line 0.

```
<Switch> system-view
[Switch] line vty 0
[Switch-line-vty0] screen-length 30
```

Related commands

screen-length disable

3.1.18. send

Use **send** to send messages to online login users.

Syntax

send { **all** | *number1* | { **aux** | **vty** } *number2* }

Views

User view

Predefined user roles

network-admin

Parameters

all: Specifies all user lines.

number1: Specifies the absolute number of a user line. The value range is 0 to 83.

aux: Specifies the AUX line.

vty: Specifies the VTY line.

number2: Specifies the relative number of a user line. The value range is 0 to 9 for AUX line, and 0 to 63 for VTY lines.

Usage guidelines

You can use this command to send notifications to online users before performing an operation that might affect other online users, for example, before rebooting the device.

To end a message, press **Enter**. To abort the send operation, press **Ctrl+C**.

Examples

Send a notification to the user on VTY 1.

```
<Switch> send vty 1
Input message, end with Enter; abort with CTRL+C:
Your attention, please. I will reboot the system in 3 minutes.
Send message? [Y/N]:y
```

The message should appear on the user's terminal screen as follows:

```
[Switch]


***
***
***Message from vty0 to vty1
***
Your attention, please. I will reboot the system in 3 minutes.
```

3.1.19. set authentication password

Use **set authentication password** to set the password for local password authentication.

Use **undo set authentication password** to restore the default.

Syntax

set authentication password { **hash** | **simple** } *string*

undo set authentication password

Default

No password is set for local password authentication.

Views

User line view

User line class view

Predefined user roles

network-admin

Parameters

hash: Specifies a password in hashed form.

simple: Sets a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in hashed form.

string:

Before V7.2.18 and Version 7.2.23:

Specifies the password. Its plaintext form is a case-sensitive string of 1 to 16 characters. Its hashed form is a case-sensitive string of 1 to 110 characters.

After v7.3.21:

Specifies the password. Its plaintext form is a case-sensitive string of 4 to 16 characters and must contain two character types. Its hashed form is a case-sensitive string of 1 to 110 characters.

Usage guidelines

Only users assigned the network-admin, or level-15 user role can execute this command. Other users cannot execute this command, even if they are granted the right to execute this command.

This command is available in both user line view and user line class view. A non-default setting in either view takes precedence over a default setting in the other view. A non-default setting in user line view takes precedence over a non-default setting in user line class view.

A password change does not take effect for the current session. It takes effect for subsequent login sessions.

Examples

Set the password to **hello** for local password authentication on VTY line 0.

```
<Switch> system-view
[Switch] line vty 0
[Switch-line-vty0] authentication-mode password
[Switch-line-vty0] set authentication password simple hello
```

Related commands

authentication-mode

3.1.20. shell

Use **shell** to enable the terminal service for user lines.

Use **undo shell** to disable the terminal service for user lines.

Syntax

shell

undo shell

Default

The terminal service is enabled on all user lines.

Views

User line view

User line class view

Predefined user roles

network-admin

Usage guidelines

The **undo shell** command is not supported in AUX line view or AUX line class view.

You cannot disable the terminal service on the user line you are using.

When the device acts as a Telnet or SSH server, you cannot configure the **undo shell** command.

If the **undo shell** command is configured in user line class view, you cannot configure the **shell** command in the view of a user line in the class.

Examples

Disable the terminal service for VTY lines VTY 0 through 4 so no user can log in to the device through the user lines.

```
<Switch> system-view
[Switch] line vty 0 4
[Switch-line-vty0-4] undo shell
Disable ui-vty0-4 , are you sure? [Y/N]:y
[Switch-line-vty0-4]
```

3.1.21. speed

Use **speed** to set the transmission rate (also called the baud rate) on a user line.

Use **undo speed** to restore the default.

Syntax

speed *speed-value*

undo speed

Default

The transmission rate is 9600 bps on a user line.

Views

User line view

Predefined user roles

network-admin

Parameters

speed-value: Specifies the transmission rate in bps. Supported transmission rates depend on the network environment. The transmission rates for asynchronous serial interfaces might include:

- 300 bps.
- 600 bps.
- 1200 bps.
- 2400 bps.
- 4800 bps.
- 9600 bps.
- 19200 bps.
- 38400 bps.
- 57600 bps.
- 115200 bps.

Usage guidelines

This command is not supported in VTY line view.

The configuration terminal and the device must be configured with the same transmission rate to communicate.

Examples

Set the transmission rate to 19200 bps for AUX line 0.

```
<Switch> system-view
[Switch] line aux 0
[Switch-line-aux0] speed 19200
```

3.1.22. stopbits

Use **stopbits** to specify the number of stop bits for a character.

Use **undo stopbits** to restore the default.

Syntax

stopbits { **1** | **1.5** | **2** }

undo stopbits

Default

One stop bit is used.

Views

User line view

Predefined user roles

network-admin

Parameters

1: Uses one stop bit.

1.5: Uses one and a half stop bits. The device does not support using one and a half stop bits. If you specify this keyword, two stop bits are used.

2: Uses two stop bits.

Usage guidelines

This command is not supported in VTY line view.

The configuration terminal and the device must use the same number of stop bits to communicate.

Examples

Set the number of stop bits to 1 for AUX line 0.

```
<Switch> system-view
[Switch] line aux 0
[Switch-line-aux0] stopbits 1
```

3.1.23. telnet

Use **telnet** to Telnet to a host in an IPv4 network.

Syntax

telnet *remote-host* [*service-port*] [**vpn-instance** *vpn-instance-name*] [**source** { **interface** *interface-type interface-number* | **ip** *ip-address* } | **dscp** *dscp-value*] *

Views

User view

Predefined user roles

network-admin

Parameters

remote-host: Specifies the IPv4 address or host name of a remote host. A host name can be a case-insensitive string of 1 to 253 characters. Valid characters include letters, digits, hyphens (-), underscores (_), and dots (.).

service-port: Specifies the TCP port number for the Telnet service on the remote host. The value range is 0 to 65535 and the default is 23.

vpn-instance *vpn-instance-name*: Specifies the VPN instance to which the remote host belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. If the remote host belongs to the public network, do not specify this option.

source: Specifies a source IPv4 address or source interface for outgoing Telnet packets. If you do not specify this option, the device uses the primary IPv4 address of the output interface for the route to the server as the source address.

interface *interface-type interface-number*: Specifies the source interface. The primary IPv4 address of the interface will be used as the source IPv4 address for outgoing Telnet packets.

ip *ip-address*: Specifies the source IPv4 address for outgoing Telnet packets.

dscp *dscp-value*: Specifies a DSCP value for outgoing Telnet packets. The value range is 0 to 63. The default is 48.

Usage guidelines

To terminate the current Telnet connection, press **Ctrl+K** or execute the **quit** command.

The source address or interface specified by this command is applied only to the Telnet connection that is being established.

Examples

Telnet to host 1.1.1.2, using 1.1.1.1 as the source IP address for outgoing Telnet packets.

```
<Switch> telnet 1.1.1.2 source ip 1.1.1.1
```

Related commands

telnet client source

3.1.24. telnet client source

Use **telnet client source** to specify a source IPv4 address or source interface for the Telnet client to use for outgoing Telnet packets.

Use **undo telnet client source** to restore the default.

Syntax

telnet client source { **interface** *interface-type interface-number* | **ip** *ip-address* }

undo telnet client source

Default

No source IPv4 address or source interface is specified. The Telnet client uses the primary IPv4 address of the output interface for the route to the server as the source IPv4 address.

Views

System view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies a source interface. The primary IPv4 address of the interface will be used as the source IPv4 address for outgoing Telnet packets.

ip *ip-address*: Specifies a source IPv4 address.

Usage guidelines

The setting configured by this command applies to all Telnet connections but has a lower precedence than the source setting specified for the **telnet** command.

Examples

Set the source IPv4 address to 1.1.1.1 for outgoing Telnet packets.

```
<Switch> system-view
[Switch] telnet client source ip 1.1.1.1
```

Related commands

display telnet client configuration

3.1.25. telnet ipv6

Use **telnet ipv6** to Telnet to a host in an IPv6 network.

Syntax

telnet ipv6 *remote-host* [**-i** *interface-type interface-number*] [*port-number*] [**vpn-instance** *vpn-instance-name*] [**dscp** *dscp-value*] *

Views

User view

Predefined user roles

network-admin

Parameters

remote-host: Specifies the IPv6 address or host name of a remote host. A host name can be a case-insensitive string of 1 to 253 characters. Valid characters include letters, digits, hyphens (-), underscores (_), and dots (.).

-i *interface-type interface-number*: Specifies the interface for sending Telnet packets. This option is required when the remote host address is a link-local address. When the server address is a global unicast address, you cannot specify this option.

port-number: Specifies the TCP port number for the Telnet service on the remote host. The value range is 0 to 65535 and the default is 23.

vpn-instance *vpn-instance-name*: Specifies the VPN instance to which the remote host belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. If the remote host belongs to the public network, do not specify this option.

dscp *dscp-value*: Specifies a DSCP value for outgoing Telnet packets. The value range is 0 to 63. The default is 48.

Usage guidelines

To terminate the current Telnet connection, press **Ctrl+K** or execute the **quit** command.

Examples

Telnet to the host at 5000::1.

```
<Switch> telnet ipv6 5000::1
```

3.1.26. telnet server acl

Use **telnet server acl** to apply an ACL to filter Telnet logins.

Use **undo telnet server acl** to restore the default.

Syntax

telnet server acl [**mac**] *acl-number*

undo telnet server acl

Default

No ACL is used to filter Telnet logins.

Views

System view

Predefined user roles

network-admin

Parameters

mac: Specifies a Layer 2 ACL. To specify an ACL of a different type, do not specify this keyword.

acl-number: Specifies an ACL by its number. If you specify the **mac** keyword, the value range of this argument is 4000 to 4999. If you do not specify the **mac** keyword, the value range of this argument is 2000 to 3999.

Usage guidelines

You can specify an ACL that does not exist for this command. However, this command takes effect only after you create the ACL and configure rules for the ACL. For more information about ACL, see *ACL and QoS Configuration Guide*.

If you execute this command multiple times, the most recent configuration takes effect.

This command does not take effect on existing Telnet connections.

Examples

Permit only the user at 1.1.1.1 to Telnet to the device.

```
<Switch> system-view
[Switch] acl basic 2001
```

```
[Switch-acl-ipv4-basic-2001] rule permit source 1.1.1.1 0
[Switch-acl-ipv4-basic-2001] quit
[Switch] telnet server acl 2001
```

3.1.27. telnet server dscp

Use **telnet server dscp** to specify the DSCP value for IPv4 to use for Telnet packets sent to a Telnet client.

Use **undo telnet server dscp** to restore the default.

Syntax

telnet server dscp *dscp-value*

undo telnet server dscp

Default

IPv4 uses the DSCP value 48 for Telnet packets sent to a Telnet client.

Views

System view

Predefined user roles

network-admin

Parameters

dscp-value: Specifies a DSCP value in the range of 0 to 63.

Usage guidelines

The DSCP value is carried in the ToS field of an IPv4 packet to indicate the packet transmission priority.

Examples

Set the DSCP value for IPv4 to use for outgoing Telnet packets to 30 on a Telnet server.

```
<Switch> system-view
[Switch] telnet server dscp 30
```

3.1.28. telnet server enable

Use **telnet server enable** to enable the Telnet server.

Use **undo telnet server enable** to disable the Telnet server.

Syntax

telnet server enable

undo telnet server enable

Default

The Telnet server is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Users can Telnet to the device only when the Telnet server is enabled.

Examples

Enable the Telnet server.

```
<Switch> system-view
[Switch] telnet server enable
```

3.1.29. telnet server ipv6 acl

Use **telnet server ipv6 acl** to apply an IPv6 ACL to filter IPv6 Telnet logins.

Use **undo telnet server ipv6 acl** to restore the default.

Syntax

telnet server ipv6 acl { **ipv6** | **mac** } *acl-number*

undo telnet server ipv6 acl

Default

No IPv6 ACL is used to filter IPv6 Telnet logins.

Views

System view

Predefined user roles

network-admin

Parameters

ipv6: Specifies an IPv6 ACL.

mac: Specifies a Layer 2 ACL. To specify an ACL of a different type, do not specify this keyword.

acl-number: Specifies an ACL by its number. If you specify the **ipv6** keyword, the value range of this argument is 2000 to 3999. If you specify the **mac** keyword, the value range of this argument is 4000 to 4999.

Usage guidelines

You can specify an ACL that does not exist for this command. However, this command takes effect only after you create the ACL and configure rules for the ACL. For more information about ACL, see *ACL and QoS Configuration Guide*.

If you execute this command multiple times, the most recent configuration takes effect.

This command does not take effect on existing Telnet connections.

Examples

Permit only the user at 2000::1 to Telnet to the device.

```
<Switch> system-view
[Switch] acl ipv6 basic 2001
[Switch-acl6-ipv6-basic-2001] rule permit source 2000::1 128
[Switch-acl6-ipv6-basic-2001] quit
[Switch] telnet server ipv6 acl ipv6 2001
```

3.1.30. telnet server ipv6 dscp

Use **telnet server ipv6 dscp** to specify the DSCP value for IPv6 to use for Telnet packets sent to a Telnet client.

Use **undo telnet server ipv6 dscp** to restore the default.

Syntax

telnet server ipv6 dscp *dscp-value*

undo telnet server ipv6 dscp

Default

IPv6 uses the DSCP value 48 for Telnet packets sent to a Telnet client.

Views

System view

Predefined user roles

network-admin

Parameters

dscp-value: Specifies a DSCP value in the range of 0 to 63.

Usage guidelines

The DSCP value is carried in the Traffic class field of an IPv6 packet to indicate the packet transmission priority.

Examples

Set the DSCP value for IPv6 to use for outgoing Telnet packets to 30 on a Telnet server.

```
<Switch> system-view
[Switch] telnet server ipv6 dscp 30
```

3.1.31. terminal type

Use **terminal type** to specify the terminal display type.

Use **undo terminal type** to restore the default.

Syntax

terminal type { **ansi** | **vt100** }

undo terminal type

Default

The terminal display type is ANSI.

Views

User line view

User line class view

Predefined user roles

network-admin

Parameters

ansi: Specifies the ANSI type.

vt100: Specifies the VT100 type.

Usage guidelines

The device supports two terminal display types: ANSI and VT100. As a best practice, specify the VT100 type on both the device and the configuration terminal. If either side uses the ANSI type, a display problem might occur when a command line has more than 80 characters. For example, a cursor positioning error might occur.

This command is available in both user line view and user line class view. A non-default setting in either view takes precedence over a default setting in the other view. A non-default setting in user line view takes precedence over a non-default setting in user line class view.

A terminal display type change does not take effect for the current session. It takes effect for subsequent login sessions.

Examples

Set the terminal display type to VT100.

```
<Switch> system-view
[Switch] line vty 0
[Switch-line-vty0] terminal type vt100
```

3.1.32. user-role

Use **user-role** to assign a user role to a user line. The device assigns the user role to a user of the line when the user logs in.

Use **undo user-role** to remove a user role or restore the default.

Syntax

user-role *role-name*

undo user-role [*role-name*]

Default

A console user is assigned the network-admin user role. Other users are assigned the network-operator user role.

Views

User line view

User line class view

Predefined user roles

network-admin

Parameters

role-name: Specifies a user role name, a case-sensitive string of 1 to 63 characters. The user role can be user-defined or predefined. Available predefined user roles include network-admin, network-operator, and level-0 to level-15. The predefined security-audit and guest-manager user roles are not supported in user line view or user line class view. If you do not specify this argument, the **undo user-role** command restores the default user role.

Usage guidelines

Only users assigned the network-admin, or level-15 user role can execute this command. Other users cannot execute this command, even if they are granted the right to execute this command.

This command is available in both user line view and user line class view. A non-default setting in either view takes precedence over a default setting in the other view. A non-default setting in user line view takes precedence over a non-default setting in user line class view.

A user role change does not take effect for the current session. It takes effect for subsequent login sessions.

You can assign up to 64 user roles to a user line.

For more information about user roles, see *Fundamentals Configuration Guide*.

Examples

Assign user role network-admin to AUX line 0.

```
<Switch> system-view
[Switch] line aux 0
[Switch-line-aux0] user-role network-admin
```

Contents

A page of this section is **1-x-x**

4. FTP commands ····· 4-1
4.1. FTP server commands ····· 4-1
4.1.1. display ftp-server ····· 4-1
4.1.2. display ftp-user ····· 4-1
4.1.3. free ftp user ····· 4-2
4.1.4. free ftp user-ip ····· 4-3
4.1.5. free ftp user-ip ipv6 ····· 4-3
4.1.6. ftp server acl ····· 4-4
4.1.7. ftp server dscp ····· 4-4
4.1.8. ftp server enable ····· 4-5
4.1.9. ftp server ipv6 dscp ····· 4-5
4.1.10. ftp timeout ····· 4-6
4.2. FTP client commands ····· 4-7
4.2.1. ? ····· 4-7
4.2.2. ascii ····· 4-8
4.2.3. binary ····· 4-8
4.2.4. bye ····· 4-9
4.2.5. cd ····· 4-9
4.2.6. cdup ····· 4-10
4.2.7. close ····· 4-11
4.2.8. debug ····· 4-11
4.2.9. delete ····· 4-12
4.2.10. dir ····· 4-12
4.2.11. disconnect ····· 4-14
4.2.12. display ftp client source ····· 4-14
4.2.13. ftp ····· 4-14
4.2.14. ftp client ipv6 source ····· 4-16
4.2.15. ftp client source ····· 4-17
4.2.16. ftp ipv6 ····· 4-18
4.2.17. get ····· 4-19
4.2.18. help ····· 4-20
4.2.19. lcd ····· 4-21
4.2.20. ls ····· 4-21
4.2.21. mkdir ····· 4-23
4.2.22. newer ····· 4-23
4.2.23. open ····· 4-24
4.2.24. passive ····· 4-24
4.2.25. put ····· 4-25
4.2.26. pwd ····· 4-26
4.2.27. quit ····· 4-27
4.2.28. rhelp ····· 4-27
4.2.29. rmdir ····· 4-29
4.2.30. user ····· 4-29
4.2.31. verbose ····· 4-30

4. FTP commands

4.1. FTP server commands

4.1.1. display ftp-server

Use **display ftp-server** to display FTP server configuration and status information.

Syntax

display ftp-server

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display FTP server configuration and status information.

```
<Switch> display ftp-server
FTP server is running.
User count:                          1
Idle-timeout timer (in minutes):  30
```

Table 4-1 Command output

Field	Description
User count	Number of the current logged-in users.
Idle-timeout timer (in minutes)	If no packet is exchanged between the FTP server and client during this period, the FTP connection is closed.

Related commands

ftp server enable

ftp timeout

4.1.2. display ftp-user

Use **display ftp-user** to display detailed information about online FTP users.

Syntax

display ftp-user

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display detailed information about online FTP users.

```
<Switch> display ftp-user
UserName      HostIP             Port     HomeDir
root          192.168.20.184     46539    flash:
```

A field value is wrapped if its length exceeds the limit. The segments are left justified.

The following are the length limits for fields:

- **UserName**—10 characters.
- **HostIP**—15 characters.
- **HomeDir**—37 characters.

```
<Switch> display ftp-user
UserName      HostIP             Port     HomeDir
user2         2000:2000:2000:    1499     flash:/user2
              2000:2000:2000:
              2000:2000
administra    100.100.100.100    10001    flash:/123456789/123456789/123456789/
tor                                       123456789/123456789/123456789/1234567
                                          89/123456789
```

Table 4-2 Command output

Field	Description
UserName	Name of the user.
HostIP	IP address of the user.
Port	Port number of the user.
HomeDir	Authorized directory for the user.

4.1.3. free ftp user

Use **free ftp user** to manually release the FTP connections established by using a specific user account.

Syntax

free ftp user *username*

Views

User view

Predefined user roles

network-admin

Parameters

username: Specifies a username. To display online FTP users, execute the **display ftp-user** command.

Examples

Release the FTP connections established by using user account **ftpuser**.

```
<Switch> free ftp user ftpuser
Are you sure to free FTP connection? [Y/N]:y
<Switch>
```

4.1.4. free ftp user-ip

Use **free ftp user-ip** to manually release the FTP connections established from a specific IPv4 address.

Syntax

free ftp user-ip *ip-address* [**port** *port*]

Views

User view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the source IP address of an FTP connection. To view the source IP addresses of FTP connections, execute the **display ftp-user** command.

port *port*: Specifies the source port of an FTP connection. To view the source ports of FTP connections, execute the **display ftp-user** command.

Examples

Release the FTP connections established from the IP address 192.168.20.184.

```
<Switch> free ftp user-ip 192.168.20.184
Are you sure to free FTP connection? [Y/N]:y
<Switch>
```

4.1.5. free ftp user-ip ipv6

Use **free ftp user-ip ipv6 to** manually release the FTP connections established from a specific IPv6 address.

Syntax

free ftp user-ip ipv6 *ipv6-address* [**port** *port*]

Views

User view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies the source IPv6 address of an FTP connection. To view the source IPv6 addresses of FTP connections, execute the **display ftp-user** command.

port *port*: Specifies the source port of an FTP connection. To view the source ports of FTP connections, execute the **display ftp-user** command.

Examples

Release the FTP connections established from IPv6 address 2000::154.

```
<Switch> free ftp user-ip ipv6 2000::154
Are you sure to free FTP connection? [Y/N]:y
<Switch>
```

4.1.6. ftp server acl

Use **ftp server acl** to use an ACL to control FTP clients' access to the FTP server.

Use **undo ftp server acl** to restore the default.

Syntax

ftp server acl { *advanced-acl-number* | *basic-acl-number* | **ipv6** { *advanced-acl-number* | *basic-acl-number* } }

undo ftp server acl [**ipv6**]

Default

No ACL is used to control FTP clients' access to the FTP server.

Views

System view

Predefined user roles

network-admin

Parameters

advanced-acl-number: Specifies an advanced IPv4 ACL number in the range of 3000 to 3999.

basic-acl-number: Specifies a basic IPv4 ACL number in the range of 2000 to 2999.

ipv6 *advanced-acl-number*: Specifies an advanced IPv6 ACL number in the range of 3000 to 3999.

ipv6 *basic-acl-number*: Specifies a basic IPv6 ACL number in the range of 2000 to 2999.

Usage guidelines

You can use this command to permit only FTP requests from specific FTP clients. This configuration takes effect only for FTP connections to be established. It does not impact existing FTP connections.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Use ACL 2001 to allow only client 1.1.1.1 to access the FTP server.

```
<Switch> system-view
[Switch] acl basic 2001
[Switch-acl-ipv4-basic-2001] rule 0 permit source 1.1.1.1 0
[Switch-acl-ipv4-basic-2001] rule 1 deny source any
[Switch-acl-ipv4-basic-2001] quit
[Switch] ftp server acl 2001
```

4.1.7. ftp server dscp

Use **ftp server dscp** to set the DSCP value for IPv4 to use for FTP packets sent to an FTP client.

Use **undo ftp server dscp** to restore the default.

Syntax

ftp server dscp *dscp-value*

undo ftp server dscp

Default

IPv4 uses the DSCP value 0 for FTP packets sent to an FTP client.

Views

System view

Predefined user roles

network-admin

Parameters

dscp-value: Specifies a DSCP value in the range of 0 to 63.

Usage guidelines

The DSCP value is carried in the ToS field of an IP packet to indicate the transmission priority of the packet.

Examples

Set the DSCP value for IPv4 to use for outgoing FTP packets to 30 on an FTP server.

```
<Switch> system-view
[Switch] ftp server dscp 30
```

4.1.8. ftp server enable

Use **ftp server enable** to enable the FTP server.

Use **undo ftp server enable** to disable the FTP server.

Syntax

ftp server enable

undo ftp server enable

Default

The FTP server is disabled.

Views

System view

Predefined user roles

network-admin

Examples

Enable the FTP server.

```
<Switch> system-view
[Switch] ftp server enable
```

4.1.9. ftp server ipv6 dscp

Use **ftp server ipv6 dscp** to set the DSCP value for IPv6 to use for FTP packets sent to an FTP client.

Use **undo ftp server ipv6 dscp** to restore the default.

Syntax

ftp server ipv6 dscp *dscp-value*

undo ftp server ipv6 dscp

Default

IPv6 uses the DSCP value 0 for FTP packets sent to an FTP client.

Views

System view

Predefined user roles

network-admin

Parameters

dscp-value: Specifies a DSCP value in the range of 0 to 63.

Usage guidelines

The DSCP value is carried in the Traffic class field of an IPv6 packet to indicate the transmission priority of the packet.

Examples

Set the DSCP value for IPv6 to use for outgoing FTP packets to 30 on an FTP server.

```
<Switch> system-view
[Switch] ftp server ipv6 dscp 30
```

4.1.10. ftp timeout

Use **ftp timeout** to set the FTP connection idle-timeout timer.

Use **undo ftp timeout** to restore the default.

Syntax

ftp timeout *minute*

undo ftp timeout

Default

The FTP connection idle-timeout timer is 30 minutes.

Views

System view

Predefined user roles

network-admin

Parameters

minute: Specifies a time interval in the range of 1 to 35791 minutes.

Usage guidelines

If no data transfer occurs on an FTP connection within the idle-timeout interval, the FTP server closes the FTP connection to release resources.

Examples

Set the FTP connection idle-timeout timer to 36 minutes.

```
<Switch> system-view
[Switch] ftp timeout 36
```

4.2. FTP client commands

For FTP users to execute FTP client configuration commands, you must configure authorization settings for users on the FTP server. Authorized operations include viewing the files in the working directory, reading/downloading/uploading/renaming/removing files, and creating directories.

The FTP client commands in this section are supported by the device, but whether they can be executed successfully depends on the FTP server.

The output in the examples of this section varies by FTP server type.

4.2.1. ?

Use **?** to display all commands supported by an FTP client.

Use **?** *command-name* to display the help information for a command.

Syntax

? [*command-name*]

Views

FTP client view

Predefined user roles

network-admin

Parameters

command-name: Specifies a command supported by the FTP client.

Usage guidelines

In FTP client view, entering **?** is the same as executing the **help** command.

Examples

Display all commands supported by the FTP client.

```
ftp> ?
Commands may be abbreviated.  Commands are:

append          delete          ls              quit            rmdir
ascii           debug           mkdir           reget           status
binary          dir             newer           rstatus         system
bye             disconnect      open            rhelp           user
cd              get             passive         rename          verbose
cdup            help            put             reset           ?
close           lcd             pwd             restart
```

Display the help information for the **dir** command.

```
ftp> ? dir
dir              list contents of remote directory
```

Related commands

help

4.2.2. ascii

Use **ascii** to set the file transfer mode to ASCII.

Syntax

ascii

Default

The file transfer mode is binary.

Views

FTP client view

Predefined user roles

network-admin

Usage guidelines

You can perform this operation only after you log in to the FTP server.

FTP transfers files in either of the following modes:

- **Binary mode**—Transfers non-text files.
- **ASCII mode**—Transfers text files.

When the device acts as the FTP server, the transfer mode is determined by the FTP client. When the device acts as the FTP client, you can set the transfer mode. The transfer mode is binary by default.

Examples

Set the file transfer mode to ASCII.

```
ftp> ascii
200 TYPE is now ASCII
```

Related commands

binary

4.2.3. binary

Use **binary** to set the file transfer mode to binary, which is also called the flow mode.

Syntax

binary

Default

The file transfer mode is binary.

Views

FTP client view

Predefined user roles

network-admin

Usage guidelines

You can perform this operation only after you log in to the FTP server.

FTP transfers files in either of the following modes:

- **Binary mode**—Transfers program file or pictures.
- **ASCII mode**—Transfers text files.

When the device acts as the FTP server, the transfer mode is determined by the FTP client. When the device acts as the FTP client, you can set the transfer mode. The default transfer mode is binary.

Examples

Set the file transfer mode to binary.

```
ftp> binary
200 TYPE is now 8-bit binary
```

Related commands

ascii

4.2.4. bye

Use **bye** to terminate the connection to the FTP server and return to user view. If no connection is established between the device and the FTP server, use this command to return to user view.

Syntax

bye

Views

FTP client view

Predefined user roles

network-admin

Examples

Terminate the connection to the FTP server and return to user view.

```
ftp> bye
221-Goodbye. You uploaded 2 and downloaded 2 kbytes.
221 Logout.
<Switch>
```

Related commands

quit

4.2.5. cd

Use **cd** to change the current working directory to another directory on the FTP server.

Syntax

cd { *directory* | **..** | **/** }

Views

FTP client view

Predefined user roles

network-admin

Parameters

directory: Specifies the target directory. If the target directory does not exist, the **cd** command does not change the current working directory.

..: Specifies the upper directory. Executing the **cd ..** command is the same as executing the **cdup** command. If the current working directory is the FTP root directory, the **cd ..** command does not change the current working directory.

/: Specifies the FTP root directory.

Usage guidelines

You can perform this operation only after you log in to the FTP server.

The directory that can be accessed must be authorized by the FTP server.

Examples

Change the working directory to the **logfile** subdirectory of the current directory.

```
ftp> cd logfile
250 OK. Current directory is /logfile
```

Change the working directory to the **folder** subdirectory of the FTP root directory.

```
ftp> cd /folder
250 OK. Current directory is /folder
```

Change the working directory to the upper directory of the current directory.

```
ftp> cd ..
250 OK. Current directory is /
```

Change the working directory to the FTP root directory.

```
ftp> cd /
250 OK. Current directory is /
```

Related commands

cdup

pwd

4.2.6. cdup

Use **cdup** to enter the upper directory of the FTP server.

Syntax

cdup

Views

FTP client view

Predefined user roles

network-admin

Usage guidelines

You can perform this operation only after you log in to the FTP server.

This command does not change the working directory if the current directory is the FTP root directory.

Examples

Change the working directory to the upper directory.

```
ftp> pwd
257 "/ftp/subdir" is your current location
ftp> cdup
250 OK. Current directory is /ftp
ftp> pwd
257 "/ftp" is your current location
```

Related commands

cd

pwd

4.2.7. close

Use **close** to terminate the connection to the FTP server without exiting FTP client view.

Syntax

close

Views

FTP client view

Predefined user roles

network-admin

Usage guidelines

You can perform this operation only after you log in to the FTP server.

Examples

Terminate the connection to the FTP server without exiting the FTP client view.

```
ftp> close
221-Goodbye. You uploaded 0 and downloaded 0 kbytes.
221 Logout.
ftp>
```

Related commands

disconnect

4.2.8. debug

Use **debug** to enable or disable FTP client debugging.

Syntax

debug

Default

FTP client debugging is disabled.

Views

FTP client view

Predefined user roles

network-admin

Usage guidelines

When FTP client debugging is enabled, executing this command disables FTP client debugging.

When FTP client debugging is disabled, executing this command enables FTP client debugging.

Examples

Enable and then disable FTP client debugging.

```
ftp> debug
Debugging on (debug=1).
ftp> debug
Debugging off (debug=0).
```

4.2.9. delete

Use **delete** to permanently delete a file from the FTP server.

Syntax

delete *remotefile*

Views

FTP client view

Predefined user roles

network-admin

Parameters

remotefile: Specifies a file on the FTP server.

Usage guidelines

You can perform this operation only after you log in to the FTP server.

To perform this operation, you must have delete permission on the FTP server.

Examples

Delete the **b.txt** file.

```
ftp> delete b.txt
250 Deleted b.txt
```

4.2.10. dir

Use **dir** to display or save detailed information about files and directories on the FTP server.

Syntax

dir [*remotefile* [*localfile*]]

Views

FTP client view

Predefined user roles

network-admin

Parameters

remotefile: Specifies a file or directory on the FTP server.

localfile: Specifies the name of the local file used to save the displayed information.

Usage guidelines

You can perform this operation only after you log in to the FTP server.

To display detailed information about the files and subdirectories in the working directory on the FTP server, use the **dir** command.

To display detailed information about a file or directory on the FTP server, use the **dir** *remotefile* command.

To save detailed information about a file or directory on the FTP server to a local file, use the **dir** *remotefile localfile* command.

In FTP client view, executing the **dir** command is the same as executing the **ls** command.

Examples

Display detailed information about the files and subdirectories in the working directory on the FTP server.

```
ftp> dir
150 Connecting to port 50201
-rwxr-xr-x    1 0          0               1481 Jul  7 15:36 a.txt
drwxr-xr-x    2 0          0               8192 Jul  2 14:33 diagfile
drwxr-xr-x    3 0          0               8192 Jul  7 15:21 ftp
drwxr-xr-x    2 0          0               8192 Jul  5 09:15 logfile
drwxr-xr-x    2 0          0               8192 Jul  2 14:33 seclog
-rwxr-xr-x    1 0          0           40808448 Jul  2 14:33 system-a1801.bin
-rwxr-xr-x    1 0          0               3050 Jul  7 12:26 startup.cfg
-rwxr-xr-x    1 0          0              54674 Jul  4 09:24 startup.mdb
-rwxr-xr-x    1 0          0               1481 Jul  7 12:34 x.cfg
226 9 matches total
```

Save detailed information about file **a.txt** to **s.txt**.

```
ftp> dir a.txt s.txt
output to local-file: s.txt ? [Y/N]y
150 Connecting to port 50203
226-Glob: a.txt
```

Display the content of the file **s.txt**.

```
ftp> bye
221-Goodbye. You uploaded 0 and downloaded 2 kbytes.
221 Logout.
<Switch> more s.txt
-rwxr-xr-x    1 0          0               1481 Jul  7 12:34 a.txt
```

Related commands

ls

4.2.11. disconnect

Use **disconnect** to terminate the connection to the FTP server without exiting FTP client view.

Syntax

disconnect

Views

FTP client view

Predefined user roles

network-admin

Usage guidelines

You can perform this operation only after you log in to the FTP server.

Examples

Terminate the connection to the FTP server without exiting the FTP client view.

```
ftp> disconnect
221-Goodbye. You uploaded 0 and downloaded 0 kbytes.
221 Logout.
ftp>
```

Related commands

close

4.2.12. display ftp client source

Use **display ftp client source** to display the source address settings on the FTP client.

Syntax

display ftp client source

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display the source address settings on the FTP client.

```
<Switch> display ftp client source
The source IP address of the FTP client is 1.1.1.1.
```

4.2.13. ftp

Use **ftp** to log in to an IPv4 FTP server and enter FTP client view.

Syntax

ftp [*ftp-server* [*service-port*] [**vpn-instance** *vpn-instance-name*] [**dscp** *dscp-value* | **source** { **interface** *interface-type interface-number* | **ip** *source-ip-address* }] *]

Views

User view

Predefined user roles

network-admin

Parameters

ftp-server: Specifies the IPv4 address or host name of an FTP server. A host name can be a case-insensitive string of 1 to 253 characters. Valid characters for a host name include letters, digits, hyphens (-), underscores (_), and dots (.).

service-port: Specifies the TCP port number of the FTP server, in the range of 0 to 65535. The default is 21.

vpn-instance *vpn-instance-name*: Specifies the VPN instance to which the FTP server belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. If the FTP server belongs to the public network, do not specify this option.

dscp *dscp-value*: Specifies the DSCP value for IPv4 to use in outgoing FTP packets to indicate the packet transmission priority. The value range is 0 to 63. The default is 0.

source { **interface** *interface-type interface-number* | **ip** *source-ip-address* }: Specifies the source address used to establish the FTP connection.

- **interface** *interface-type interface-number*: Specifies an interface by its type and number. The device will use the interface's primary IPv4 address as the source address. To establish the FTP connection successfully, make sure the interface is up and has the primary IPv4 address configured.
- **ip** *source-ip-address*: Specifies an IPv4 address. To establish the FTP connection successfully, make sure this address is the IPv4 address of an interface in up state on the device.

Usage guidelines

This command is only applicable to IPv4 networks.

If no parameters are specified, this command enters the FTP client view without logging in to an FTP server.

If the server parameters are specified, you are prompted to enter the username and password for logging in to the FTP server.

Examples

Log in to FTP server 192.168.0.211. Use 192.168.0.212 as the source IPv4 address for outgoing FTP packets.

```
<Switch>ftp 192.168.0.211 source ip 192.168.0.212
Press CTRL+C to abort.
Connected to 192.168.0.211 (192.168.0.211).
220 WFTPD 2.0 service (by Texas Imperial Software) ready for new user
User (192.168.0.211:(none)): abc
331 Give me your password, please
Password:
```

```
230 Logged in successfully
Remote system type is MSDOS.
ftp>
```

Log in to FTP server 192.168.0.211 and enable FTP client debugging.

```
<Switch> ftp 192.168.0.211 -d
Press CTRL+C to abort.
Connected to 192.168.0.211 (192.168.0.211).
220 FTP service ready.
User (192.168.0.211:(none)): abc
*Apr 10 09:02:24:139 2017 Switch FTPC/7/EVENT: PAM initialization result: 0.
*Apr 10 09:02:24:150 2017 Switch FTPC/7/EVENT: PAM: Sent a start-accounting request. Result:
0.
*Apr 10 09:02:24:860 2017 Switch FTPC/7/COMMAND: USER abc
331 Password required for abc.
Password:
*Apr 10 09:02:25:575 2017 Switch FTPC/7/COMMAND: PASS XXXX
230 User logged in.
215 UNIX Type: L8
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> *Apr 10 09:02:25:640 2017 SIMWARE FTPC/7/COMMAND: SYST
ftp>
```

4.2.14. ftp client ipv6 source

Use **ftp client ipv6 source** to specify the source IPv6 address for FTP packets sent to an IPv6 FTP server.

Use **undo ftp client ipv6 source** to restore the default.

Syntax

ftp client ipv6 source { **interface** *interface-type interface-number* | **ipv6** *source-ipv6-address* }

undo ftp client ipv6 source

Default

No source address is specified for FTP packets sent to an IPv6 FTP server. The device selects a source IPv6 address as defined in RFC 3484.

Views

System view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. The device will use the interface's IPv6 address as the source address. For successful FTP packet transmission, make sure the interface is up and is configured with an IPv6 address.

ipv6 *source-ipv6-address*: Specifies an IPv6 address. For successful FTP packet transmission, make sure this address is the IPv6 address of an interface in up state on the device.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

The source address specified with the **ftp ipv6** command takes precedence over the source address specified with the **ftp client ipv6 source** command.

The source address specified with the **ftp client ipv6 source** command applies to all FTP connections. The source address specified with the **ftp ipv6** command applies only to the FTP connection that is being established.

Examples

Specify the source IPv6 address of 2000::1 for FTP packets sent to an IPv6 FTP server.

```
<Switch> system-view
[Switch] ftp client ipv6 source ipv6 2000::1
```

Related commands

ftp ipv6

4.2.15. ftp client source

Use **ftp client source** to specify the source IPv4 address for FTP packets sent to an IPv4 FTP server.

Use **undo ftp client source** to restore the default.

Syntax

ftp client source { **interface** *interface-type interface-number* | **ip** *source-ip-address* }

undo ftp client source

Default

No source IPv4 address is specified for FTP packets sent to an IPv4 FTP server. The device uses the primary IPv4 address of the output interface for the route to the server as the source address.

Views

System view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. The device will use the interface's primary IPv4 address as the source address. For successful FTP packet transmission, make sure the interface is up and has the primary IPv4 address configured.

ip *source-ip-address*: Specifies an IPv4 address. For successful FTP packet transmission, make sure this address is the IPv4 address of an interface in up state on the device.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

The source address specified with the **ftp** command takes precedence over the source address specified with the **ftp client source** command.

The source address specified with the **ftp client source** command applies to all FTP connections. The source address specified with the **ftp** command applies only to the FTP connection that is being established.

Examples

Specify the source IPv4 address of 192.168.20.222 for FTP packets sent to an IPv4 FTP server.

```
<Switch> system-view
[Switch] ftp client source ip 192.168.20.222
```

Related commands

ftp

4.2.16. ftp ipv6

Use **ftp ipv6** to log in to an IPv6 FTP server and enter FTP client view.

Syntax

ftp ipv6 [*ftp-server* [*service-port*] [**vpn-instance** *vpn-instance-name*] [**dscp** *dscp-value* | **source** { **ipv6** *source-ipv6-address* | **interface** *interface-type interface-number* }] * [**-i** *interface-type interface-number*]]

Views

User view

Predefined user roles

network-admin

Parameters

ftp-server: Specifies the IPv6 address or host name of an FTP server. A host name can be a case-insensitive string of 1 to 253 characters. Valid characters for a host name include letters, digits, hyphens (-), underscores (_), and dots (.).

service-port: Specifies the TCP port number of the FTP server, in the range of 0 to 65535. The default is 21.

dscp *dscp-value*: Specifies the DSCP value for IPv6 to use in outgoing FTP packets to indicate the packet transmission priority. The value range is 0 to 63. The default is 0.

source { **ipv6** *source-ipv6-address* | **interface** *interface-type interface-number* }: Specifies the source address used to establish the FTP connection.

- **interface** *interface-type interface-number*: Specifies an interface by its type and number. This option can be used only when the FTP server address is a link local address and the specified output interface has a link local address. For information about link local addresses, see *Layer 3—IP Services Configuration Guide*.
- **ipv6** *source-ipv6-address*: Specifies an IPv6 address. To establish the FTP connection successfully, make sure this address is the IPv6 address of an interface in up state on the device.

vpn-instance *vpn-instance-name*: Specifies the VPN instance to which the FTP server belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. If the FTP server belongs to the public network, do not specify this option.

-i *interface-type interface-number*: Specifies an output interface by its type and number. This option can be used only when the FTP server address is a link local address and the specified output interface has a link local address.

Usage guidelines

This command is only applicable to IPv6 networks.

If no parameters are specified, this command enters the FTP client view.

If the FTP server parameters are specified, you are prompted to enter the username and password for logging in to the FTP server.

Examples

Log in to FTP server 2000::154.

```
<Switch>ftp ipv6 2000::154
Press CTRL+C to abort.
Connected to 2000::154 (2000::154).
220 FTP service ready.
User (2000::154): root
331 Password required for root.
Password:
230 User logged in
Remote system type is NEC
```

4.2.17. get

Use **get** to download a file from the FTP server and save the file.

Syntax

get *remotefile* [*localfile*]

Views

FTP client view

Predefined user roles

network-admin

Parameters

remotefile: Specifies the file to be downloaded.

localfile: Specifies a name for the downloaded file. If you do not specify this argument, the system uses the name of the source file.

Usage guidelines

You can perform this operation only after you log in to the FTP server.

To save the downloaded file to the working directory accessed by the **ftp** command, perform one of the following tasks:

- Execute the command without specifying the *localfile* argument.
- Specify a file name without any path information for the *localfile* argument, for example, a.cfg.

To save the downloaded file to some other directory, you must specify a fully qualified file name for the *localfile* argument, for example, flash:/subdirectory/a.cfg.

Examples

Download the **a.txt** file and save it as **b.txt** in the working directory accessed by the **ftp** command.

```
ftp> get a.txt b.txt
local: b.txt remote: a.txt
150 Connecting to port 47457
226 File successfully transferred
1569 bytes received in 0.00527 seconds (290.6 kbyte/s)
```

Download the **a.txt** file to the **test** directory in the working directory accessed by the **ftp** command.

```
ftp> get a.txt flash:/test/b.txt
local: flash:/test/b.txt remote: a.txt
150 Connecting to port 47457
226 File successfully transferred
1569 bytes received in 0.00527 seconds (290.6 kbyte/s)
```

Download the **a.txt** file to the root directory of the flash memory on a member device. Save the file as **c.txt**.

```
ftp> get a.txt slot1#flash:/c.txt
local: slot1#flash:/c.txt remote: a.txt
150 Connecting to port 47460
226 File successfully transferred
1569 bytes received in 0.0564 seconds (27.2 kbyte/s)
```

Related commands

put

4.2.18. help

Use **help** to display all commands supported by the FTP client.

Use **help** *command-name* to display the help information for a command.

Syntax

help [*command-name*]

Views

FTP client view

Predefined user roles

network-admin

Parameters

command-name: Specifies a command supported by the FTP client.

Usage guidelines

In FTP client view, executing the **help** command is the same as entering **?**.

Examples

Display all commands supported by the FTP client.

```
ftp> help
```

```
append          delete          ls              quit            rmdir
ascii           debug           mkdir           reget           status
binary          dir             newer           rstatus         system
bye             disconnect      open            rhelp           user
cd              get             passive         rename          verbose
cdup            help            put             reset           ?
close           lcd             pwd             restart
```

Display the help information for the **dir** command.

```
ftp> help dir
dir              list contents of remote directory
```

Related commands

?

4.2.19. lcd

Use **lcd** to display or change the local working directory of the FTP client.

Syntax

lcd [*directory* | **/**]

Views

FTP client view

Predefined user roles

network-admin

Parameters

directory: Changes the local working directory of the FTP client to the specified local directory. There must be a slash sign (/) before the name of the storage medium, for example, /flash:/logfile.

/: Changes the local working directory of the FTP client to the local root directory.

Usage guidelines

To display the local working directory of the FTP client, do not specify the *directory* or **/** argument.

Examples

Display the local working directory.

```
ftp> lcd
Local directory now /flash:
```

Change the local working directory to **flash:/logfile**.

```
ftp> lcd /flash:/logfile
Local directory now /flash:/logfile
```

4.2.20. ls

Use **ls** to display or save detailed information about files and directories on the FTP server.

Syntax

ls [*remotefile* [*localfile*]]

Views

FTP client view

Predefined user roles

network-admin

Parameters

remotefile: Specifies a file or directory on the FTP server.

localfile: Specifies the name of the local file used to save the displayed information.

Usage guidelines

You can perform this operation only after you log in to the FTP server.

To display detailed information about the files and subdirectories in the working directory on the FTP server, use the **ls** command.

To display detailed information about a file or directory on the FTP server, use the **ls** *remotefile* command.

To save detailed information about a file or directory on the FTP server to a local file, use the **ls** *remotefile localfile* command.

In FTP client view, executing the **ls** command is the same as executing the **dir** command.

Examples

Display detailed information about the files and subdirectories in the working directory on the FTP server.

```
ftp> ls
150 Connecting to port 50201
-rwxr-xr-x    1 0          0               1481 Jul  7 15:36 a.txt
drwxr-xr-x    2 0          0               8192 Jul  2 14:33 diagfile
drwxr-xr-x    3 0          0               8192 Jul  7 15:21 ftp
drwxr-xr-x    2 0          0               8192 Jul  5 09:15 logfile
drwxr-xr-x    2 0          0               8192 Jul  2 14:33 seclog
-rwxr-xr-x    1 0          0           40808448 Jul  2 14:33 system-a1801.bin
-rwxr-xr-x    1 0          0               3050 Jul  7 12:26 startup.cfg
-rwxr-xr-x    1 0          0              54674 Jul  4 09:24 startup.mdb
-rwxr-xr-x    1 0          0               1481 Jul  7 12:34 x.cfg
226 9 matches total
```

Save detailed information about the file **a.txt** to **s.txt**.

```
ftp> ls a.txt s.txt
output to local-file: s.txt ? [Y/N]y
150 Connecting to port 50203
226-Glob: s.txt
```

Display the content of the file **s.txt**.

```
ftp> bye
221-Goodbye. You uploaded 0 and downloaded 2 kbytes.
221 Logout.
<Switch> more s.txt
-rwxr-xr-x    1 0          0               1481 Jul  7 12:34 a.txt
```

Related commands

dir

4.2.21. mkdir

Use **mkdir** to create a subdirectory in the current directory on the FTP server.

Syntax

mkdir *directory*

Views

FTP client view

Predefined user roles

network-admin

Parameters

directory: Specifies the name for the directory to be created.

Usage guidelines

You can perform this operation only after you log in to the FTP server.

You must have permission to perform this operation on the FTP server.

Examples

Create a subdirectory named **newdir** in the current directory of the FTP server.

```
ftp> mkdir newdir
257 "newdir" : The directory was successfully created
```

4.2.22. newer

Use **newer** to update a local file by using a file on the FTP server.

Syntax

newer *remotefile* [*localfile*]

Views

FTP client view

Predefined user roles

network-admin

Parameters

remotefile: Specifies a file on the FTP server.

localfile: Specifies the local file to be updated.

Usage guidelines

You can perform this operation only after you log in to the FTP server.

If the local file does not exist, this command downloads the file from the FTP server and saves it locally.

If the file on the FTP server is not newer than the local file, this command does not update the local file.

Examples

Update the local file with the **a.txt** file on the FTP server.

```
ftp> newer a.txt
local: a.txt remote: a.txt
150 Connecting to port 63513
226 File successfully transferred
1573 bytes received in 0.0293 seconds (52.3 kbyte/s)
```

4.2.23. open

Use **open** to log in to an FTP server from FTP client view.

Syntax

open *server-address* [*service-port*]

Views

FTP client view

Predefined user roles

network-admin

Parameters

server-address: Specifies the IPv4 address, IPv6 address, or host name of the FTP server.

service-port: Specifies the TCP port number of the FTP server, in the range of 0 to 65535. The default is 21.

Usage guidelines

After you issue this command, the system will prompt you to enter the username and password.

After you log in to one FTP server, you must disconnect from the server before you can use the **open** command to log in to another server.

Examples

In FTP client view, log in to FTP server 192.168.40.7.

```
<Switch>ftp
ftp> open 192.168.40.7
Press CTRL+C to abort.
Connected to 192.168.40.7 (192.168.40.7).
220 FTP service ready.
User (192.168.40.7:(none)): root
331 Password required for root.
Password:
230 User logged in.
Remote system type is NEC.
ftp>
```

4.2.24. passive

Use **passive** to change the FTP operation mode.

Syntax

passive

Default

The FTP operation mode is passive.

Views

FTP client view

Predefined user roles

network-admin

Usage guidelines

FTP can operate in either of the following modes:

- **Active mode**—The FTP server initiates the TCP connection.
- **Passive mode**—The FTP client initiates the TCP connection.

When the FTP operation mode is passive, executing this command changes the mode to active.

When the FTP operation mode is active, executing this command changes the mode to passive.

This command is typically used together with a firewall to control FTP session establishment between private network users and public network users.

Examples

Change the FTP operation mode to passive.

```
ftp> passive
Passive mode on.
ftp> passive
Passive mode off.
```

4.2.25. put

Use **put** to upload a file from the FTP client to the FTP server.

Syntax

put *localfile* [*remotefile*]

Views

FTP client view

Predefined user roles

network-admin

Parameters

localfile: Specifies the local file to be uploaded.

remotefile: Specifies the name of the file for saving the uploaded file on the FTP server.

Usage guidelines

You can perform this operation only after you log in to the FTP server.

To upload a file in the current working directory, specify a file name without the path for the *localfile* argument, for example, a.cfg.

To upload a file in some other directory, specify a fully qualified file name for the *localfile* argument, for example, flash:/subdirectory/a.cfg.

Examples

Upload the **a.txt** file from the local working directory to the FTP server. Save the file as **b.txt**.

```
ftp> put a.txt b.txt
local: a.txt remote: b.txt
150 Connecting to port 47461
226 File successfully transferred
1569 bytes sent in 0.000671 seconds (2.23 Mbyte/s)
```

Upload the **a.txt** file from the **test** directory of the local working directory to the FTP server. Save the file as **b.txt**.

```
ftp> put flash:/test/a.txt b.txt
local: flash:/test/a.txt remote: b.txt
150 Connecting to port 47461
226 File successfully transferred
1569 bytes sent in 0.000671 seconds (2.23 Mbyte/s)
```

Upload file **a.txt** from the **test** directory of the storage medium on a member device. Save the file as **b.txt** on the FTP server.

```
ftp> put slot2#flash:/test/a.txt b.txt
local: slot2#flash:/test/a.txt remote: b.txt
150 Connecting to port 47461
226 File successfully transferred
1569 bytes sent in 0.000671 seconds (2.23 Mbyte/s)
```

Related commands

get

4.2.26. pwd

Use **pwd** to display the currently accessed directory on the FTP server.

Syntax

pwd

Views

FTP client view

Predefined user roles

network-admin

Usage guidelines

You can perform this operation only after you log in to the FTP server.

Examples

Display the currently accessed directory on the FTP server.

```
ftp> cd subdir
250 OK. Current directory is /subdir
ftp> pwd
257 "/subdir" is your current location
```

4.2.27. quit

Use **quit** to terminate the connection to the FTP server and return to user view.

Syntax

quit

Views

FTP client view

Predefined user roles

network-admin

Examples

Terminate the connection to the FTP server and return to user view.

```
ftp> quit
221-Goodbye. You uploaded 0 and downloaded 0 kbytes.
221 Logout.
<Switch>
```

Related commands

bye

4.2.28. rhelp

Use **rhelp** to display the FTP commands supported by the FTP server.

Use **rhelp** *protocol-command* to display the help information for an FTP command supported by the FTP server.

Syntax

rhelp [*protocol-command*]

Views

FTP client view

Predefined user roles

network-admin

Parameters

protocol-command: Specifies an FTP command.

Usage guidelines

You can perform this operation only after you log in to the FTP server.

Examples

Display the FTP-related commands supported by the FTP server.

```
ftp> rhelp
214-The following FTP commands are recognized
 USER PASS NOOP QUIT SYST TYPE
 HELP CWD  XCWD PWD  CDUP XCUP
 XPWD LIST NLST MLSD PORT EPRT
 PASV EPSV REST RETR STOR APPE
```

```
 DELE MKD  XMKD RMD  XRMD ABOR
 SIZE RNFR RNTO
214 UNIX Type: L8
```

Table 4-3 Command output

Field	Description
USER	Username.
PASS	Password.
NOOP	Null operation.
SYST	System parameters.
TYPE	Request type.
CWD	Changes the current working directory.
XCWD	Extended command with the meaning of CWD.
PWD	Prints the working directory.
CDUP	Changes the directory to the upper directory.
XCUP	Extended command with the meaning of CDUP.
XPWD	Extended command with the meaning of PWD.
LIST	Lists files.
NLST	Lists brief file description.
MLSD	Lists file content.
PORT	Active mode (IPv4).
EPRT	Active mode (IPv6).
PASV	Passive mode (IPv4).
EPSV	Passive mode (IPv6).
REST	Restarts.
RETR	Downloads files.
STOR	Uploads files.
APPE	Appends uploading.
DELE	Deletes files.
MKD	Creates folders.
XMKD	Extended command with the meaning of MKD.
RMD	Deletes folders.
XRMD	Extended command with the meaning of RMD.
ABOR	Aborts the transmission.
SIZE	Size of the transmission file.
RNFR	Original name.
RNTO	New name.

4.2.29. rmdir

Use **rmdir** to permanently delete a directory from the FTP server.

Syntax

rmdir *directory*

Views

FTP client view

Predefined user roles

network-admin

Parameters

directory: Specifies a directory on the FTP server.

Usage guidelines

You can perform this operation only after you log in to the FTP server.

To perform this operation, you must have delete permission on the FTP server.

Delete all files and subdirectories in a directory before you delete the directory. For more information about how to delete files, see the **delete** command.

The **rmdir** command does not delete the files of the specified directory from the recycle bin.

Examples

Delete empty directory **subdir1**.

```
ftp>rmdir subdir1
250 The directory was successfully removed
```

Related commands

delete

4.2.30. user

Use **user** to initiate an FTP authentication on the current FTP connection.

Syntax

user *username* [*password*]

Views

FTP client view

Predefined user roles

network-admin

Parameters

username: Specifies the username.

password: Specifies the password.

Usage guidelines

If you tried to access an FTP server but failed to pass the authentication, you can use this command to try again before the connection to the FTP server expires.

After you log in to an FTP server, you can initiate an FTP authentication to change to a new account. By changing to a new account, you can get a different privilege without re-establishing the FTP connection.

Make sure the specified username and password have been configured on the FTP server. If the username or password is not configured, this command fails and the FTP connection is closed.

Examples

After logging in to the FTP server, use username **ftp** and password **123456** to log in again to the FTP server.

- Method 1:

```
ftp> user ftp 123456
331 Password required for ftp.
230 User logged in.
```

- Method 2:

```
ftp> user ftp
331 Password required for ftp.
Password:
230 User logged in.
```

4.2.31. verbose

Use **verbose** to enable or disable the device to display detailed information about FTP operations.

Syntax

verbose

Default

The device displays detailed information about FTP operations.

Views

FTP client view

Predefined user roles

network-admin

Usage guidelines

This command affects only the current FTP session.

Examples

Disable the device from displaying detailed information about FTP operations.

```
ftp> verbose
Verbose mode off.
```

Execute the **get** command.

```
ftp> get a.cfg 1.cfg
```

Enable the device to display detailed information about FTP operations.

```
ftp> verbose
Verbose mode on.
```

Execute the **get** command.

```
ftp> get a.cfg 2.cfg
227 Entering Passive Mode (192,168,1,58,68,14)
```

```
150-Accepted data connection
150 The computer is your friend. Trust the computer
226 File successfully transferred
3796 bytes received in 0.00762 seconds (486.5 kbyte/s)
```

Contents

A page of this section is **1-x-x**

5. TFTP commands 5-1
5.1. TFTP commands 5-1
5.1.1. tftp 5-1
5.1.2. tftp client ipv6 source 5-3
5.1.3. tftp client source 5-3
5.1.4. tftp ipv6 5-4
5.1.5. tftp-server acl 5-6
5.1.6. tftp-server ipv6 acl 5-6

5. TFTP commands

5.1. TFTP commands

5.1.1. tftp

Use **tftp** to download a file from a TFTP server or upload a file to a TFTP server in an IPv4 network.

Syntax

tftp *tftp-server* { **get** | **put** | **sget** } *source-filename* [*destination-filename*] [**vpn-instance** *vpn-instance-name*] [**dscp** *dscp-value* | **source** { **interface** *interface-type interface-number* | **ip** *source-ip-address* }] *

Views

User view

Predefined user roles

network-admin

Parameters

tftp-server: Specifies the IPv4 address or host name of a TFTP server. The host name can be a case-insensitive string of 1 to 253 characters and can contain only letters, digits, hyphens (-), underscores (_), and dots (.).

get: Downloads a file and writes the file directly to the destination folder. If the destination folder already has a file with the same name, the system deletes the existing file before starting the download operation. The existing file is permanently deleted even if the download operation fails.

put: Uploads a file.

sget: Downloads a file and saves the file to memory before writing it to the destination folder. The system starts to write the file to the destination folder only after the file is downloaded and saved to memory successfully. If the destination folder already has a file with the same name, the system overwrites the existing file. If the download or save-to-memory operation fails, the existing file in the destination folder is not overwritten.

source-filename: Specifies the source file name, a case-insensitive string of 1 to 1 to 255 characters.

destination-filename: Specifies the destination file name, a case-insensitive string of 1 to 255 characters. If this argument is not specified, the file uses the source file name.

vpn-instance *vpn-instance-name*: Specifies the VPN instance to which the TFTP server belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. If the TFTP server belongs to the public network, do not specify this option.

dscp *dscp-value*: Specifies the DSCP value for IPv4 to use for outgoing TFTP packets to indicate the packet transmission priority. The value range is 0 to 63. The default is 0.

source { **interface** *interface-type interface-number* | **ip** *source-ip-address* }: Specifies the source address for outgoing TFTP packets. If you do not specify this option, the device uses the primary IPv4 address of the output interface for the route to the TFTP server as the source address.

- **interface** *interface-type interface-number*: Specifies an interface by its type and number. The device will use the interface's primary IPv4 address as the source IPv4 address. For successful TFTP packet transmission, make sure the interface is up and has the primary IPv4 address configured.
- **ip** *source-ip-address*: Specifies an IPv4 address. For successful TFTP packet transmission, make sure this address is the IPv4 address of an interface in up state on the device.

Usage guidelines

The source address specified with the **tftp** command takes precedence over the source address specified with the **tftp client source** command.

The source address specified with the **tftp client source** command applies to all TFTP connections. The source address specified with the **tftp** command applies only to the current TFTP connection.

Examples

Download the **new.bin** file from TFTP server 192.168.1.1 and save the file as **new.bin**.

```
<Switch> tftp 192.168.1.1 get new.bin
Press CTRL+C to abort.
   % Total    % Received % Xferd  Average Speed   Time    Time     Time   Current
                                   Dload  Upload   Total   Spent    Left   Speed
100 13.9M  100 13.9M    0     0  1206k      0  0:00:11  0:00:11  --:--:-- 1206k
Writing file...Done.
<System>
```

Table 5-1 Command output

Field	Description
%	Percentage of file transmission progress.
Total	Size of files to be transmitted, in bytes.
%	Percentage of received file size to total file size.
Received	Received file size, in bytes.
%	Percentage of sent file size to total file size.
Xferd	Sent file size, in bytes.
Average Dload	Average download speed, in bps.
Speed Upload	Average upload speed, in bps.
Writing file…	The system was writing the downloaded file to the storage medium. This field is displayed only when the **get** or **sget** keyword is specified. If the operation succeeded, this command displays **Done** at the end of this field. If the operation failed, this command displays **Failed**.

Related commands

tftp client source

5.1.2. tftp client ipv6 source

Use **tftp client ipv6 source** to specify the source IPv6 address for TFTP packets sent to an IPv6 TFTP server.

Use **undo tftp client ipv6 source** to restore the default.

Syntax

tftp client ipv6 source { **interface** *interface-type interface-number* | **ipv6** *source-ipv6-address* }

undo tftp client ipv6 source

Default

No source address is specified for TFTP packets sent to an IPv6 TFTP server. The device selects a source IPv6 address as defined in RFC 3484.

Views

System view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. The device will use the interface's IPv6 address as the source address. For successful TFTP packet transmission, make sure the interface is up and is configured with an IPv6 address.

ipv6 *source-ipv6-address*: Specifies an IPv6 address . For successful TFTP packet transmission, make sure this address is the IPv6 address of an interface in up state on the device.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

The source address specified with the **tftp ipv6** command takes precedence over the source address specified with the **tftp client ipv6 source** command.

The source address specified with the **tftp client ipv6 source** command applies to all TFTP connections. The source address specified with the **tftp ipv6** command applies only to the TFTP connection that is being established.

Examples

Specify the source IPv6 address of 2000::1 for TFTP packets sent to an IPv6 TFTP server.

```
<Switch> system-view
[Switch] tftp client ipv6 source ipv6 2000::1
```

Related commands

tftp ipv6

5.1.3. tftp client source

Use **tftp client source** to specify the source IPv4 address for TFTP packets sent to an IPv4 TFTP server.

Use **undo tftp client source** to restore the default.

Syntax

tftp client source { **interface** *interface-type interface-number* | **ip** *source-ip-address* }

undo tftp client source

Default

No source IPv4 address is specified for TFTP packets sent to an IPv4 TFTP server. The device uses the primary IPv4 address of the output interface for the route to the server as the source address.

Views

System view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. The device will use the interface's primary IPv4 address as the source address. For successful TFTP packet transmission, make sure the interface is up and has the primary IPv4 address configured.

ip *source-ip-address*: Specifies an IPv4 address. For successful TFTP packet transmission, make sure this address is the IPv4 address of an interface in up state on the device.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

The source address specified with the **tftp** command takes precedence over the source address specified with the **tftp client source** command.

The source address specified with the **tftp client source** command applies to all TFTP connections. The source address specified with the **tftp** command applies only to the TFTP connection that is being established.

Examples

Specify the source IP address of 192.168.20.222 for TFTP packets sent to an IPv4 TFTP server.

```
<Switch> system-view
[Switch] tftp client source ip 192.168.20.222
```

Related commands

tftp

5.1.4. tftp ipv6

Use **tftp ipv6** to download a file from a TFTP server or upload a file to a TFTP server in an IPv6 network.

Syntax

tftp ipv6 *tftp-server* [**-i** *interface-type interface-number*] { **get** | **put** | **sget** } *source-filename* [*destination-filename*] [**vpn-instance** *vpn-instance-name*] [**dscp** *dscp-value* | **source** { **interface** *interface-type interface-number* | **ipv6** *source-ipv6-address* }] *

Views

User view

Predefined user roles

network-admin

Parameters

tftp-server: Specifies the IPv6 address or host name of a TFTP server. The host name can be a case-insensitive string of 1 to 253 characters and can contain only letters, digits, hyphens (-), underscores (_), and dots (.).

-i *interface-type interface-number*: Specifies an output interface by its type and number. This option can be used only when the TFTP server address is a link local address and the specified output interface has a link local address. For information about link local addresses, see *Layer 3—IP Services Configuration Guide*.

get: Downloads a file and writes the file directly to the destination folder. If the destination folder already has a file with the same name, the system deletes the existing file before starting the download operation. The existing file is permanently deleted even if the download operation fails.

put: Uploads a file.

sget: Downloads a file and saves the file to memory before writing it to the destination folder. The system starts to write the file to the destination folder only after the file is downloaded and saved to memory successfully. If the destination folder already has a file using the same name, the system overwrites the existing file. If the download or save-to-memory operation fails, the existing file in the destination folder is not overwritten.

source-filename: Specifies the source file name, a case-insensitive string of 1 to 255 characters.

destination-filename: Specifies the destination file name, a case-insensitive string of 1 to 255 characters. If this argument is not specified, the file uses the source file name.

vpn-instance *vpn-instance-name*: Specifies the VPN instance to which the TFTP server belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. If the TFTP server belongs to the public network, do not specify this option.

dscp *dscp-value*: Specifies the DSCP value for IPv6 to use in outgoing TFTP packets to indicate the packet transmission priority. The value range is 0 to 63. The default is 0.

source { **interface** *interface-type interface-number* | **ipv6** *source-ipv6-address* }: Specifies the source address for outgoing TFTP packets. If you do not specify this option, the device selects a source IPv6 address as defined in RFC 3484.

- **interface** *interface-type interface-number*: Specifies an interface by its type and number. The device will use the interface's IPv6 address as the source IPv6 address. For successful TFTP packet transmission, make sure the interface is up and is configured with an IPv6 address.
- **ipv6** *source-ipv6-address*: Specifies an IPv6 address. For successful TFTP packet transmission, make sure this address is the IPv6 address of an interface in up state on the device.

Usage guidelines

The source address specified with the **tftp ipv6** command takes precedence over the source address specified with the **tftp client ipv6 source** command.

The source address specified with the **tftp client ipv6 source** command applies to all TFTP connections. The source address specified with the **tftp ipv6** command applies only to the current TFTP connection.

Examples

Download the **new.bin** file from TFTP server 2001::1 and save the file as **new.bin**.

```
<Switch> tftp ipv6 2001::1 get new.bin new.bin
Press CTRL+C to abort.
   % Total    % Received % Xferd  Average Speed   Time    Time     Time   Current
                                  Dload  Upload   Total   Spent    Left   Speed
100 13.9M  100 13.9M    0     0  1206k      0  0:00:11  0:00:11  --:--:-- 1206k
Writing file...Done.
```

For more information about the command output, see Table 5-1 .

5.1.5. tftp-server acl

Use **tftp-server acl** to use an ACL to control the device's access to TFTP servers in an IPv4 network.

Use **undo tftp-server acl** to restore the default.

Syntax

tftp-server acl *acl-number*

undo tftp-server acl

Default

No ACL is used to control the device's access to TFTP servers.

Views

System view

Predefined user roles

network-admin

Parameters

acl-number: Specifies the number of a basic ACL, in the range of 2000 to 2999.

Usage guidelines

You can use an ACL to deny or permit the device's access to specific TFTP servers.

Examples

Allow the device to access only TFTP server 1.1.1.1.

```
<Switch> system-view
[Switch] acl basic 2000
[Switch-acl-ipv4-basic-2000] rule permit source 1.1.1.1 0
[Switch-acl-ipv4-basic-2000] quit
[Switch] tftp-server acl 2000
```

5.1.6. tftp-server ipv6 acl

Use **tftp-server ipv6 acl** to use an ACL to control the device's access to TFTP servers in an IPv6 network.

Use **undo tftp-server ipv6 acl** to restore the default.

Syntax

tftp-server ipv6 acl *ipv6-acl-number*

undo tftp-server ipv6 acl

Default

No ACL is used to control the device's access to TFTP servers.

Views

System view

Predefined user roles

network-admin

Parameters

ipv6-acl-number: Specifies the number of a basic ACL, in the range of 2000 to 2999.

Usage guidelines

You can use an ACL to deny or permit the device's access to specific TFTP servers.

Examples

Allow the device to access only TFTP server 2001::1.

```
<Switch> System-view
[Switch] acl ipv6 basic 2001
[Switch-acl-ipv6-basic-2001] rule permit source 2001::1/128
[Switch-acl-ipv6-basic-2001] quit
[Switch] tftp-server ipv6 acl 2001
```

Contents

A page of this section is **1-x-x**

6. File system management commands ····· 6-1
6.1. File system management commands ····· 6-1
6.1.1. cd ····· 6-1
6.1.2. copy ····· 6-2
6.1.3. delete ····· 6-4
6.1.4. dir ····· 6-5
6.1.5. file prompt ····· 6-7
6.1.6. fixdisk ····· 6-7
6.1.7. format ····· 6-8
6.1.8. gunzip ····· 6-8
6.1.9. gzip ····· 6-9
6.1.10. mkdir ····· 6-10
6.1.11. more ····· 6-11
6.1.12. mount ····· 6-11
6.1.13. move ····· 6-12
6.1.14. pwd ····· 6-13
6.1.15. rename ····· 6-13
6.1.16. reset recycle-bin ····· 6-14
6.1.17. rmdir ····· 6-14
6.1.18. tar create ····· 6-15
6.1.19. tar extract ····· 6-16
6.1.20. tar list ····· 6-17
6.1.21. umount ····· 6-17
6.1.22. undelete ····· 6-18

6. File system management commands

6.1. File system management commands

IMPORTANT:

- Before managing storage media, file systems, directories, and files, make sure you know the possible impact.
- A file or directory whose name starts with a dot character (.) is a hidden file or directory. To prevent the system from hiding a file or directory, make sure the file or directory name does not start with a dot character.
- Some system files and directories are hidden. For correct system operation and full functionality, do not modify or delete hidden files or directories.

File system names, directory names, and file names must be compliant with the naming conventions. For more information about the naming conventions and the methods for specifying the names, see *Fundamentals Configuration Guide*.

Before you use the **copy**, **delete**, **fixdisk**, **format**, **gunzip**, **gzip**, **mkdir**, **move**, **rename**, **rmdir**, or **undelete** command on a file system, make sure the file system is not write protected.

You cannot access a storage medium that is being partitioned, or a file system that is being formatted or repaired. To access the file system, wait for the ongoing operation to be completed and then use one of the following methods:

- Use the absolute path to specify a file or directory. For example, use the **dir flash:/** command to display the files and directories in the **flash:** file system.
- Use the **cd** command to change the working directory to the root directory of the file system before accessing a file or directory in the file system. For example, to display the files and directories in the root directory of the **flash:** file system, perform the following tasks:
  a. Use the **cd flash:/** command to change the working directory to the root directory of the file system.
  b. Execute the **dir** command.

6.1.1. cd

Use **cd** to change the working directory.

Syntax

cd { *directory* | **..** }

Views

User view

Predefined user roles

network-admin

Parameters

directory: Specifies the destination directory.

..: Specifies the parent directory. If the working directory is the root directory, an error message appears when you execute the **cd ..** command. No online help information is available for this keyword.

Examples

Access the **test** directory after logging in to the device.

```
<Switch> cd test
```

Change to the parent directory.

```
<Switch> cd ..
```

6.1.2. copy

Use **copy** to copy a file.

Syntax

copy *source-file* { *dest-file* | *dest-directory* }

Views

User view

Predefined user roles

network-admin

Parameters

source-file: Specifies the name or URL of the file to be copied. If the file resides on an FTP, TFTP, or HTTP server rather than on the device, specify the URL of the file. Whether a URL is case sensitive depends on the server.

dest-file: Specifies the name or URL for the destination file. To copy the source file to an FTP, TFTP, or HTTP server, specify a URL. Whether a URL is case sensitive depends on the server.

dest-directory: Specifies the destination directory or URL. To copy the source file to an FTP, TFTP, or HTTP server, specify a URL. The device copies the source file to the destination location and saves the file with its original file name. Whether a URL is case sensitive depends on the server.

Usage guidelines

You can use the **copy** command to perform the following tasks:

- Copy a local file and save it locally.
- Copy a local file and save it to an FTP, TFTP, or HTTP server.
- Copy a file from an FTP, TFTP, or HTTP server and save it locally.

To specify a file or directory, use the following guidelines:

Location	Name format	Remarks
On the device	Use the file name guidelines in *Fundamentals Configuration Guide*.	N/A
On an FTP server	Enter the URL in the format of **ftp://***FTP username*[**:***password*]**@***server address*[**:***port number*]*/file path*[*/file name*].	The username and password must be the same as the username and password configured on the FTP server. If the server authenticates users only by the username, you are not required to enter the password. For example, to use the username a and

Location	Name format	Remarks
		password 1 and specify the startup.cfg file in the authorized working directory on the FTP server 1.1.1.1, enter ftp://a:1@1.1.1.1/startup.cfg.
On a TFTP server	Enter the URL in the format of **tftp://***server address*[**:***port number*]*/file path*[*/file name*].	For example, to specify the startup.cfg file in the working directory on TFTP server 1.1.1.1, enter the URL tftp://1.1.1.1/startup.cfg.
On an HTTP server	Enter the URL in the format of **http://**[*HTTP username*[**:***password*]**@**]*server address*[**:***port number*]*/filepath*[*/file name*].	The username and password in the URL must be the same as the username and password configured on the server. If only the username is required for authentication, you do not need to enter the password. If authentication is not required, you do not need to enter the username or password. For example, the **startup.cfg** file is saved in the authorized directory on the HTTP server at 1.1.1.1. The HTTP account username and password are **a** and **1**, respectively. To copy the file, enter the URL http://a:1@1.1.1.1/startup.cfg. If authentication is not required, enter the URL http://1.1.1.1/startup.cfg.

To specify an IPv6 address, enclose the IPv6 address in square brackets ([ ]), for example, ftp://test:test@[2001::1]:21/test.cfg.

Examples

Copy the **test.cfg** file in the current directory and save it to the current directory as **testbackup.cfg**.

```
<Switch> copy test.cfg testbackup.cfg
Copy flash:/test.cfg to flash:/testbackup.cfg? [Y/N]:y
Copying file flash:/test.cfg to flash:/testbackup.cfg...Done.
```

Copy the **1.cfg** file from the **flash:** file system's **test** directory to the USB disk. Save the copy to the **testbackup** directory on the first partition as **1backup.cfg**.

```
<Switch> copy flash:/test/1.cfg usba0:/testbackup/1backup.cfg
Copy flash:/test/1.cfg to usba0:/testbackup/1backup.cfg? [Y/N]:y
Copying file flash:/test/1.cfg to usba0:/testbackup/1backup.cfg...Done.
```

Copy the **test.cfg** file in the current directory and save it to the root directory of a file system in a specific slot as **testbackup.cfg**.

```
<Switch> copy test.cfg slot2#flash:/
Copy flash:/test.cfg to slot2#flash:/test.cfg? [Y/N]:y
Copying file flash:/test.cfg to slot2#flash:/test.cfg...Done.
```

Copy **test.cfg** from the working directory on FTP server 1.1.1.1. Save the copy to the local current directory as **testbackup.cfg.** The FTP username is **user**. The password is **private**.

```
<Switch> copy ftp://user:private@1.1.1.1/test.cfg testbackup.cfg
Copy ftp://user:private@1.1.1.1/test.cfg to flash:/testbackup.cfg? [Y/N]:y
Copying file ftp://user:private@1.1.1.1/test.cfg to flash:/testbackup.cfg... Done.
```

Copy **test.cfg** from the current directory. Save the copy to the working directory on FTP server 1.1.1.1 as **testbackup.cfg**. The FTP username is **user**. The password is **private**.

```
<Switch> copy test.cfg ftp://user:private@1.1.1.1/testbackup.cfg
Copy flash:/test.cfg to ftp://user:private@1.1.1.1/testbackup.cfg? [Y/N]:y
Copying file flash:/test.cfg to ftp://user:private@1.1.1.1/testbackup.cfg... Done.
```

Copy **test.cfg** from the working directory on TFTP server 1.1.1.1. Save the copy to the local current directory as **testbackup.cfg**.

```
<Switch> copy tftp://1.1.1.1/test.cfg testbackup.cfg
Copy tftp://1.1.1.1/test.cfg to flash:/testbackup.cfg? [Y/N]:y
Copying file tftp://1.1.1.1/test.cfg to flash:/testbackup.cfg... Done.
```

Copy **test.cfg** from the current directory. Save the copy to the working directory on TFTP server 1.1.1.1 as **testbackup.cfg**.

```
<Switch> copy test.cfg tftp://1.1.1.1/testbackup.cfg
Copy flash:/test.cfg to tftp://1.1.1.1/testbackup.cfg? [Y/N]:y
Copying file flash:/test.cfg to tftp://1.1.1.1/testbackup.cfg... Done.
```

Copy **test.cfg** from the working directory on FTP server 2001::1. Save the copy to the local current directory as **testbackup.cfg**. The FTP username is **user**. The password is **private**.

```
<Switch> copy ftp://user:private@[2001::1]/test.cfg testbackup.cfg
Copy ftp://user:private@[2001::1]/test.cfg to flash:/testbackup.cfg? [Y/N]:y
Copying file ftp://user:private@[2001::1]/test.cfg to flash:/testbackup.cfg... Done.
```

Copy **test.cfg** from the working directory on TFTP server 2001::1. Save the copy to the local current directory as **testbackup.cfg**.

```
<Switch> copy tftp://[2001::1]/test.cfg testbackup.cfg
Copy tftp://[2001::1]/test.cfg to flash:/testbackup.cfg? [Y/N]:y
Copying file tftp://[2001::1]/test.cfg to flash:/testbackup.cfg... Done.
```

Copy **test.cfg** from the authorized directory on HTTP server 1.1.1.1. Save the copy to the local current directory as **testbackup.cfg**. The HTTP login username is **user**. The password is **private**.

```
<Switch> copy http://user:private@1.1.1.1/test.cfg testbackup.cfg
Copy http://user:private@1.1.1.1/test.cfg to flash:/testbackup.cfg? [Y/N]:y
Copying file http://user:private@1.1.1.1/test.cfg to flash:/testbackup.cfg... Done.
```

Copy **test.cfg** from the current directory. Save the copy to the authorized directory on HTTP server 1.1.1.1 as **testbackup.cfg**. The HTTP login username is **user**. The password is **private**.

```
<Switch> copy test.cfg http://user:private@1.1.1.1/testbackup.cfg
Copy flash:/test.cfg to http://user:private@1.1.1.1/testbackup.cfg? [Y/N]:y
Copying file flash:/test.cfg to http://user:private@1.1.1.1/testbackup.cfg... Done.
```

Copy **test.cfg** from the authorized directory on HTTP server 2001::1. Save the copy to the local current directory as **testbackup.cfg**. The HTTP login username is **user**. The password is **private**.

```
<Switch> copy http://user:private@[2001::1]/test.cfg testbackup.cfg
Copy http://user:private@[2001::1]/test.cfg to flash:/testbackup.cfg? [Y/N]:y
Copying file http://user:private@[2001::1]/test.cfg to flash:/testbackup.cfg... Done.
```

6.1.3. delete

Use **delete** to delete a file.

Syntax

delete [**/unreserved**] *file*

Views

User view

Predefined user roles

network-admin

Parameters

/unreserved: Permanently deletes the specified file. If you do not specify this keyword, the command moves the file to the recycle bin.

file: Specifies the name of the file to be deleted. Asterisks (*) are acceptable as wildcards. For example, to remove files with the **.txt** extension in the current directory, enter **delete *.txt**.

Usage guidelines

The **delete /unreserved** *file* command deletes a file permanently. The file cannot be restored.

The **delete** *file* command (without **/unreserved**) moves a file to the recycle bin.

A file moved to the recycle bin can be restored by using the **undelete** command.

Do not use the **delete** command to delete files from the recycle bin. To delete files from the recycle bin, use the **reset recycle-bin** command.

If you delete two files that have the same name from different directories, both files are retained in the recycle bin. If you successively delete two files that have the same name from the same directory, only the most recently deleted file is retained in the recycle bin.

Examples

Remove the **1.cfg** file from the current directory.

```
<Switch> delete 1.cfg
Delete flash:/1.cfg? [Y/N]:y
Deleting file flash:/1.cfg...Done.
```

Permanently delete the **1.cfg** file from the current directory.

```
<Switch> delete /unreserved 1.cfg
The file cannot be restored. Delete flash:/1.cfg? [Y/N]:y
Deleting the file permanently will take a long time. Please wait...
Deleting file flash:/1.cfg...Done.
```

Related commands

reset recycle-bin

undelete

6.1.4. dir

Use **dir** to display files or directories.

Syntax

dir [**/all**] [*file* | *directory* | **/all-filesystems**]

Views

User view

Predefined user roles

network-admin

Parameters

/all: Displays all files and directories in the current directory, visible or hidden. If you do not specify this option, only visible files and directories are displayed.

file: Displays a specific file. This argument can use the asterisk (*) as a wildcard. For example, to display files with the **.txt** extension in the current directory, enter **dir *.txt**.

directory: Displays a specific directory.

/all-filesystems: Displays files and directories in the root directories of all file systems on the device.

Usage guidelines

If no option is specified, the command displays all visible files and directories in the current directory.

The directory name of the recycle bin is **.trash**. To display files in the recycle bin, use either of the following methods:

- Execute the **dir /all .trash** command.
- Execute the **cd .trash** command and then the **dir** command.

If multiple users perform file operations (for example, creating or deleting files or directories) at the same time, the output for this command might be incorrect.

Examples

Display information about all files and directories in the current directory.

```
<Switch> dir /all
Directory of flash:/
...
```

Display files and directories in the root directories of all file systems on the device.

```
<Switch> dir /all-filesystems
Directory of flash:/
...

Directory of usba0:/
...
```

Table 6-1 Command output

Field	Description
Directory of	Current directory.
0 -rwh 3144 Apr 26 2014 13:45:28 xx.xx	File or directory information: • **0**—File or directory number, which is automatically allocated by the system. • **-rwh**—Attributes of the file or directory. The first character is the directory indicator (**d** for directory and **–** for file). The second character indicates whether the file or directory is readable (**r** for readable). The third character indicates whether the file or directory is writable (**w** for writable). The fourth character indicates whether the file or directory is hidden (**h** for hidden, **-** for visible). Modifying, renaming, or deleting hidden files might affect functions. • **3144**—File size in bytes. For a directory, a hyphen (-) is displayed. • **Apr 26 2014 13:45:28**—Last date and time when the file or directory was modified.

Field	Description
	• **xx.xx**—File or directory name.

6.1.5. file prompt

Use **file prompt** to set the operation mode for files and directories.

Use **undo file prompt** to restore the default.

Syntax

file prompt { **alert** | **quiet** }

undo file prompt

Default

The operation mode is **alert**. The system prompts for confirmation when you perform a destructive file or directory operation.

Views

System view

Predefined user roles

network-admin

Parameters

alert: Prompts for confirmation when a destructive file or directory operation is being performed.

quiet: Gives no confirmation prompt for file or directory operations.

Usage guidelines

In quiet mode, the system does not prompt for confirmation when a user performs a file or directory operation. The **alert** mode provides an opportunity to cancel a disruptive operation.

Examples

Set the file and directory operation mode to **alert**.

```
<Switch> system-view
[Switch] file prompt alert
```

6.1.6. fixdisk

Use **fixdisk** to check a file system for damage and repair any damage.

Syntax

fixdisk *filesystem*

Views

User view

Predefined user roles

network-admin

Parameters

filesystem: Specifies the name of a file system.

Usage guidelines

Use this command to fix a file system when space in the file system cannot be used or released.

You can repair a file system only when no other users are accessing the file system.

Examples

Repair file system **flash:**.

```
<Switch> fixdisk flash:
Restoring flash: may take some time...
Restoring flash:...Done.
```

6.1.7. format

Use **format** to format a file system.

Syntax

format *filesystem*

Views

User view

Predefined user roles

network-admin

Parameters

filesystem: Specifies the name of a file system.

Usage guidelines

The device requires that the file systems on hot swappable storage media be VFAT file systems. To use a file system of a different type on the device, you must use this command to format the file system.

Formatting a file system permanently deletes all files in the file system. If a startup configuration file exists in the file system, back up the file if necessary.

You can format a file system only when no other users are accessing the file system.

Examples

Format file system **flash:**.

```
<Switch> format flash:
All data on flash: will be lost, continue? [Y/N]:y
Formatting flash:... Done.
```

Format the file system on the third partition of the USB disk.

```
<Switch> format usba2:
All data on usba2: will be lost, continue? [Y/N]:y
Formatting usba2:... Done.
```

6.1.8. gunzip

Use **gunzip** to decompress a file.

Syntax

gunzip *file*

Views

User view

Predefined user roles

network-admin

Parameters

file: Specifies the name of the file to be decompressed. This argument must use the **.gz** extension.

Usage guidelines

This command deletes the specified file after decompressing it.

Examples

Decompress file **system.bin.gz**:

1. Before decompressing the file, you can display files whose names start with the **system.** string.

```
<Switch> dir system.*
Directory of flash:
   1 -rw-          20 Jun 14 2012 10:18:53   system.bin.gz


524288 KB total (184664 KB free)
```

2. Decompress the file **system.bin.gz**.

```
<Switch> gunzip system.bin.gz
Decompressing file flash:/system.bin.gz..... Done.
```

3. Verify the decompress operation.

```
<Switch> dir system.*
Directory of flash:
   1 -rw-           0 May 30 2012 11:42:25   system.bin


524288 KB total (184664 KB free)
```

6.1.9. gzip

Use **gzip** to compress a file.

Syntax

gzip *file*

Views

User view

Predefined user roles

network-admin

Parameters

file: Specifies the name of the file to be compressed.

Usage guidelines

This command saves the compressed file to the *file***.gz** file and deletes the source file.

Examples

Compress file **system.bin**:

1. Before compressing the file, you can display files whose names start with the **system.** string.

```
<Switch> dir system.*
Directory of flash:
   1 -rw-           0 May 30 2012 11:42:24   system.bin


524288 KB total (184664 KB free)
```

2. Compress the file **system.bin**.

```
<Switch> gzip system.bin
Compressing file flash:/system.bin..... Done.
```

3. Verify the compress operation.

```
<Switch> dir system.*
Directory of flash:
   1 -rw-          20 Jun 14 2012 10:18:53   system.bin.gz


524288 KB total (184664 KB free)
```

6.1.10. mkdir

Use **mkdir** to create a directory.

Syntax

mkdir *directory*

Views

User view

Predefined user roles

network-admin

Parameters

directory: Specifies a directory.

Usage guidelines

The name of the directory to be created must be unique in the parent directory.

You can create a directory only in an existing directory. For example, to create the **flash:/test/mytest** directory, make sure the **test** directory already exists.

Examples

Create the **test** directory in the current directory.

```
<Switch> mkdir test
Creating directory flash:/test... Done.
```

Create the **test/subtest** directory in the current directory.

```
<Switch> mkdir test/subtest
Creating directory flash:/test/subtest... Done.
```

6.1.11. more

Use **more** to display the contents of a text file.

Syntax

more *file*

Views

User view

Predefined user roles

network-admin

Parameters

file: Specifies the name of a file.

Examples

Display the contents of the **test.txt** file.

```
<Switch> more test.txt
Have a nice day.
```

Display the contents of the **testcfg.cfg** file.

```
<Switch> more testcfg.cfg

#
 version 7.1.0
#
 sysname Switch
#
vlan 2
#
return
<Switch>
```

6.1.12. mount

Use **mount** to mount a file system.

Syntax

mount *filesystem*

Views

User view

Predefined user roles

network-admin

Parameters

filesystem: Specifies the name of a file system.

Usage guidelines

Generally, file systems on a hot-swappable storage medium are automatically mounted when the storage medium is connected to the device. If the system cannot recognize a file system, however, you must mount the file system before you can access it.

To avoid file system corruption, do not perform the following tasks while the system is mounting a file system:

- Reboot, power cycle, or power off the device.
- Install or remove storage media.
- Perform a switchover.

To remove a hot-swappable storage medium from the device, you must first unmount all file systems on the storage medium. Removing a mounted hot-swappable storage medium might damage files on the storage medium or even the storage medium.

Examples

Mount a file system on the USB disk.

```
<Switch> mount usba0:
```

Related commands

umount

6.1.13. move

Use **move** to move a file.

Syntax

move *source-file* { *dest-file* | *dest-directory* }

Views

User view

Predefined user roles

network-admin

Parameters

source-file: Specifies the name of the source file.

dest-file: Specifies the name of the destination file.

dest-directory: Specifies the name of the destination directory.

Usage guidelines

If you specify a destination directory, the system moves the source file to the specified directory without changing the file name.

Examples

Move the **flash:/test/sample.txt** file to **flash:/**, and save it as **1.txt**.

```
<Switch> move test/sample.txt 1.txt
Move flash:/test/sample.txt to flash:/1.txt? [Y/N]:y
Moving file flash:/test/sample.txt to flash:/1.txt ...Done.
```

Move the **b.cfg** file to the **test2** directory.

```
<Switch> move b.cfg test2
Move flash:/b.cfg to flash:/test2/b.cfg? [Y/N]:y
```

```
Moving file flash:/b.cfg to flash:/test2/b.cfg... Done.
```

6.1.14. pwd

Use **pwd** to display the working directory.

Syntax

pwd

Views

User view

Predefined user roles

network-admin

Examples

Display the working directory.

```
<Switch> pwd
flash:
```

6.1.15. rename

Use **rename** to rename a file or directory.

Syntax

rename { *source-file* | *source-directory* } { *dest-file* | *dest-directory* }

Views

User view

Predefined user roles

network-admin

Parameters

source-file: Specifies the name of the source file.

source-directory: Specifies the name of the source directory.

dest-file: Specifies the name of the destination file.

dest-directory: Specifies the name of the destination directory.

Usage guidelines

This command is not executed if the destination file or directory name is already used by an existing file or directory in the working directory.

Examples

Rename the **copy.cfg** file as **test.cfg**.

```
<Switch> rename copy.cfg test.cfg
Rename flash:/copy.cfg as flash:/test.cfg? [Y/N]:y
Renaming flash:/copy.cfg as flash:/test.cfg... Done.
```

6.1.16. reset recycle-bin

Use **reset recycle-bin** to delete files from the recycle bin.

Syntax

reset recycle-bin [**/force**]

Views

User view

Predefined user roles

network-admin

Parameters

/force: Deletes all files in the recycle bin without prompting for confirmation. If you do not specify this option, the command prompts you to confirm the deletion operation for each file.

Usage guidelines

The **delete** *file* command only moves a file to the recycle bin. To permanently delete the file, use the **reset recycle-bin** command to delete the file from the recycle bin.

Examples

Empty the recycle bin. (In this example there are two files in the recycle bin.)

```
<Switch> reset recycle-bin
Clear flash:/a.cfg? [Y/N]:y
Clearing file flash:/a.cfg... Done.
Clear flash:/b.cfg? [Y/N]:y
Clearing file flash:/b.cfg... Done.
```

Delete the **b.cfg** file from the recycle bin. (In this example there are two files in the recycle bin.)

```
<Switch> reset recycle-bin
Clear flash:/a.cfg? [Y/N]:n
Clear flash:/b.cfg? [Y/N]:y
Clearing file flash:/b.cfg... Done.
```

Related commands

delete

6.1.17. rmdir

Use **rmdir** to delete a directory.

Syntax

rmdir *directory*

Views

User view

Predefined user roles

network-admin

Parameters

directory: Specifies a directory.

Usage guidelines

To delete a directory, you must delete all files and subdirectories in the directory permanently or move them to the recycle bin. If you move them to the recycle bin, executing the **rmdir** command permanently deletes them.

Examples

Delete the **subtest** directory.

```
<Switch>rmdir subtest/
Remove directory flash:/test/subtest and the files in the recycle-bin under this directory
will be deleted permanently. Continue? [Y/N]:y
Removing directory flash:/test/subtest... Done.
```

6.1.18. tar create

Use **tar create** to archive files and directories.

Syntax

tar create [**gz**] **archive-file** *dest-file* [**verbose**] **source** { *source-file* | *source-directory* }&<1-5>

Views

User view

Predefined user roles

network-admin

Parameters

gz: Uses gzip to compress the files and directories before archiving them. If you do not specify this keyword, the command archives the files and directories without compressing them.

archive-file *dest-file*: Specifies the archive file name. If you specified the **gz** keyword, the extension of the archive file name must be **.tar.gz**. If you did not specify the **gz** keyword, the extension of the archive file name must be **.tar**.

verbose: Displays the names of the successfully archived files and directories. If you do not specify this keyword, the command does not display the names of the successfully archived files and directories.

source { *source-file* | *source-directory* }&<1-5>: Specifies the files and directories to be archived. The argument can be a space-separated list of up to five items. Each item can be a file or directory name.

Examples

Archive the **1.cfg** and **2.cfg** files and the **test** directory to **a.tar**.

```
<Switch> tar create archive-file a.tar source 1.cfg 2.cfg test
Creating archive flash:/a.tar Done.
```

Compress and archive the **1.cfg** and **2.cfg** files and the **test** directory to **b.tar.gz**.

```
<Switch> tar create gz archive-file b.tar.gz source 1.cfg 2.cfg test
Creating archive flash:/b.tar.gz Done.
```

Compress and archive files and directories, and display the successfully archived files and directories.

```
<Switch> tar create gz archive-file c.tar.gz verbose source 1.cfg 2.cfg test
1.cfg
```

```
2.cfg
test/
test/a.log
test/subtest/
test/subtest/aa.log
```

Related commands

tar extract

tar list

6.1.19. tar extract

Use **tar extract** to extract files and directories.

Syntax

tar extract archive-file *file* [**verbose**] [**screen** | **to** *directory*]

Views

User view

Predefined user roles

network-admin

Parameters

archive-file *file*: Specifies the archive file name. The extension can be **.tar** or **.tar.gz**.

verbose: Displays the names of the successfully extracted files and directories.

screen: Displays the content of the extracted files and directories on the screen. The extracted files are not saved.

to *directory*: Saves the extracted files and directories to a different directory. The *directory* argument specifies the directory.

Usage guidelines

If you do not specify the **screen** keyword or the **to** *directory* option, the command saves the extracted files and directories to the working directory.

The command saves the extracted files and directories by using their original names. If a file or directory that has the same name as an extracted file or directory already exists in the destination directory, the file or directory is overwritten.

Examples

Extract files and directories from archive file **a.tar**.

```
<Switch> tar extract archive-file a.tar
Extracting archive flash:/a.tar Done.
```

Extract files and directories from archive file **a.tar**, and display the names of the successfully extracted files and directories.

```
<Switch> tar extract archive-file b.tar.gz verbose
1.cfg
2.cfg
test/
test/a.log
test/subtest/
```

```
test/subtest/aa.log
```

Extract files and directories from archive file **a.tar**, and display the content of the files on the screen.

```
<Switch> tar extract archive-file c.tar.gz screen
#
 version 7.1.070, Release 1201
#
 sysname Switch
#
...
```

Related commands

tar create

tar list

6.1.20. tar list

Use **tar list** to display the names of archived files and directories.

Syntax

tar list archive-file *file*

Views

User view

Predefined user roles

network-admin

Parameters

archive-file *file*: Specifies the archive file name. The extension can be **.tar** or **.tar.gz**.

Examples

Display the names of archived files and directories.

```
<Switch> tar list archive-file a.tar
1.cfg
2.cfg
test/
test/a.log
test/subtest/
test/subtest/aa.log
```

Related commands

tar create

tar extract

6.1.21. umount

Use **umount** to unmount a file system.

Syntax

umount *filesystem*

Views

User view

Predefined user roles

network-admin

Parameters

filesystem: Specifies the name of a file system.

Usage guidelines

File systems on a storage medium are automatically mounted when the storage medium is connected to the device. To remove a hot-swappable storage medium from the device, you must first unmount all file systems on the storage medium. Removing a mounted hot-swappable storage medium might damage files on the storage medium or even the storage medium.

You can unmount a file system only when no other users are accessing the file system.

To avoid file system corruption, do not perform the following tasks while the system is unmounting a file system:

- Reboot, power cycle, or power off the device.
- Install, remove, or access storage media.
- Perform a switchover.

Examples

Unmount a file system on a USB disk.

```
<Switch> umount usba0:
```

Related commands

mount

6.1.22. undelete

Use **undelete** to restore a file from the recycle bin.

Syntax

undelete *file*

Views

User view

Predefined user roles

network-admin

Parameters

file: Specifies the name of the file to be restored.

Usage guidelines

If a file with the same name already exists in the directory, the system prompts whether or not you want to overwrite the existing file. If you enter **Y**, the existing file is overwritten. If you enter **N**, the command is not executed.

Examples

Restore the **copy.cfg** file, which was moved from the root directory of the **flash:** file system to the recycle bin.

```
<Switch>undelete copy.cfg
Undelete flash:/copy.cfg? [Y/N]:y
Undeleting file flash:/copy.cfg... Done.
```

Restore the **startup.cfg** file, which was moved from the **flash:/seclog** directory to the recycle bin.

- Method 1:

```
<Switch>undelete seclog/startup.cfg
Undelete flash:/seclog/startup.cfg? [Y/N]:y
Undeleting file flash:/seclog/startup.cfg... Done.
<Switch>
```

- Method 2:

```
<Switch> cd seclog
<Switch> undelete startup.cfg
Undelete flash:/seclog/startup.cfg? [Y/N]:y
Undeleting file flash:/seclog/startup.cfg... Done.
```

Contents

A page of this section is **1-x-x**

7. Configuration file management commands 7-1
7.1. Configuration file management commands 7-1
7.1.1. backup startup-configuration 7-1
7.1.2. display current-configuration 7-1
7.1.3. display current-configuration diff 7-3
7.1.4. display default-configuration 7-4
7.1.5. display diff 7-5
7.1.6. display saved-configuration 7-6
7.1.7. display startup 7-7
7.1.8. display this 7-8
7.1.9. reset saved-configuration 7-8
7.1.10. restore startup-configuration 7-9
7.1.11. save 7-10
7.1.12. startup saved-configuration 7-13

7. Configuration file management commands

7.1. Configuration file management commands

7.1.1. backup startup-configuration

Use **backup startup-configuration** to back up the main next-startup configuration file to a TFTP server.

Syntax

backup startup-configuration to *ipv4-server* [*dest-filename*] [**vpn-instance** *vpn-instance-name*]

Views

User view

Predefined user roles

network-admin

Parameters

ipv4-server: Specifies a TFTP server by its IPv4 address or host name. The host name is a case-insensitive string of 1 to 253 characters. Valid characters include letters, digits, hyphens (-), underscores (_), and dots (.).

dest-filename: Specifies the name of the target file used for saving the file on the server. The file must be a .cfg file. The file name is a case-insensitive string of up to 255 characters. If you do not specify a target file name, the source file name is used.

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. If the TFTP server is on the public network, do not specify this option.

Examples

Back up the main next-startup configuration file to the IPv4 TFTP server at 2.2.2.2 in the public network, and set the target file name to **192-168-1-26.cfg**.

```
<Switch> backup startup-configuration to 2.2.2.2 192-168-1-26.cfg
Backing up the main startup configuration file to 2.2.2.2...
Done.
```

Back up the main next-startup configuration file to the IPv4 TFTP server at 2.2.2.2 in VPN instance **VPN1**, and set the target file name to **192-168-1-26.cfg**.

```
<Switch> backup startup-configuration to 2.2.2.2 192-168-1-26.cfg vpn-instance VPN1
Backing up the main startup configuration file to 2.2.2.2 in VPN VPN1...
Done.
```

Related commands

restore startup-configuration

7.1.2. display current-configuration

Use **display current-configuration** to display the running configuration.

Syntax

display current-configuration [[**configuration** [*module-name*] | **interface** [*interface-type* [*interface-number*]]]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

configuration [*module-name*]: Displays the feature configuration. The *module-name* argument specifies a feature module. If you do not specify a feature module, the command displays all feature settings you have made.

interface [*interface-type* [*interface-number*]]: Displays interface configuration, where the *interface-type* argument represents the interface type and the *interface-number* argument represents the interface number. If you do not specify the *interface-type* *interface-number* arguments, the command displays the running configuration for all interfaces. If you specify only the *interface-type* argument, the command displays the running configuration for all interfaces of this type.

Usage guidelines

Use this command to verify the configuration you have made.

If the system has automatically changed the setting you have made for a parameter, this command displays the effective setting instead of the configured one. An automatic change typically occurs because of system restrictions. This command does not display parameters that are using the default settings.

Examples

Display local user configuration.

```
<Switch> display current-configuration configuration local-user
#
local-user ftp
 password hash
$h$6$Twd73mLrN8O2vvD5$Cz1vgdpR4KoTiRQNE9pg33gU14Br2p1VguczLSVyJLO2huV5Syx/LfDIf8ROLtV
ErJ/C31oq2rFtmNuyZf4STw==
 service-type ftp
 authorization-attribute user-role network-operator
#
local-user root
 password hash
$h$6$Twd73mLrN8O2vvD5$Cz1vgdpR4KoTiRQNE9pg33gU14Br2p1VguczLSVyJLO2huV5Syx/LfDIf8ROLtV
ErJ/C31oq2rFtmNuyZf4STw==
 service-type ssh telnet terminal
 authorization-attribute user-role network-admin
#
return
```

Display VLAN interface configuration.

```
<Switch> display current-configuration interface Vlan-interface
#
```

```
interface Vlan-interface1
 ip address 192.168.1.84 255.255.255
#
Return
```

7.1.3. display current-configuration diff

Use **display current-configuration diff** to display the differences that the running configuration has as compared with the next-startup configuration.

Syntax

display current-configuration diff

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display the differences that the running configuration has as compared with the next-startup configuration.

```
<Switch> display current-configuration diff
--- Startup configuration
+++ Current configuration
@@ -5,7 +5,7 @@
 #
  sysname Switch
 #
-alias dhc display history-command
+alias dh display hotkey
 #
  system-working-mode standard
<Switch>
```

Table 7-1 Command output

Field	Description
--- *A* +++ *B*	• *A* represents the source configuration for comparison, which can be **Startup configuration**, **Current configuration**, or the name of the source configuration file with its directory information. • *B* represents the target configuration for comparison, which can be **Current configuration**, **Startup configuration**, or the name of the target configuration file with its directory information. In this example, the startup configuration and the current configuration are the source and target, respectively.
@@ *-linenumber1*,*number1* *+linenumber2*,*number2*	Location information for identifying the command line differences: • *-linenumber1*,*number1*—Source configuration section

Field	Description
@@	that contains differences. The *linenumber1* argument represents the start line of the section. The *number1* argument represents the number of lines between the start line and the end line of the section. • *+linenumber2*,*number2*—Target configuration section that contains differences. The *linenumber2* argument represents the start line of the section. The *number2* argument represents the number of lines between the start line and the end line of the section.
cmd1 *- cmd2* *+ cmd3* *cmd4*	Displays command differences. • *cmd1* and *cmd4*—Command lines are contained in both source and target configurations if they are not prefixed with a minus (-) or plus (+) sign. They provide a context for locating command line differences. • *- cmd2*—Command lines are prefixed with a minus sign if they are contained in the source configuration but not in the target configuration. • *+ cmd3*—Command lines are prefixed with a plus sign if they are contained in the target configuration but not in the source configuration. In this example, the sample output shows that the **alias dhc display history-command** command is contained only in the source configuration, and the **alias dh display hotkey** command is contained only in the target configuration.

Related commands

display current-configuration

display diff

display saved-configuration

7.1.4. display default-configuration

Use **display default-configuration** to display the factory defaults.

Syntax

display default-configuration

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

Factory defaults are custom basic settings that came with the device. Factory defaults vary by device models and might differ from the initial default settings for the commands.

The device starts up with the factory defaults if no next-startup configuration files are available.

Examples

Display the factory defaults.

```
<Switch> display default-configuration
```

7.1.5. display diff

Use **display diff** to display differences between configurations.

Syntax

display diff configfile *file-name-s* { **configfile** *file-name-d* | **current-configuration** | **startup-configuration** }

display diff current-configuration { **configfile** *file-name-d* | **startup-configuration** }

display diff startup-configuration { **configfile** *file-name-d* | **current-configuration** }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

configfile *file-name-s*: Specifies the source configuration file for comparison.

configfile *file-name-d*: Specifies the target configuration file for comparison.

current-configuration: Specifies the running configuration. In the **display diff current-configuration** command, this keyword specifies the source configuration for comparison. In the **display diff configfile** *file-name-s* and **display diff startup-configuration** commands, this keyword specifies the target configuration.

startup-configuration: Specifies the next-startup configuration. In the **display diff startup-configuration** command, this keyword specifies the source configuration for comparison. In the **display diff configfile** *file-name-s* and **display diff current-configuration** commands, this keyword specifies the target configuration.

Examples

Display the differences between **startup.cfg** and **test.cfg**.

```
<Switch> display diff configfile startup.cfg configfile test.cfg
--- flash:/startup.cfg
+++ flash:/test.cfg
@@ -5,7 +5,7 @@
 #
  sysname Switch
 #
-alias dhc display history-command
+alias dh display hotkey
 #
  system-working-mode standard
<Switch>
```

The output shows that the **alias dhc display history-command** command is contained only in **startup.cfg**, and the **alias dh display hotkey** command is contained only in **test.cfg**.

Display the differences between the running configuration and the next-startup configuration.

```
<Switch> display diff current-configuration startup-configuration
--- Current configuration
+++ Startup configuration
@@ -5,7 +5,7 @@
 #
  sysname Switch
 #
-alias dhc display history-command
+alias dh display hotkey
 #
  system-working-mode standard
<Switch>
```

The output shows that the **alias dhc display history-command** command is contained only in the running configuration, and the **alias dh display hotkey** command is contained only in the next-startup configuration.

For the command output description, see Table 7-1 .

Related commands

display current-configuration

display current-configuration diff

display saved-configuration

7.1.6. display saved-configuration

Use **display saved-configuration** to display the contents of the configuration file for the next system startup.

Syntax

display saved-configuration

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

Use this command to verify that important settings have been saved to the configuration file for the next system startup.

This command selects the configuration file to display in the following order:

1. If the main startup configuration file is available, this command displays the contents of the main startup configuration file.
2. If only the backup startup configuration file is available, this command displays the contents of the backup file.
3. If both the main and backup startup configuration files are not available, this command does not display anything.

Examples

Display the contents of the configuration file for the next system startup.

```
<Switch> display saved-configuration
#
 version 7.1.070, Release 1201
#
 sysname Switch
#
 ftp server enable
#
 telnet server enable
#
 domain default enable system
#
vlan 1
#
domain system
#
  ---- More ----
```

Related commands

reset saved-configuration

save

7.1.7. display startup

Use **display startup** to display the names of the current startup configuration file and the next-startup configuration files.

Syntax

display startup

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

All IRF members use the same current startup configuration file as the master.

After a master/subordinate switchover, it is normal that the current startup configuration files on all IRF members are displayed as NULL. This is because the new master continues to run with the running configuration rather than rebooting with a startup configuration file.

Examples

Display names of the startup configuration files.

```
<Switch> display startup
 Current startup saved-configuration file: flash:/startup.cfg
 Next main startup saved-configuration file: flash:/startup.cfg
```

```
Next backup startup saved-configuration file: NULL
```

Table 7-2 Command output

Field	Description
Current startup saved-configuration file	Configuration file that the device has started up with.
Next main startup saved-configuration file	Primary configuration file to be used at the next startup.
Next backup startup saved-configuration file	Backup configuration file to be used at the next startup.

Related commands

startup saved-configuration

7.1.8. display this

Use **display this** to display the running configuration in the current view.

Syntax

display this

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

Use this command to verify the configuration you have made in a certain view.

This command does not display parameters that are using the default settings.

Some parameters can be successfully set even if their dependent features are not enabled. For these parameters, this command displays their settings after the dependent features are enabled.

This command can be executed in any user line view to display the running configuration of all user lines.

Examples

Display the running configuration on VLAN-interface 1.

```
<Switch> system-view
[Switch] interface vlan-interface 1
[Switch-Vlan-interface1] display this
#
interface Vlan-interface1
#
return
```

7.1.9. reset saved-configuration

Use **reset saved-configuration** to delete a next-startup configuration file.

Syntax

reset saved-configuration [**backup** | **main**]

Views

User view

Predefined user roles

network-admin

Parameters

backup: Specifies the backup next-startup configuration file.

main: Specifies the main next-startup configuration file.

Usage guidelines

CAUTION:
This command permanently deletes the specified next-startup configuration file from all IRF member devices.

You can delete the main file, the backup file, or both.

To delete a file that is set as both main and backup next-startup configuration files, you must execute both the **reset saved-configuration backup** command and the **reset saved-configuration main** command. Using only one of the commands sets the target file attribute to NULL instead of deleting the file.

If you do not specify a configuration file attribute, the **reset saved-configuration** command deletes the main next-startup configuration file.

Examples

Delete the main next-startup configuration file.

```
<Switch> reset saved-configuration
The saved configuration file will be erased. Are you sure? [Y/N]:y
Configuration file in flash: is being cleared.
Please wait ..........
Configuration file is cleared.
```

Related commands

display saved-configuration

7.1.10. restore startup-configuration

Use **restore startup-configuration** to download a configuration file from a TFTP server and specify it as the main next-startup configuration file.

Syntax

restore startup-configuration from *ipv4-server src-filename* [**vpn-instance** *vpn-instance-name*]

Views

User view

Predefined user roles

network-admin

Parameters

ipv4-server: Specifies a TFTP server by its IPv4 address or host name. The host name is a case-insensitive string of 1 to 253 characters. Valid characters include letters, digits, hyphens (-), underscores (_), and dots (.).

src-filename: Specifies the name of the configuration file to be downloaded. The file must be a .cfg file. The file name is a case-insensitive string of up to 255 characters.

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. If the TFTP server is on the public network, do not specify this option.

Usage guidelines

Before restoring the configuration file for the next startup, make sure the following requirements are met:

- The server is reachable.
- The server is enabled with TFTP service.
- You have read and write permissions to the server.

This command downloads the configuration file to the root directory of the default storage medium on each member device and specifies the file as the main next-startup configuration file. If a partitioned USB disk is used as the default storage medium, the configuration file is saved on the first partition. Make sure all IRF members use the same type of default storage media. If a subordinate device uses a different type of default storage medium than the master, the command cannot propagate the configuration file to the subordinate device. For example, the subordinate device uses a USB disk, but the master uses a flash memory. In this situation, you must manually restore the main next-startup configuration file on the subordinate device.

Examples

Download **test.cfg** from the IPv4 TFTP server at 2.2.2.2 in the public network, and specify the file as the main next-startup configuration file.

```
<Switch> restore startup-configuration from 2.2.2.2 test.cfg
Restoring the next startup-configuration file from 2.2.2.2. Please wait...finished.
```

Download **test.cfg** from the IPv4 TFTP server at 2.2.2.2 in VPN instance **VPN1**, and specify the file as the main next-startup configuration file.

```
<Switch> restore startup-configuration from 2.2.2.2 test.cfg vpn-instance VPN1
Restoring the next startup-configuration file from 2.2.2.2. Please wait...finished.
```

Related commands

backup startup-configuration

7.1.11. save

Use **save** *file-url* [**all** | **slot** *slot-number*] to save the running configuration to a configuration file, without specifying the file as a next-startup configuration file.

Use **save** [**safely**] [**backup** | **main**] [**force**] to save the running configuration to a file in the root directory of the storage medium. This command automatically saves the file on each IRF member device and specifies the file as a next-startup configuration file.

Syntax

save *file-url* [**all** | **slot** *slot-number*]

save [**safely**] [**backup** | **main**] [**force**]

Views

Any view

Predefined user roles

network-admin

Parameters

file-url: Specifies a file path, a string of up to 255 characters. The file must be a .cfg file. If you specify the **all** keyword or the **slot** *slot-number* option, the file path cannot include a member ID. If the file path includes a folder name, the folder must already exist on all IRF member devices.

all: Saves the running configuration to all member devices. If you do not specify this keyword or the **slot** *slot-number* option, the command saves the running configuration only to the master.

slot *slot-number*: Specifies a subordinate device by its member ID. If you do not specify a subordinate device or the **all** keyword, this command saves the running configuration only to the master.

safely: Saves the configuration file in safe mode. If you do not specify this keyword, the device saves the configuration file in fast mode.

backup: Saves the running configuration to a configuration file, and specifies the file as the backup next-startup configuration file. If you do not specify this keyword or the **main** keyword, the command specifies the saved file as the main next-startup configuration file.

main: Saves the running configuration to a configuration file, and specifies the file as the main next-startup configuration file. If you do not specify this keyword or the **backup** keyword, the command specifies the saved file as the main next-startup configuration file.

force: Saves the running configuration to the existing next-startup configuration file without prompting for confirmation. If you do not specify this keyword, the system prompts you to confirm the operation. If you do not confirm the operation within 30 seconds, the system automatically aborts the operation. If you enter **Y** within the time limit, you can continue the save process and change the target file name during the process.

Usage guidelines

If the file specified for this command does not exist, the system creates the file before saving the configuration. If the file already exists, the system prompts you to confirm whether to overwrite the file. If you choose to not overwrite the file, the system cancels the save operation.

This command saves the running configuration to an .mdb binary file as well as a .cfg text file. The two files use the same file name. An .mdb file takes less time to load than a .cfg file.

When you use the **save** [**safely**] [**backup** | **main**] [**force**] command, follow these guidelines:

- In safe mode, the system saves configuration in a temporary file and starts overwriting the target next-startup configuration file after the save operation is complete. If a reboot, power failure, or out of memory or storage space event occurs during the save operation, the next-startup configuration file is retained.
- In fast mode, the device directly overwrites the target next-startup configuration file. If a reboot, power failure, or out of memory or storage space event occurs during this process, all settings in the next-startup configuration file are lost.

Safe mode is slower than fast mode, but more secure. As a best practice, specify the **safely** keyword for reliable configuration saving.

Examples

Save the running configuration to **backup.cfg**, without specifying the file as a next-startup configuration file.

```
<Switch> save backup.cfg
The current configuration will be saved to flash:/backup.cfg. Continue? [Y/N]:y
Now saving current configuration to the device.
Saving configuration flash:/backup.cfg. Please wait...
Configuration is saved to device successfully.
```

Save the running configuration to the main next-startup configuration file without any confirmation required.

```
<Switch> save force
Validating file. Please wait....
Saved the current configuration to mainboard device successfully.
```

Save the running configuration to a file in the root directory of the default storage medium, and specify the file as the main next-startup configuration file.

Before V7.2.18 :

```
<Switch> save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/backup.cfg]
(To leave the existing filename unchanged, press the enter key):test.cfg
Validating file. Please wait.....
```

Saved the current configuration to mainboard device successfully.

After V7.3.21 :

[Switch] save

```
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/ startup.cfg]
(To leave the existing filename unchanged, press the enter key):
Validating file. Please wait...
The startup.cfg file already exists.
Compared with the startup.cfg file, The current configuration adds 0 commands and deletes
0 commands.
If you want to see the configuration differences, please cancel this operation, and then
use the display diff command to show the details.
If you continue the save operation, the file will be overwritten.
Are you sure you want to continue the save operation? [Y/N]:y
Saving the current configuration to the file. Please wait...
Saved the current configuration to mainboard device successfully.
Compared with the startup.cfg file, The current configuration adds 0 commands and deletes
0 commands.
If you want to see the configuration differences, please cancel this operation, and then
use the display diff command to show the details.
If you continue the save operation, the file will be overwritten.
Are you sure you want to continue the save operation? [Y/N]:y
Saving the current configuration to the file. Please wait...
Saved the current configuration to mainboard device successfully.
```

Related commands

display current-configuration

display saved-configuration

7.1.12. startup saved-configuration

Use **startup saved-configuration** to specify a file as a next-startup configuration file.

Use **undo startup saved-configuration** to configure the system to start up with the factory defaults at the next startup.

Syntax

startup saved-configuration *cfgfile* [**backup** | **main**]

undo startup saved-configuration

Default

No next-startup configuration files are specified.

Views

User view

Predefined user roles

network-admin

Parameters

cfgfile: Specifies the path of a configuration file, a string of up to 255 characters. The file must be a .cfg file. The file path can include only the file name, or the storage medium information and file name. If the file is not on the default storage medium, you must specify the file name with storage medium information.

backup: Specifies the configuration file as the backup next-startup configuration file.

main: Specifies the configuration file as the main next-startup configuration file. This is the primary configuration file that the device attempts to load at startup. If the loading attempt fails, the device tries the backup next-startup configuration file.

Usage guidelines

CAUTION:
In an IRF fabric, the **undo startup saved-configuration** command can cause an IRF split after the IRF fabric or an IRF member reboots.

The **startup saved-configuration** command applies to all IRF members. To successfully execute this command, make sure the specified file has been saved in the root directory of the storage medium on each member.

If you do not specify the **backup** or **main** keyword, the **startup saved-configuration** command specifies the main next-startup configuration file.

As a best practice, specify different files as the main and backup next-startup configuration files.

The **undo startup saved-configuration** command changes the file attribute of the main and backup next-startup configuration files to NULL. However, the command does not delete the two configuration files.

You can also specify a configuration file as a next startup file when you use the **save** command to save the running configuration.

Examples

Specify the main next-startup configuration file.

```
<Switch> startup saved-configuration testcfg.cfg
Please wait ....... Done.
```

Related commands

display startup

Contents

A page of this section is **1-x-x**

8. Software upgrade commands 8-1
8.1. Software upgrade commands 8-1
8.1.1. boot-loader file 8-1
8.1.2. bootrom update 8-3
8.1.3. display boot-loader 8-4

8. Software upgrade commands

8.1. Software upgrade commands

As a best practice, store the startup images in a fixed storage medium. If you store the startup images in a hot swappable storage medium, do not remove the hot swappable storage medium during the startup process.

8.1.1. boot-loader file

Use **boot-loader file** to specify startup image files.

Syntax

boot-loader file boot *filename* **system** *filename* [**feature** *filename*&<1-30>] { **all** | **slot** *slot-number* } { **backup** | **main** }

boot-loader file *ipe-filename* { **all** | **slot** *slot-number* } { **backup** | **main** }

Views

User view

Predefined user roles

network-admin

Parameters

boot: Specifies a boot image file.

system: Specifies a system image file.

feature: Specifies a space-separated list of up to 30 feature image files.

filename: Specifies a .bin file in the *filesystemname*/*filename*.**bin** format. The file must be stored in the root directory of a file system on the device. Excluding the file system location section (if any), the value string can have a maximum of 63 characters. For more information about specifying a file, see *Fundamentals Configuration Guide*.

ipe-filename: Specifies an .ipe image package file in the *filesystemname*/*filename*.**ipe** format. The file must be stored in the root directory of a file system on the device. Excluding the file system location section (if any), the value string can have a maximum of 63 characters. For more information about specifying a file, see *Fundamentals Configuration Guide*.

all: Specifies all IRF member devices.

slot *slot-number*: Specifies the IRF member ID of a member device.

backup: Specifies the files as backup startup image files. Backup images are used only when main images are not available.

main: Specifies the files as main startup image files. The device always first attempts to start up with main startup files.

Usage guidelines

The **boot-loader file** command overwrites the entire startup image list. To add new startup feature images, specify all feature image files in the old startup image list, including feature image files. The new startup image list will contain only the feature image files that are specified in the command.

To load the specified startup software images, you must reboot the system.

If the upgrade images are not found in the file system on the slot specified to upgrade, the system automatically copies the images to that file system. The destination directory is the root directory of the file system. If the destination root directory already contains a startup image with the same name as an upgrade image, you must choose whether to overwrite the image.

Examples

Specify **flash:/all.ipe** as the main startup image file for IRF member device 1.

```
<Switch> boot-loader file flash:/all.ipe slot 1 main
Verifying the file flash:/all.ipe on slot 1.....Done.
NEC QX-S5624GT-4X1C images in IPE:
  boot.bin
  system.bin
This command will set the main startup software images. Continue? [Y/N]:Y
Add images to slot 1.
File flash:/boot.bin already exists on slot 1.
File flash:/system.bin already exists on slot 1.
Overwrite the existing files? [Y/N]:Y
Decompressing file boot.bin to flash:/boot.bin.....Done.
Decompressing file system.bin to flash:/system.bin.....Done.
Verifying the file flash:/boot.bin on slot 1...Done.
Verifying the file flash:/system.bin on slot 1.....Done.
The images that have passed all examinations will be used as the main startup software
images at the next reboot on slot 1.
```

Specify **flash:/all.ipe** as the main startup image file for all IRF member devices.

```
<Switch> boot-loader file slot1#flash:/all.ipe all main
Verifying the file flash:/all.ipe on slot 1.....Done.
NEC QX-S5624GT-4X1C Switch images in IPE:
  boot.bin
  system.bin
This command will set the main startup software images. Continue? [Y/N]:y
Add images to slot 1.
File flash:/boot.bin already exists on slot 1.
File flash:/system.bin already exists on slot 1.
Overwrite the existing files? [Y/N]:y
Decompressing file boot.bin to flash:/boot.bin.....Done.
Decompressing file system.bin to flash:/system.bin.....Done.
The images that have passed all examinations will be used as the main startup software
images at the next reboot on slot 1.
File flash:/boot.bin already exists on slot 2.
Do you want to overwrite the file?
 Y: Overwrite the file.
 N: Not overwrite the file.
 A: From now on, overwrite or not overwrite without prompt.
Please make a choice. [Y/N/A]:a
What type of overwrite operation do you want to perform?
 Y: Overwrite without prompt.
 N: Not overwrite or display prompt.
```

```
 Q: Return to the previous step.
Please make a choice. [Y/N/Q]:y
An existing file will be overwritten without prompt if it has the same name as any upgrade
file.
Loading.....................Done.
Loading.....................Done.
Loading.....................Done.
Loading.....................Done.
Loading.....................Done.
Loading.....................Done.
The images that have passed all examinations will be used as the main startup software
images at the next reboot on slot 2.
The images that have passed all examinations will be used as the main startup software
images at the next reboot on slot 3.
Decompression completed.
Do you want to delete flash:/all.ipe now? [Y/N]:n
```

Related commands

display boot-loader

8.1.2. bootrom update

Use **bootrom update** to load the BootWare image from a file system to the Normal BootWare area.

Syntax

bootrom update file *file* **slot** *slot-number-list*

Views

User view

Predefined user roles

network-admin

Parameters

file *file*: Specifies the file that contains the BootWare image. The *file* argument represents the file name, a string of 1 to 63 characters.

slot *slot-number-list*: Specifies a space-separated list of up to seven slot number items. An item specifies an IRF member device by its member ID or a range of IRF member devices in the form of *start-slot-number* **to** *end-slot-number*. The end slot number must be equal to or greater than the start slot number.

Usage guidelines

BootWare images are contained in the .bin Comware boot image file. You can specify a Comware boot image file in this command to upgrade the BootWares in the system before you upgrade the Comware images. If you do not upgrade BootWares before upgrading Comware images, the system automatically upgrades BootWares as necessary when loading Comware images.

The new BootWare images take effect after you reboot the device.

Examples

Use the file **a.bin** in the root directory of the flash memory to upgrade the BootWare image.

```
<Switch> bootrom update file flash:/a.bin slot 1
```

```
This command will update the Boot ROM file on the specified board(s), Continue? [Y/N]:y
Now updating the Boot ROM, please wait.............Done.
```

Related commands

boot-loader file

8.1.3. display boot-loader

Use **display boot-loader** to display current software images and startup software images.

Syntax

display boot-loader [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies the member ID of an IRF member device. If you do not specify a member device, this command displays the software images on each IRF member device.

Examples

Display the current software images and startup software images.

```
<Switch> display boot-loader
Software images on slot 1:
Current software images:
  flash:/boot.bin
  flash:/system.bin
Main startup software images:
  flash:/boot.bin
  flash:/system.bin
Backup startup software images:
  flash:/boot.bin
  flash:/system.bin
```

Table 8-1 Command output

Field	Description
Current software images	Comware images that have been loaded.
Main startup software images	Primary Comware images for the next startup.
Backup startup software images	Backup Comware images for the next startup.

Related commands

boot-loader file

Contents

A page of this section is **1-x-x**

9. ISSU commands 9-1
9.1. ISSU commands 9-1
9.1.1. display issu rollback-timer 9-1
9.1.2. display issu state 9-1
9.1.3. display version comp-matrix file 9-4
9.1.4. issu accept 9-5
9.1.5. issu commit 9-6
9.1.6. issu load 9-7
9.1.7. issu rollback 9-9
9.1.8. issu rollback-timer 9-10
9.1.9. issu run switchover 9-11

9. ISSU commands

9.1. ISSU commands

9.1.1. display issu rollback-timer

Use **display issu rollback-timer** to display automatic rollback timer information.

Syntax

display issu rollback-timer

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

Change to the automatic rollback interval does not take effect on the ongoing ISSU process. The current remaining rollback time might be greater than the specified automatic rollback interval.

Examples

Display automatic rollback timer information after the **issu run switchover** command is executed.

```
<Switch> display issu rollback-timer
Rollback timer: Working
Rollback interval: 45 minutes
Rollback time remaining : 40 minutes
```

Display automatic rollback timer information after the **issu accept** command is executed.

```
<Switch> display issu rollback-timer
Rollback timer: Not working
Rollback interval: 30 minutes
```

Display automatic rollback timer information when no ISSU process is taking place.

```
<Switch> display issu rollback-timer
Rollback timer: Not working
Rollback interval: 45 minutes
```

Related commands

issu rollback-timer

9.1.2. display issu state

Use **display issu state** to display ISSU status information.

Syntax

display issu state

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

During an ISSU that uses **issu** commands, you can use this command to verify the ISSU status and determine what to do next.

This command does not apply to an ISSU that uses **install** commands, because the ISSU state machine is not involved.

Examples

Display ISSU status information when no upgrade is taking place.

```
<Switch> display issu state
ISSU state: Init
Compatibility: Unknown
Work state: Normal
Upgrade method: Card by card
Upgraded slot: None
Current upgrading slot: None
Current version list:
  boot: 7.1.070, Test 0001015
  system: 7.1.070, Test 0001015
  feature1: 7.1.070, Test 0001015
Current software images:
  flash:/boot-t0001015.bin
  flash:/system-t0001015.bin
  flash:/feature1-t0001015.bin
```

Display ISSU status information while the **issu load** command is being executed.

```
<Switch> display issu state
ISSU state: Loading
Compatibility: Incompatible
Work state: Normal
Upgrade method: Card by card
Upgraded slot: None
Current upgrading slot:
  slot 1
Previous version list:
  boot: 7.1.070, Test 0001015
  system: 7.1.070, Test 0001015
  feature1: 7.1.070, Test 0001015
Previous software images:
  flash:/boot-t0001015.bin
  flash:/system-t0001015.bin
  flash:/feature1-t0001015.bin
Upgrade version list:
```

```
  boot: 7.1.070, Test 0001016
  system: 7.1.070, Test 0001016
  feature1: 7.1.070, Test 0001016
Upgrade software images:
  flash:/boot-t0001016.bin
  flash:/system-t0001016.bin
  flash:/feature1-t0001016.bin
```

Table 9-1 Command output

Field	Description
ISSU state	ISSU status: • **Init**—The ISSU process has not started or has finished. • **Loading**—The system is executing the **issu load** command. • **Loaded**—The **issu load** command is completed. • **Switching**—The system is executing the **issu run switchover** command. • **Switchover**—The **issu run switchover** command is completed. • **Accepted**—The **issu accept** command is completed. • **Committing**—The system is executing the **issu commit** command. • **Rollbacking**—A rollback is in progress. • **Unknown**—An upgrade is in progress. This value is displayed if you execute the command on an original subordinate member.
Compatibility	Version compatibility: • **Compatible**—Upgrade to a compatible version. • **Incompatible**—Upgrade to an incompatible version. • **Unknown**—No upgrade is in progress.
Work state	Operating status of the device: • **Normal**—The device is operating correctly. • **Independent active**—When you perform an ISSU to an incompatible version, a subordinate member that is upgraded first enters this state. In this state, member devices are not running the same software versions.
Upgrade method	Upgrade mode. The value of this field is fixed at **Card by card**. In this mode, member devices are upgraded one by one.
Upgraded slot	Upgraded members. During a rollback, this field displays **Unknown**.
Current upgrading slot	Members that are being upgraded. During a rollback, this field displays **Unknown**.
Current version list	Versions of currently running images. This field is displayed if no upgrade is taking place.
Current software images	File names of currently running images. This field is displayed if no upgrade is taking place.
Previous version list	Versions of the images that were running on the device before the ISSU. If you execute the command on an original subordinate member while the member is being upgraded to an incompatible version, this field

Field	Description
	displays **Unknown**.
Previous software images	File names of the images that were running on the device before the ISSU. If you execute the command on an original subordinate member while the member is being upgraded to an incompatible version, this field displays **Unknown**.
Upgrade version list	Versions of the upgrade images. If you execute the command on an original subordinate member while the member is being upgraded to an incompatible version, this field displays **Unknown**.
Upgrade software images	File names of the upgrade images. If you execute the command on an original subordinate member while the member is being upgraded to an incompatible version, this field displays **Unknown**.

Related commands

issu accept

issu commit

issu load

issu rollback

issu run switchover

9.1.3. display version comp-matrix file

Use **display version comp-matrix file** to display the recommended ISSU methods.

Syntax

display version comp-matrix file { **boot** *filename* | **system** *filename* } *

display version comp-matrix file ipe *ipe-filename*

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

boot: Specifies a boot image file.

system: Specifies a system image file.

filename: Specifies a .bin file in the *filesystemnamelfilename***.bin** format. The file must be stored in the root directory of a file system on the device. The value string excluding the file system location section (if any) can have a maximum of 63 characters. For more information about specifying a file, see file system management in *Fundamentals Configuration Guide.*

ipe-filename: Specifies an .ipe file in the *filesystemnamelfilename***.ipe** format. The file must be stored in the root directory of a file system on the device. The value string excluding the file system

location section (if any) can have a maximum of 63 characters. For more information about specifying a file, see file system management in *Fundamentals Configuration Guide.*

Usage guidelines

If one or more images are incompatible, the incompatible upgrade method applies. The entire system needs to be rebooted during an incompatible upgrade.

Examples

Display the recommended ISSU methods. In this example, the specified images are compatible with the running images.

```
<Switch> display version comp-matrix file boot flash:/boot-t0001015.bin system
flash:/system-t0001015.bin feature flash:/feature1-t0001015.bin
Verifying the file flash:/feature1-t0001015.bin on slot 1.....Done.
Verifying the file flash:/boot-t0001015.bin on slot 1.....Done.
Verifying the file flash:/system-t0001015.bin on slot 1.....Done.
Identifying the upgrade methods.........Done.

  Slot     Upgrade Way
  1        File Upgrade
```

Table 9-2 Command output

Field	Description
Verifying the file	The system was verifying the validity of the file.
Upgrade Way	ISSU method: • **Service Upgrade**. • **File Upgrade**. • **Reboot**. This field is displayed only for compatible versions. For more information about ISSU methods, see *Fundamentals Configuration Guide*.
Influenced service according to following table	Services that will be affected by the upgrade. This field is displayed only for compatible versions.

Related commands

issu load

9.1.4. issu accept

Use **issu accept** to accept the upgrade to a compatible version and delete the automatic rollback timer.

Syntax

issu accept

Views

User view

Predefined user roles

network-admin

Usage guidelines

The system cannot perform automatic rollback for the ISSU process after you execute this command. However, you can use the **issu rollback** command to perform a manual rollback.

The **issu accept** command does not apply to an ISSU to an incompatible version.

Examples

Accept the upgrade to a compatible version.

```
<Switch> issu accept
```

Related commands

issu load

issu run switchover

9.1.5. issu commit

Use **issu commit** to upgrade the original master and the subordinate members that have not been upgraded and complete the ISSU upgrade.

Syntax

issu commit slot *slot-number*

Views

User view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies the member ID of the original master or a subordinate member that has not been upgraded.

Usage guidelines

At reboot, a subordinate device automatically synchronizes the master device's configuration and status data. You must wait for the synchronization to complete before using the **issu commit** command on the subordinate device. To identify whether the synchronization is complete, use the **display system stable state** command. The synchronization is complete if the **System State** field displays **Stable**.

Use this command to upgrade the original master and the subordinate members that have not been upgraded, one by one. You must wait for one upgraded member to start up again and join the IRF fabric before upgrading another member. After all members are upgraded, the ISSU status changes to Init, and the ISSU process ends and cannot be rolled back.

Examples

After member 2 is upgraded and becomes the new master, upgrade the original master (member 3) and the other subordinate members that have not been upgraded (member 4 and member 1).

```
<Switch> issu commit slot 3
Upgrade summary according to following table:

flash:/feature1.bin
  Running Version              New Version
  Test 0001015                 Test 0001016
```

```
  Slot                        Upgrade Way
  3                           Service Upgrade
Upgrading software images to compatible versions. Continue? [Y/N]:y
This operation might take several minutes, please wait...Done.
<Switch> issu commit slot 4
Verifying the file flash:/feature1.bin on slot 4..............Done.
Copying file flash:/feature1.bin to slot4#flash:/feature1.bin...Done.
Upgrade summary according to following table:

flash:/feature1.bin
  Running Version             New Version
  Test 0001015                Test 0001016

  Slot                        Upgrade Way
  4                           Service Upgrade
Upgrading software images to compatible versions. Continue? [Y/N]:y
This operation might take several minutes, please wait...Done.
<Switch> issu commit slot 1
Verifying the file flash:/feature1.bin on slot 1..............Done.
Copying file flash:/feature1.bin to slot1#flash:/feature1.bin...Done.
Upgrade summary according to following table:

flash:/feature1.bin
  Running Version             New Version
  Test 0001015                Test 0001016

  Slot                        Upgrade Way
  1                           Service Upgrade
Upgrading software images to compatible versions. Continue? [Y/N]:y
This operation might take several minutes, please wait...Done.
```

For information about the command output, see Table 9-2 .

Related commands

issu accept

issu load

issu run switchover

9.1.6. issu load

Use **issu load** to upgrade the software images of subordinate members and configure the new images as main startup software images for those members.

Syntax

issu load file { **boot** *filename* | **system** *filename*| **feature** *filename*&<1-30> } * **slot** *slot-number*&<1-9>

issu load file ipe *ipe-filename* **slot** *slot-number*&<1-9>

Views

User view

Predefined user roles

network-admin

Parameters

boot: Specifies a boot image file.

system: Specifies a system image file.

feature: Specifies a space-separated list of up to 30 feature image files.

filename: Specifies a .bin file in the *filesystemname*/*filename***.bin** format. The file must be stored in the root directory of a file system on the master device. The value string excluding the file system location section (if any) can have a maximum of 63 characters. For more information about specifying a file, see file system management in *Fundamentals Configuration Guide.*

ipe-filename: Specifies an .ipe file in the *filesystemname*/*filename***.ipe** format. The file must be stored in the root directory of a file system on the master device. The value string excluding the file system location section (if any) can have a maximum of 63 characters. For more information about specifying a file, see file system management in *Fundamentals Configuration Guide.*

slot *slot-number*: Specifies the member ID of a subordinate member. You can specify a space-separated list of up to nine member IDs. On a single-chassis IRF fabric, enter the member ID of the member device to upgrade the entire fabric. On a multichassis IRF fabric, you can specify only one member ID for a compatible upgrade and can specify multiple member IDs for an incompatible upgrade. As a best practice, specify half of the subordinate members if the member devices form a ring. Make sure the specified subordinate members are directly connected by physical links.

Usage guidelines

You may upgrade all or some of the software images. If you are upgrading only some of the images, make sure the new images are compatible with the images that are not to be upgraded. The upgrade will fail if a conflict exists.

This command performs the following operations:

- Checks the version compatibility.
- Identifies the upgrade method.
- Loads the new images to upgrade the member devices.
- Sets the new images as the main startup software images so the upgrade can survive a reboot.

At reboot, a subordinate device automatically synchronizes the master device's configuration and status data. You must wait for the synchronization to complete before using the **issu load** command on the subordinate device. To identify whether the synchronization is complete, use the **display system stable state** command. The synchronization is complete if the **System State** field displays **Stable**.

Examples

Upgrade member device 1 (a subordinate member) with system image file **flash:/ soft-system-V714.bin**, boot image file **flash:/ soft-boot-V714.bin** and feature image file **soft-freeradius-V714.bin**. (In this example, the image is compatible with the running images.)

<Switch> issu load file boot flash:/soft-boot-V714.bin system flash:/soft-system-V714.bin feature flash:/soft-freeradius-V714.bin slot 1

```
This operation will delete the rollback point information for the previous upgrade and
maybe get unsaved configuration lost. Continue? [Y/N]:y
Verifying the file flash:/soft-freeradius-V714.bin on slot 1...Done.
Verifying the file flash:/soft-boot-V714.bin on slot 1...Done.
```

```
Verifying the file flash:/soft-system-V714.bin on slot 1........Done.
Identifying the upgrade methods...Done.
Upgrade summary according to following table:

flash:/soft-boot-V714.bin
  Running Version             New Version
  7.1.3                       7.1.4

flash:/soft-system-V714.bin
  Running Version             New Version
  7.1.3                       7.1.4

flash:/soft-freeradius-V714.bin
  Running Version             New Version
  7.1.3                       7.1.4

  Slot                        Upgrade Way
  1                           Reboot
Upgrading software images to compatible versions. Continue? [Y/N]:y
This operation might take several minutes, please wait.....
```

Table 9-3 Command output

Field	Description
Verifying the file	The system was verifying the validity of the file.
Copying file	The system was copying the upgrade file to a subordinate member. This field is displayed if you specified a subordinate member for the command.
Upgrade Way	ISSU method: • **Service Upgrade**. • **File Upgrade**. • **Reboot**. This field is displayed only for an upgrade to a compatible version. For more information about ISSU methods, see *Fundamentals Configuration Guide*.

NOTE:

When you upgrade the software by ISSU, you cannot upgrade only the boot package and system package, and you must upgrade the Freeradius package at the same time. Please use **issu load file boot** *filename* **system** *filename* **feature** *filename* **slot** *slot-number* command.

QX-S5600G series does not support the Radius server feature.

9.1.7. issu rollback

Use **issu rollback** to cancel the ISSU and roll back to the original software versions.

Syntax

issu rollback

Views

User view

Predefined user roles

network-admin

Usage guidelines

The device supports automatic rollback and manual rollback. This command performs a manual rollback.

You can perform a manual rollback while an ISSU is in one of the following states:

- Loaded.
- Switching (during an upgrade to a compatible version).
- Switchover (during an upgrade to a compatible version).
- Accepted.

If the ISSU is in Loading state, the rollback might fail. Use the **display version** command to examine the rollback result after the rollback is completed.

If a rollback occurs while an ISSU is in Switching state, the entire system reboots automatically.

A rollback performed for a multichassis IRF fabric after you execute the **issu run switchover** command cancels all operations performed during the ISSU process, including the master/subordinate switchover.

Examples

Roll back to the original software versions.

```
<Switch> issu rollback
This command will quit the ISSU process and roll back to the previous version. Continue? [Y/N]:y
```

Related commands

issu accept

issu commit

issu load

issu run switchover

9.1.8. issu rollback-timer

Use **issu rollback-timer** to set the automatic rollback timer.

Use **undo issu rollback-timer** to restore the default.

Syntax

issu rollback-timer *minutes*

undo issu rollback-timer

Default

The automatic rollback timer is set to 45 minutes.

Views

System view

Predefined user roles

network-admin

Parameters

minutes: Specifies the automatic rollback interval in minutes. The value range is 0 to 120. Setting it to 0 disables automatic rollback.

Usage guidelines

The automatic software version rollback feature is available only during an ISSU to a compatible version when the IRF fabric has multiple members.

The system starts the automatic rollback timer when you execute the **issu run switchover** command in a scenario where automatic rollback is supported. If you do not execute the **issu accept** or **issu commit** command before the timer expires, the system automatically rolls back to the software version used before the ISSU.

Change to the automatic rollback interval does not take effect on the ongoing ISSU process.

Examples

Set the automatic rollback timer to 50 minutes.

```
<Switch> system-view
[Switch] issu rollback-timer 50
```

Related commands

issu rollback

9.1.9. issu run switchover

Use **issu run switchover** to perform an ISSU switchover.

Syntax

issu run switchover

Views

User view

Predefined user roles

network-admin

Usage guidelines

Use this command on a multichassis IRF fabric.

- For a compatible upgrade, this command performs operations depending on the ISSU method.
  - **Incremental upgrade**—Performs a process-level master/subordinate switchover for the processes to be upgraded.
  - **Reboot upgrade**—Reboots the current master with the old software version, causing the upgraded subordinate member to be elected as the new master.
- For an incompatible upgrade, the **issu load** command splits the IRF fabric into two fabrics, with the upgraded members forming a new fabric. The **issu run switchover** command reboots the members in the old IRF fabric with the upgrade images to upgrade the members. After startup, the members join the new IRF fabric as subordinate members.

At reboot, a subordinate device automatically synchronizes the master device's configuration and status data. You must wait for the synchronization to complete before using the **issu run switchover** command on the subordinate device. To identify whether the synchronization is

complete, use the **display system stable state** command. The synchronization is complete if the **System State** field displays **Stable**.

When you execute the **issu run switchover** command during an ISSU to a compatible version, the system starts the automatic rollback timer. If you do not execute the **issu accept** or **issu commit** command before the timer expires, the system automatically rolls back to the original software versions.

Examples

On a multichassis IRF fabric, perform a master/subordinate switchover during an ISSU to a compatible version.

```
<Switch> issu run switchover
Upgrade summary according to following table:

flash:/feature1.bin
  Running Version             New Version
  Test 0001015                Test 0001016

  Slot                        Switchover Way
  1                           Active standby process switchover
Upgrading software images to compatible versions. Continue? [Y/N]:y
This operation might take several minutes, please wait...Done.
```

On a multichassis IRF fabric, perform a master/subordinate switchover, and upgrade members that have not been upgraded (member 1 and member 2) during an ISSU to an incompatible version.

```
<Switch> issu run switchover
Upgrade summary according to following table:

flash:/feature1.bin
  Running Version             New Version
  Test 0001015                Test 0001016

  Slot                        Upgrade Way
  1                           Reboot
  2                           Reboot
Upgrading software images to incompatible versions. Continue? [Y/N]:y
This operation might take several minutes, please wait...Done.
```

Table 9-4 Command output

Field	Description
Switchover Way	Switchover method: • **Active standby process switchover**—Switch from the active process to the standby process. • **Master subordinate switchover**—Switch from the master to a subordinate member.

For more information about the command output, see Table 9-2 .

Related commands

issu load

Contents

A page of this section is **1-x-x**

10. Device management commands ····· 10-1
10.1. Device management commands ····· 10-1
10.1.1. clock datetime ····· 10-1
10.1.2. clock protocol ····· 10-2
10.1.3. clock summer-time ····· 10-2
10.1.4. clock timezone ····· 10-4
10.1.5. command ····· 10-5
10.1.6. copyright-info enable ····· 10-6
10.1.7. display clock ····· 10-6
10.1.8. display cpu-usage ····· 10-7
10.1.9. display cpu-usage configuration ····· 10-8
10.1.10. display cpu-usage history ····· 10-9
10.1.11. display device ····· 10-10
10.1.12. display device manuinfo ····· 10-11
10.1.13. display diagnostic-information ····· 10-12
10.1.14. display environment ····· 10-13
10.1.15. display fan ····· 10-14
10.1.16. display memory ····· 10-15
10.1.17. display memory-threshold ····· 10-17
10.1.18. display power ····· 10-18
10.1.19. display resource-monitor ····· 10-19
10.1.20. display scheduler job ····· 10-20
10.1.21. display scheduler logfile ····· 10-21
10.1.22. display scheduler reboot ····· 10-21
10.1.23. display scheduler schedule ····· 10-22
10.1.24. display switch-mode status ····· 10-23
10.1.25. display transceiver alarm ····· 10-24
10.1.26. display transceiver diagnosis ····· 10-25
10.1.27. display transceiver interface ····· 10-26
10.1.28. display transceiver manuinfo ····· 10-27
10.1.29. display version ····· 10-27
10.1.30. dying-gasp host ····· 10-28
10.1.31. dying-gasp source ····· 10-29
10.1.32. fan prefer-direction ····· 10-30
10.1.33. header ····· 10-31
10.1.34. job ····· 10-32
10.1.35. memory-threshold ····· 10-32
10.1.36. monitor cpu-usage enable ····· 10-34
10.1.37. monitor cpu-usage interval ····· 10-34
10.1.38. monitor cpu-usage threshold ····· 10-35
10.1.39. monitor resend cpu-usage ····· 10-36
10.1.40. monitor resend memory-threshold ····· 10-37
10.1.41. parity-error monitor log enable ····· 10-38
10.1.42. parity-error monitor period ····· 10-39
10.1.43. parity-error monitor threshold ····· 10-39
10.1.44. password-recovery enable ····· 10-40
10.1.45. reboot ····· 10-41
10.1.46. reset scheduler logfile ····· 10-42
10.1.47. resource-monitor minor resend enable ····· 10-42
10.1.48. resource-monitor output ····· 10-43
10.1.49. resource-monitor resource ····· 10-44
10.1.50. scheduler job ····· 10-46

10.1.51. scheduler logfile size ····· 10-46
10.1.52. scheduler reboot at ····· 10-47
10.1.53. scheduler reboot delay ····· 10-48
10.1.54. scheduler schedule ····· 10-49
10.1.55. shutdown-interval ····· 10-49
10.1.56. switch-mode ····· 10-50
10.1.57. sysname ····· 10-51
10.1.58. temperature-limit ····· 10-51
10.1.59. time at ····· 10-53
10.1.60. time once ····· 10-54
10.1.61. time repeating ····· 10-55
10.1.62. usb disable ····· 10-56
10.1.63. user-role ····· 10-57

10. Device management commands

10.1. Device management commands

10.1.1. clock datetime

Use **clock datetime** to set the system time.

Syntax

clock datetime *time date*

Default

The system time is UTC time 00:00:00 01/01/2013.

Views

User view

Predefined user roles

network-admin

Parameters

time: Specifies a time in the *hh:mm:ss* format. The value range for *hh* is 0 to 23. The value range for *mm* is 0 to 59. The value range for *ss* is 0 to 59. The leading zero in a segment can be omitted. If the seconds segment is 0 (*hh*:*mm*:00), you can omit it. If both the minutes and seconds segments are 0 (*hh*:00:00), you can omit both of the segments. For example, to specify 08:00:00, you can enter 8.

date: Specifies a date in the *MM/DD/YYYY* or *YYYY/MM/DD* format. The value range for *YYYY* is 2000 to 2035. The value range for *MM* is 1 to 12. The value range for *DD* varies by month.

Usage guidelines

Correct system time is essential to network management and communication. You must configure the system time correctly before you run the device on the network.

For the device to use the local system time, execute the **clock protocol none** command and this command in turn. The specified system time takes effect immediately. Then, the device uses the clock signals generated by its built-in crystal oscillator to maintain the system time.

A device power cycling operation restores the local system time to the default. After the device is power cycled, you must execute this command again to set the local system time.

Examples

Set the system time to 08:08:08 01/01/2015.

```
<Switch> clock datetime 8:8:8 1/1/2015
```

Set the system time to 08:10:00 01/01/2015.

```
<Switch> clock datetime 8:10 2015/1/1
```

Related commands

clock protocol

clock summer-time

clock timezone

display clock

10.1.2. clock protocol

Use **clock protocol** to specify the system time source.

Use **undo clock protocol** to restore the default.

Syntax

clock protocol { **none** | **ntp** }

undo clock protocol

Default

The device obtains the UTC time from an NTP time source.

Views

System view

Predefined user roles

network-admin

Parameters

none: Uses the system time set by using the **clock datetime** command.

ntp: Uses NTP to obtain the UTC time. You must configure NTP correctly. For more information about NTP and NTP configuration, see *Network Management and Monitoring Configuration Guide*.

Usage guidelines

Correct system time is essential to network management and communication. You must configure the system time correctly before you run the device on the network.

The device can use the locally set system time, or obtain the UTC time from a time source on the network and calculate the system time.

If you configure the **clock protocol none** command, the device uses the locally set system time. The device then uses the clock signals generated by its built-in crystal oscillator to maintain the system time.

If you configure the **clock protocol ntp** command, the device obtains the UTC time through NTP and calculates the system time. The device then periodically synchronizes the UTC time and recalculates the system time.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure the device to use the local UTC time.

```
<Switch> system-view
[Switch] clock protocol none
```

10.1.3. clock summer-time

Use **clock summer-time** to set the daylight saving time.

Use **undo clock summer-time** to restore the default.

Syntax

clock summer-time *name start-time start-date end-time end-date add-time*

undo clock summer-time

Default

The daylight saving time is not set.

Views

System view

Predefined user roles

network-admin

Parameters

name: Specifies a name for the daylight saving time schedule, a case-sensitive string of 1 to 32 characters.

start-time: Specifies the start time in the *hh:mm:ss* format. The value range for *hh* is 0 to 23. The value range for *mm* is 0 to 59. The value range for *ss* is 0 to 59. The leading zero in a segment can be omitted. If the seconds segment is 0 (*hh*:*mm*:00), you can omit it. If both the minutes and seconds segments are 0 (*hh*:00:00), you can omit both of the segments. For example, to specify 08:00:00, you can enter 8.

start-date: Specifies the start date in one of the following formats:

- *MM/DD*. The value range for *MM* is 1 to 12. The value range for *DD* varies by month.
- *month week day*, where:
  - *month*—Takes **January**, **February**, **March**, **April**, **May**, **June**, **July**, **August**, **September**, **October**, **November** or **December**.
  - *week*—Represents week of the month. It takes **first**, **second**, **third**, **fourth**, **fifth**, or **last**.
  - *day*—Takes **Sunday**, **Monday**, **Tuesday**, **Wednesday**, **Thursday**, **Friday**, or **Saturday**.

end-time: Specifies the end time in the *hh:mm:ss* format. The value range for *hh* is 0 to 23. The value range for *mm* is 0 to 59. The value range for *ss* is 0 to 59. The leading zero in a segment can be omitted. If the seconds segment is 0 (*hh*:*mm*:00), you can omit it. If both the minutes and seconds segments are 0 (*hh*:00:00), you can omit both of the segments. For example, to specify 08:00:00, you can enter 8.

end-date: Specifies the end date in one of the following formats:

- *MM/DD*. The value range for *MM* is 1 to 12. The value range for *DD* varies by month.
- *month week day*, where:
  - *month*—Takes **January**, **February**, **March**, **April**, **May**, **June**, **July**, **August**, **September**, **October**, **November** or **December**.
  - *week*—Represents week of the month. It takes **first**, **second**, **third**, **fourth**, **fifth**, or **last**.
  - *day*—Takes **Sunday**, **Monday**, **Tuesday**, **Wednesday**, **Thursday**, **Friday**, or **Saturday**.

add-time: Specifies the time to be added to the standard time, in the *hh:mm:ss* format. The value range for *hh* is 0 to 23. The value range for *mm* is 0 to 59. The value range for *ss* is 0 to 59. The leading zero in a segment can be omitted. If the seconds segment is 0 (*hh*:*mm*:00), you can omit it. If both the minutes and seconds segments are 0 (*hh*:00:00), you can omit both of the segments. For example, to specify 08:00:00, you can enter 8.

Usage guidelines

Correct system time is essential to network management and communication. You must configure the system time correctly before you run the device on the network.

After you set the daylight saving time, the device recalculates the system time. To view the system time, use the **display clock** command.

Make sure all devices on the network are using the same daylight saving time as the local time.

Examples

Set the system time ahead 1 hour for the period between 06:00:00 on 08/01 and 06:00:00 on 09/01.

```
<Switch> system-view
[Switch] clock summer-time PDT 6 08/01 6 09/01 1
```

Related commands

clock datetime

clock timezone

display clock

10.1.4. clock timezone

Use **clock timezone** to set the time zone.

Use **undo clock timezone** to restore the default.

Syntax

clock timezone *zone-name* { **add** | **minus** } *zone-offset*

undo clock timezone

Default

The UTC time zone is used.

Views

System view

Predefined user roles

network-admin

Parameters

zone-name: Specifies a time zone by its name, a case-sensitive string of 1 to 32 characters.

add: Adds an offset to the UTC time.

minus: Decreases the UTC time by an offset.

zone-offset: Specifies an offset to the UTC time, in the *hh:mm:ss* format. The value range for *hh* is 0 to 23. The value range for *mm* is 0 to 59. The value range for *ss* is 0 to 59. The leading zero in a segment can be omitted. If the seconds segment is 0 (*hh*:*mm*:00), you can omit it. If both the minutes and seconds segments are 0 (*hh*:00:00), you can omit both of the segments. For example, to specify 08:00:00, you can enter 8.

Usage guidelines

Correct system time is essential to network management and communication. You must configure the system time correctly before you run the device on the network.

After you set the time zone, the device recalculates the system time. To view the system time, use the **display clock** command.

Make sure all devices on the network are using the same time zone as the local time.

Examples

Set the name of the time zone to **Z5**, and add 5 hours to the UTC time.

```
<Switch> system-view
```

```
[Switch] clock timezone Z5 add 5
```

Related commands

clock datetime

clock summer-time

display clock

10.1.5. command

Use **command** to assign a command to a job.

Use **undo command** to revoke a command.

Syntax

command *id command*

undo command *id*

Default

No command is assigned to a job.

Views

Job view

Predefined user roles

network-admin

Parameters

id: Specifies an ID for the command, in the range of 0 to 4294967295. A command ID uniquely identifies a command in a job. Commands in a job are executed in ascending order of their command IDs.

command: Specifies the command to be assigned to the job.

Usage guidelines

To assign a command (command A) to a job, you must first assign the job the command or commands for entering the view of command A.

If you specify the ID of an existing command for another command, the existing command is replaced.

Make sure all commands in a schedule are compliant to the command syntax. The system does not examine the syntax when you assign a command to a job.

If a command requires a yes or no answer, the system always assumes that a **Y** or **Yes** is entered. If a command requires a character string input, the system assumes that either the default character string (if any) or a null string is entered.

A job cannot contain the **telnet**, **ftp**, **ssh2**, or **monitor process** command.

Examples

Assign commands to the **backupconfig** job to back up the **startup.cfg** file to the TFTP server at 192.168.100.11.

```
<Switch> system-view
[Switch] scheduler job backupconfig
[Switch-job-backupconfig] command 2 tftp 192.168.100.11 put flash:/startup.cfg backup.cfg
```

Assign commands to the **shutdownGE** job to shut down GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] scheduler job shutdownGE
[Switch-job-shutdownGE] command 1 system-view
[Switch-job-shutdownGE] command 2 interface gigabitethernet 1/0/1
[Switch-job-shutdownGE] command 3 shutdown
```

Related commands

scheduler job

10.1.6. copyright-info enable

Use **copyright-info enable** to enable copyright statement display.

Use **undo copyright-info enable** to disable copyright statement display.

Syntax

copyright-info enable

undo copyright-info enable

Default

Copyright statement display is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

To use a command to enable copyright statement display.

10.1.7. display clock

Use **display clock** to display the system time, date, time zone, and daylight saving time.

Syntax

display clock

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display the system time and date when the time zone is not specified.

```
<Switch> display clock
10:09:00.258 UTC Fri 03/16/2015
```

The time is in the *hour*:*minute*:*second*.*milliseconds* format.

Display the system time and date when the time zone Z5 is specified.

```
<Switch> display clock
```

```
15:10:00.152 Z5 Fri 03/16/2015
Time Zone : Z5 add 05:00:00
```

Display the system time and date when the time zone Z5 and daylight saving time PDT are specified.

```
<Switch> display clock
15:11:00.211 Z5 Fri 03/16/2015
Time Zone : Z5 add 05:00:00
Summer Time : PDT 06:00:00 08/01 06:00:00 09/01 01:00:00
```

Related commands

clock datetime

clock timezone

clock summer-time

10.1.8. display cpu-usage

Use **display cpu-usage** to display the current CPU usage statistics.

Syntax

display cpu-usage [**slot** *slot-number* [**cpu** *cpu-number*]]

display cpu-usage [**control-plane** | **data-plane**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

control-plane: Displays CPU usage statistics for the control plane. If you do not specify this keyword or the **data-plane** keyword, the command displays the total CPU usage statistics.

data-plane: Displays CPU usage statistics for the data plane. If you do not specify this keyword or the **control-plane** keyword, the command displays the total CPU usage statistics.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays CPU usage statistics for all member devices.

cpu *cpu-number*: Specifies a CPU by its number. The *cpu-number* argument must be 0.

IMPORTANT:

- If you do not specify the **control-plane** keyword or the **data-plane** keyword, the command displays the total CPU usage statistics.
- Maximum of the total CPU usage statistics is 100%.
- If control-plane is 45% and data-plane is 5%, total CPU usage statistics is 25%.

Examples

Display the current CPU usage statistics in text form.

```
<Switch> display cpu-usage
Slot 1 CPU 0 CPU usage:
```

```
        1% in last 5 seconds
        1% in last 1 minute
        1% in last 5 minutes
```

Display the current CPU usage statistics in table form.

```
<Switch> display cpu-usage
Slot CPU        Last 5 sec        Last 1 min        Last 5 min
1    0          17%               29%               28%
```

Table 10-1 Command output

Field	Description
x% in last 5 seconds Last 5 sec	Average CPU or CPU core usage during the most recent 5-second interval.
y% in last 1 minute Last 1 min	Average CPU or CPU core usage during the most recent 1-minute interval.
z% in last 5 minutes Last 5 min	Average CPU or CPU core usage during the most recent 5-minute interval.

10.1.9. display cpu-usage configuration

Use **display cpu-usage configuration** to display CPU usage monitoring settings.

Syntax

display cpu-usage configuration [**slot** *slot-number* [**cpu** *cpu-number*]]

Views

Any view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays the CPU usage monitoring settings for the master device.

cpu *cpu-number*: Specifies a CPU by its number. The *cpu-number* argument must be 0.

Examples

Display the CPU usage monitoring settings.

```
<Switch> display cpu-usage configuration
CPU usage monitor is enabled.
Current monitor interval is 60 seconds.
Current severe alarm threshold is 90%.
Current minor alarm threshold is 80%.
Current recovery-threshold is 40%.
```

Related commands

monitor cpu-usage enable

monitor cpu-usage interval

monitor cpu-usage threshold

10.1.10. display cpu-usage history

Use **display cpu-usage history** to display the historical CPU usage statistics in a coordinate system.

Syntax

display cpu-usage history [**job** *job-id*] [**slot** *slot-number* [**cpu** *cpu-number*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

job *job-id*: Specifies a process by its ID. The value range for *job-id* is 1 to 2147483647. If you do not specify a process, this command displays the statistics for the entire system's CPU usage (the total CPU usage of all processes). To view the IDs and names of the running processes, use the **display process** command. For more information, see *Network Management and Monitoring Configuration Guide*.

slot *slot-number*: Specifies an IRF member device by its member ID. If you specify a process but do not specify a member device, this command displays the statistics for the process on the master device. If you do not specify any options, this command displays the statistics for all processes on all member devices.

cpu *cpu-number*: Specifies a CPU by its number. The *cpu-number* argument must be 0. If you specify a process but do not specify a CPU, this command displays the statistics for the default CPU. If you do not specify a process or CPU, this command displays the historical statistics for all CPUs.

Usage guidelines

After CPU usage monitoring is enabled, the system regularly samples CPU usage and saves the samples to the history record buffer. This command displays the most recent 60 samples in a coordinate system as follows:

The vertical axis represents the CPU usage. If a statistic is not a multiple of the usage step, it is rounded up or down to the closest multiple of the usage step. For example, if the CPU usage step is 5%, the statistic 53% is rounded up to 55%, and the statistic 52% is rounded down to 50%.

The horizontal axis represents the time.

Pound signs (#) indicate the CPU usage. The value on the vertical axis for the topmost pound sign at a specific time represents the CPU usage at that time.

Examples

Display the historical CPU usage statistics.

```
<Switch> display cpu-usage history
100%|
 95%|
 90%|
 85%|
 80%|
 75%|
 70%|
```

```
 65%|
 60%|
 55%|
 50%|
 45%|
 40%|
 35%|
 30%|
 25%|
 20%|
 15%|              #
 10%|             ###  #
  5%|            ########
     ------------------------------------------------------------
               10        20        30        40        50        60   (minutes)
                       cpu-usage (Slot 1 CPU 0) last 60 minutes (SYSTEM)
```

The output shows the following items:

- Process name. The name **SYSTEM** represents the entire system.
- CPU that is holding the process: CPU 0 in slot 1.
- Historical CPU usage statistics for the entire system during the last 60 minutes.
  - **12 minutes ago**—Approximately 5%.
  - **13 minutes ago**—Approximately 10%.
  - **14 minutes ago**—Approximately 15%.
  - **15 minutes ago**—Approximately 10%.
  - **16 and 17 minutes ago**—Approximately 5%.
  - **18 minutes ago**—Approximately 10%.
  - **19 minutes ago**—Approximately 5%.
  - **Other time**—2% or lower.

Related commands

monitor cpu-usage enable

monitor cpu-usage interval

10.1.11. display device

Use **display device** to display device information.

Syntax

display device [**usb**] [**slot** *slot-number* | **verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

usb: Displays USB interface information.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information for all member devices.

verbose: Displays detailed information. If you do not specify this keyword, this command displays brief information, and does not display firewall card information.

Usage guidelines

If you do not specify the **usb** keywords, this command displays information about member devices.

Examples

Display device information.

```
<Switch> display device
Slot 1
Slot Type             State    Subslot  Soft Ver             Patch Ver
1    QX-S5628GT-4X2Q Master   1        1115                 None
```

Table 10-2 Command output

Field	Description
Type	Device type.
State	Role of the device in an IRF fabric: • **Master**—The device is the master. • **Standby**—The device is a subordinate member.
Soft Ver	Software version of the device.
Patch Ver	Patch version of the device. If no patch is installed, the value of this field is **None**.

10.1.12. display device manuinfo

Use **display device manuinfo** to display electronic label information for the device.

Syntax

display device manuinfo [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays electronic label information for all member devices.

Usage guidelines

An electronic label contains the permanent configuration information, including the hardware serial number, manufacturing date, MAC address, and vendor name. The data is written to the storage

component during hardware debugging or testing. This command displays only part of the electronic label information.

Examples

Display electronic label information for the device.

```
<Switch> display device manuinfo
...
```

10.1.13. display diagnostic-information

Use **display diagnostic-information** to display or save operating information for features and hardware modules.

Syntax

display diagnostic-information [**hardware** | **infrastructure** | **l2** | **l3** | **service**] [*filename*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

hardware: Specifies hardware-related operating information.

infrastructure: Specifies operating information for the fundamental features.

l2: Specifies operating information for the Layer 2 features.

l3: Specifies operating information for the Layer 3 features.

service: Specifies operating information for Layer 4 and upper-layer features.

filename: Saves the information to a file. The *filename* argument must use the **.tar.gz** extension. If you do not specify this argument, the command prompts you to choose whether to save the information to a file or display the information.

Usage guidelines

You can use one of the following methods to collect operating statistics for diagnostics and troubleshooting:

- Use separate **display** commands to collect operating information feature by feature or module by module.
- Use the **display diagnostic-information** command to collect operating information for multiple or all features and hardware modules.

To save storage space, this command automatically compresses the information before saving the information to a file. To view the file content:

1. Use the **tar extract** command to extract the file.
2. Use the **gunzip** command to decompress the extracted file.
3. Use the **more** command to view the content of the decompressed file.

If you abort the **display diagnostic-information** command, the **gunzip** command might not be able to decompress the extracted file. To decompress the extracted file, export the extracted file to a PC that is running Linux, and use the **gunzip -c** command.

If you do not specify a file name for the command, the system prompts you to choose whether to display or save the information. If you choose to save the information, the system automatically assigns a file name and displays the file name in brackets. For file name uniqueness, the file name includes the device name and the current system time. If the device name contains any of the following special characters, the system uses an underscore (_) to replace each special character: forward slashes (/), backward slashes (\), colons (:), asterisks (*), question marks (?), less than signs (<), greater than signs (>), pipeline signs (|), and quotation marks ("). For example, device name **A/B** will change to **A_B** in the file name, as in **flash:/diag_A_B_20160101-000438.tar.gz**.

If you do not specify any feature parameters, this command displays or saves the operating information for all features and modules.

This command does not support the |, **>**, and **>>** options.

While the device is executing this command, do not execute any other commands. Executing other commands might affect the collected operating information.

Examples

Display the operating information for all features and modules.

```
<Switch> display diagnostic-information
Save or display diagnostic information (Y=save, N=display)? [Y/N]:n
================================================
  ===============display clock===============
14:03:55 UTC Thu 01/05/2015
================================================
  ===============display version===============
...
```

Save the operating information to the default file.

```
<Switch> display diagnostic-information
Save or display diagnostic information (Y=save, N=display)? [Y/N]:y
Please input the file name(*.tar.gz)[flash:/diag_Switch_20160101-024601.tar.gz]:
Diagnostic information is outputting to flash:/diag_Switch_20160101-024601.tar.gz.
Please wait...
Save successfully.
```

Press **Enter** when the system prompts you to enter the file name.

Save the operating information for all features and modules to file **test.tar.gz**.

```
<Switch> display diagnostic-information test.tar.gz
Diagnostic information is outputting to flash:/test.tar.gz.
Please wait...
Save successfully.
```

Related commands

gunzip

more

tar extract

10.1.14. display environment

Use **display environment** to display temperature information.

Syntax

display environment [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays temperature information for all member devices.

Examples

Display information about all temperature sensors on the device.

```
<Switch> display environment
 System temperature information (degree centigrade):
 ---------------------------------------------------------------------
 Slot   Sensor    Temperature  Lower  Warning  Alarm  Shutdown
 1      hotspot 1 31           0      63       68     NA
 1      hotspot 2 0            0      110      130    137
```

Table 10-3 Command output

Field	Description
System Temperature information (degree centigrade)	Temperature information (°C).
sensor	Temperature sensor, which is fixed at **hotspot**.
Slot	Sensor position.
Temperature	Current temperature.
Lower	Lower temperature limit. If the device does not support this field, this field displays **NA**.
Warning	Warning temperature threshold. If the device does not support this field, this field displays **NA**.
Alarm	Alarming temperature threshold. If the device does not support this field, this field displays **NA**.
Shutdown	Shutdown temperature threshold. When the sensor temperature reaches the limit, the system shuts down automatically. If the device does not support this field, this field displays **NA**.

10.1.15. display fan

Use **display fan** to display fan tray operating status information.

Syntax

display fan [**slot** *slot-number* [*fan-id*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays fan tray operating status information for all member devices.

fan-id: Specifies a fan tray by its ID. If you do not specify a fan tray, this command displays operating status information for all fan trays at the specified position.

Examples

Display the operating states of all fan trays.

```
<Switch> display fan
 Slot 1:
 Fan 1:
 State    : Normal
 Airflow Direction: Port-to-power
 Prefer Airflow Direction: Port-to-power
```

Table 10-4 Command output

Field	Description
Slot 1	Number of the member device.
Fan 1	Fan tray number.
State	Fan status: • **Absent**—The slot is not installed with a fan tray. • **Fault**—The fan is faulty. • **Normal**—The fan is operating correctly. • **FanDirectionFault**—The actual airflow direction is not the preferred direction.
Airflow Direction	Actual airflow direction: • **Port-to-power**—From the port side to the power supply side. • **Power-to-port**—From the power supply side to the port side.
Prefer Airflow Direction	Preferred airflow direction: • **Port-to-power**—From the port side to the power supply side. • **Power-to-port**—From the power supply side to the port side.

10.1.16. display memory

Use **display memory** to display memory usage information.

Syntax

display memory [**slot** *slot-number* [**cpu** *cpu-number*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays memory usage for all member devices.

cpu *cpu-number*: Specifies a CPU by its number. The *cpu-number* argument must be 0.

Examples

Display detailed memory usage information.

```
<Switch> display memory
Memory statistics are measured in KB:
Slot 1:
             Total       Used       Free     Shared    Buffers     Cached   FreeRatio
Mem:       2036536     496116    1540420          0       1436     113644       75.7%
-/+ Buffers/Cache:     381036    1655500
Swap:            0          0          0
LowMem:    1651512     279856    1371656         --         --         --       83.1%
HighMem:    385024     216260     168764         --         --         --       43.8%
```

Table 10-5 Command output

Field	Description
Mem	Memory usage information.
Total	Total size of the physical memory space that can be allocated. The memory space is virtually divided into two parts. Part 1 is solely used for kernel code, kernel management, and ISSU functions. Part 2 can be allocated and used for such tasks as running service modules and storing files. The size of part 2 equals the total size minus the size of part 1.
Used	Used physical memory.
Free	Free physical memory.
Shared	Physical memory shared by processes. If this field is not supported, two hyphens (--) are displayed.
Buffers	Physical memory used for buffers. If this field is not supported, two hyphens (--) are displayed.
Cached Caches	Physical memory used for caches. If this field is not supported, two hyphens (--) are displayed.
FreeRatio	Free memory ratio.
-/+ Buffers/Cache	-/+ Buffers/Cache:used = Mem:Used – Mem:Buffers – Mem:Cached, which indicates the physical memory used by applications. -/+ Buffers/Cache:free = Mem:Free + Mem:Buffers + Mem:Cached, which indicates the physical memory available for applications.
Swap	Memory space for swapping.
LowMem	Low-memory usage information.
HighMem	High-memory usage information.

10.1.17. display memory-threshold

Use **display memory-threshold** to display memory alarm thresholds and statistics.

Syntax

display memory-threshold [**slot** *slot-number* [**cpu** *cpu-number*]]

Views

Any view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays the memory usage thresholds and statistics for the master device.

cpu *cpu-number*: Specifies a CPU by its number. The *cpu-number* argument must be 0.

Usage guidelines

For more information about memory usage notifications, see log information containing **MEM_EXCEED_THRESHOLD** or **MEM_BELOW_THRESHOLD**.

Examples

Display memory alarm thresholds and statistics.

```
<Switch> display memory-threshold
Memory usage threshold: 100%
Free-memory thresholds:
    Minor: 96M
    Severe: 64M
    Critical: 48M
    Normal: 128M
    Early-warning: 192M
    Secure: 304M

Current free-memory state: Normal (secure)
Free-memory event statistics:
 [Back to secure state]
    First notification: 0.0
    Latest notification: 0.0
    Total number of notifications sent: 0
 [Entered early-warning state]
    First notification at: 0.0
    Latest notification at: 0.0
    Total number of notifications sent: 0
 [Back to normal state]
    First notification: 0.0
    Latest notification: 0.0
    Total number of notifications sent: 0
```

```
[Entered minor alarm state]
   First notification at: 0.0
   Latest notification at: 0.0
   Total number of notifications sent: 0
[Back to minor alarm state]
   First notification at: 0.0
   Latest notification at: 0.0
   Total number of notifications sent: 0
[Entered severe alarm state]
   First notification at: 0.0
   Latest notification at: 0.0
   Total number of notifications sent: 0
[Back to severe alarm state]
   First notification at: 0.0
   Latest notification at: 0.0
   Total number of notifications sent: 0
[Entered critical alarm state]
   First notification at: 0.0
   Latest notification at: 0.0
   Total number of notifications sent: 0
```

10.1.18. display power

Use **display power** to display power supply information.

Syntax

display power [**slot** *slot-number* [*power-id*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays power supply information for all member devices.

power-id: Specifies a power supply by its ID. If you do not specify a power supply, this command displays information about all power supplies at the specified position.

Examples

Display power supply information.

```
<Switch> display power
 Slot 1:
 PowerID State    Mode   Current(A)  Voltage(V)  Power(W)
 1       Absent   --       --          --          --
 2       Normal   AC       --          --          --
```

Table 10-6 Command output

Field	Description
PowerID	Power supply ID.
State	Power supply status. • **Absent**—The slot is not installed with a power supply. • **Fault**—The power supply is faulty. • **Normal**—The power supply is operating correctly.
Mode	Mode of the power supply: • **AC**–AC power supply. • **DC**–DC power supply.
Current(A)	Output current of the power supply, in amperes. This field is not supported.
Voltage(V)	Output voltage of the power supply, in volts. This field is not supported.
Power(W)	Output power of the power supply, in watts. This field is not supported.

10.1.19. display resource-monitor

Use **display resource-monitor** to display resource monitoring information.

Syntax

display resource-monitor [**resource** *resource-name*] [**slot** *slot-number* [**cpu** *cpu-number*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

resource *resource-name*: Specifies a resource type by its name. For information about available resource types, see Table 10-13 .

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays resource monitoring information for all member devices.

cpu *cpu-number*: Specifies a CPU by its number.

Examples

Display ARP resource monitoring information.

```
<Switch> display resource-monitor resource arp
Minor alarms resending: Enabled

Slot 1:
Resource                          Minor Severe Free/Total
                                  (%)   (%)    (absolute)
```

```
arp                                 50    20      90095/90098
```

Command output

Field	Description
Minor alarms resending	Status of the minor resource depletion alarm resending feature, **Enabled** or **Disabled.**
Resource	Monitored resource type.
Minor (%)	Minor resource depletion threshold, in percentage.
Severe (%)	Severe resource depletion threshold, in percentage.
Free/Total (absolute)	Numbers of available resources and total resources, in absolute values.

Related commands

resource-monitor minor resend enable

resource-monitor resource

10.1.20. display scheduler job

Use **display scheduler job** to display job configuration information.

Syntax

display scheduler job [*job-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

job-name: Specifies a job by its name, a case-sensitive string of 1 to 47 characters. If you do not specify a job, this command displays configuration information for all jobs.

Examples

Display configuration information for all jobs.

```
<Switch> display scheduler job
Job name: saveconfig
 copy startup.cfg backup.cfg

Job name: backupconfig

Job name: creat-VLAN100
 system-view
 vlan 100
```

// The output shows that the device has three jobs: the first has one command, the second does not have any commands, and the third has two commands. Jobs are separated by blank lines.

10.1.21. display scheduler logfile

Use **display scheduler logfile** to display job execution log information.

Syntax

display scheduler logfile

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display job execution log information.

```
<Switch> display scheduler logfile
Logfile Size: 1902 Bytes.

Job name        : shutdown
Schedule name   : shutdown
Execution time  : Tue Dec 27 10:44:42 2015
Completion time : Tue Dec 27 10:44:47 2015
---------------------------------- Job output ----------------------------------
<Switch>system-view
System View: return to User View with Ctrl+Z.
[Switch]interface rang gigabitethernet 1/0/1 to gigabitethernet 1/0/3
[Switch-if-range]shutdown
```

Table 10-7 Command output

Field	Description
Logfile Size	Size of the log file, in bytes.
Schedule name	Schedule to which the job belongs.
Execution time	Time when the job was started.
Completion time	Time when the job was completed. If the job has never been executed or the job does not have any commands, this field is blank.
Job output	Commands in the job and their output.

Related commands

reset scheduler logfile

10.1.22. display scheduler reboot

Use **display scheduler reboot** to display the automatic reboot schedule.

Syntax

display scheduler reboot

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display the automatic reboot schedule.

```
<Switch> display scheduler reboot
System will reboot at 16:32:00 05/23/2015 (in 1 hours and 39 minutes).
```

Related commands

scheduler reboot at

scheduler reboot delay

10.1.23. display scheduler schedule

Use **display scheduler schedule** to display schedule information.

Syntax

display scheduler schedule [*schedule-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

schedule-name: Specifies a schedule by its name, a case-sensitive string of 1 to 47 characters. If you do not specify a schedule, this command displays information about all schedules.

Examples

Display information about all schedules.

```
<Switch> display scheduler schedule
Schedule name        : shutdown
Schedule type        : Run once after 0 hours 2 minutes
Start time           : Tue Dec 27 10:44:42 2015
Last execution time  : Tue Dec 27 10:44:42 2015
Last completion time : Tue Dec 27 10:44:47 2015
Execution counts     : 1
------------------------------------------------------------------------
Job name                                        Last execution status
shutdown                                        Successful
```

Table 10-8 Command output

Field	Description
Schedule type	Execution time setting of the schedule. If no execution time is specified, this field is not displayed.
Start time	Time to execute the schedule for the first time. If no execution time is specified, this field is not displayed.
Last execution time	Last time when the schedule was executed. If no execution time is specified, this field is not displayed. If the schedule has never been executed, "Yet to be executed" is displayed for this field.
Last completion time	Last time when the schedule was completed. If no execution time is specified, this field is not displayed.
Execution counts	Number of times the schedule has been executed. If the schedule has never been executed, this field is not displayed.
Job name	Name of a job under the schedule.
Last execution status	Result of the most recent execution: • **Successful**. • **Failed**. • **Waiting**—The device is executing the schedule and the job is waiting to be executed. • **In process**—The job is being executed. • **-NA-**—The execution time has not arrived yet. To view information about whether the commands in the job has been executed and the execution results, execute the **display scheduler logfile** command.

10.1.24. display switch-mode status

Use **display switch-mode status** to display the operating mode of the device.

Syntax

display switch-mode status

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display operating mode about the device.

<Switch> display switch-mode status

```
Switch-mode in use: NORMAL MODE(default).
Switch-mode for next reboot:: VXLAN MODE.
Switch-mode for next reboot: VXLAN MODE.
```

10.1.25. display transceiver alarm

Use **display transceiver alarm** to display transceiver alarms.

Syntax

display transceiver alarm interface [*interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface [*interface-type interface-number*]: Specifies an interface by its type and number. If no interface is specified, this command displays the alarms present on every transceiver module.

Usage guidelines

Table 10-9 shows the common transceiver alarm components. If no error occurs, "None" is displayed.

Table 10-9 Common transceiver alarm components

Field	Description
APD	Avalanche photo diode
PCS	Physical coding sublayer
PHY XS	PHY extended sublayer
PMA/PMD	Physical medium attachment/physical medium dependent
power	Optical power
REFCLK	Reference clock
RX	Receive
TEC	Thermoelectric cooler
Temp	Temperature
TX	Transmit
WIS	WAN interface sublayer

Examples

Display the alarms present on the transceiver module in interface GigabitEthernet 1/0/1.

```
<Switch> display transceiver alarm interface gigabitethernet 1/0/1
GigabitEthernet1/0/1 transceiver current alarm information:
  RX signal loss
  RX power low
```

Table 10-10 Common output

Field	Description
transceiver current alarm information	Alarms present on the transceiver module.
RX signal loss	Inbound signal loss occurred.
RX power low	Received power is low.

NOTE:
The **display transceiver alarm** command is supported on Ver7.4.45 and later.

10.1.26. display transceiver diagnosis

Use **display transceiver diagnosis** to display the current values of the digital diagnosis parameters on transceiver modules.

Syntax

display transceiver diagnosis interface [*interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface [*interface-type interface-number*]: Specifies an interface by its type and number. If no interface is specified, this command displays the current values of the digital diagnosis parameters on every transceiver module.

Examples

Display the current values of the digital diagnosis parameters on the transceiver module in interface GigabitEthernet 1/0/1.

```
<Switch> display transceiver diagnosis interface gigabitethernet 1/0/1
GigabitEthernet1/0/1 transceiver diagnostic information:
  Current diagnostic parameters:
    Temp(°C)  Voltage(V)  Bias(mA)  RX power(dBm)  TX power(dBm)
    36        3.31        6.13      -35.64          -5.19
  Alarm thresholds:
            Temp(°C)   Voltage(V)  Bias(mA)  RX power(dBM)  TX power(dBM)
    High    50         3.55        1.44      -10.00         5.00
    Low     30         3.01        1.01      -30.00         0.00
```

Table 10-11 Common output

Field	Description
transceiver diagnostic information	Digital diagnosis information for the transceiver module in

Field	Description
	the interface.
Temp.(°C)	Temperature in °C, accurate to 1°C.
Voltage(V)	Voltage in V, accurate to 0.01 V.
Bias(mA)	Bias current in mA, accurate to 0.01 mA.
RX power(dBm)	Receive power in dBm, accurate to 0.01 dBm.
TX power(dBm)	Transmit power in dBm, accurate to 0.01 dBm.

NOTE:
The **display transceiver diagnosis** command is supported on Ver7.4.45 and later.

10.1.27. display transceiver interface

Use **display transceiver interface** to display the key parameters of transceiver modules.

Syntax

display transceiver interface [*interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number: Specifies an interface by its type and number. If you do not specify an interface, this command displays the key parameters of every transceiver module.

Examples

Display the key parameters of the transceiver module in interface Ten-GigabitEthernet 1/0/50.

<Switch> display transceiver interface ten-gigabitethernet 1/0/50

```
Ten-GigabitEthernet1/0/50 transceiver information:
  Transceiver Type              : 10G_BASE_SR_SFP
  Connector Type                : LC
  Wavelength(nm)                : 850
  Transfer Distance(m)          : 80(OM2),20(OM1),300(OM3)
  Digital Diagnostic Monitoring : YES
  Vendor Name                   : Hisense
  Ordering Name                 : SFP-XG-SX-MM850-D
  Part Number                   : LTF8502-BC+
  Serial Number                 : U8AC2H029BP
```

NOTE:
The “Ordering Name” may not be displayed for some modules.

10.1.28. display transceiver manuinfo

Use **display transceiver manuinfo** to display electronic label information for transceiver modules.

Syntax

display transceiver manuinfo interface [*interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number: Specifies an interface by its type and number. If no interface is specified, this command displays electronic label information for all transceiver modules.

Examples

Display the key parameters of the transceiver module in interface Ten-GigabitEthernet 1/0/50.

```
<Switch> display transceiver interface Ten-gigabitethernet 1/0/50
Ten-GigabitEthernet1/0/50 transceiver manufacture information:
  Manu. Serial Number : 210231A1RPN22600345K
  Manufacturing Date  : 2022-06-27
  Vendor Name         : Hisense
```

NOTE:

- The **display transceiver manuinfo** command is supported on Ver7.4.45 and later.
- For modules that do not support this command, the following message is displayed. To view transceiver information, use the **display transceiver interface** command.

```
The transceiver does not support this function.
```

10.1.29. display version

Use **display version** to display system version information.

Syntax

display version

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display system version information.

```
<Switch> display version
...
```

Table 10-12 Command output

Field	Description
Last reboot reason	Reason for the last reboot: • **User reboot**–The reboot was manually initiated from a user interface, such as the CLI or SNMP. • **Cold reboot**–The reboot was caused by a power cycle. • **Kernel abnormality reboot**–The reboot was caused by kernel exceptions. • **DeadLoop reboot**–The reboot was caused by a kernel thread dead loop. • **DEV HandShake reboot**–The reboot was caused by a device management handshake failure. • **SlaveSwitch reboot**–The reboot was caused by a master/subordinate switchover. • **IRF Merge reboot**–The reboot was caused by an IRF merge. • **Auto Update reboot**–The reboot was caused by an automatic software upgrade. • **Memory exhaust reboot**–The reboot was caused by a memory-exhausted event.

10.1.30. dying-gasp host

Use **dying-gasp host** to configure poweroff alarm destination host settings.

Use **undo dying-gasp host** to remove poweroff alarm destination host settings.

Syntax

dying-gasp host { *ip-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] **snmp-trap version** { **v1** | **v2c** | **v3** [**authentication** | **privacy**] } **securityname** *security-string*

dying-gasp host { *ip-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] **syslog**

undo dying-gasp host { *ip-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] { **snmp-trap** | **syslog** }

Default

No poweroff alarm destination host settings are configured.

Views

System view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the IPv4 address of the destination host to which the device sends the poweroff alarm.

ipv6 *ipv6-address*: Specifies the IPv6 address of the destination host to which the device sends the poweroff alarm.

vpn-instance *vpn-instance-name*: Specifies the **MPLS L3VPN** instance to which the destination host belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. If the destination host belongs to the public network, do not specify this option.

snmp-trap: Uses an SNMP notification to send the poweroff alarm.

version: Specifies the SNMP version.

- **v1**: Uses SNMPv1.
- **v2c**: Uses SNMPv2c.
- **v3**: Uses SNMPv3. If you do not specify the **authentication** or **privacy** keyword, no authentication or encryption is performed.
  - **authentication**: Performs only authentication on packets.
  - **privacy**: Performs both authenticaiton and encrypton on packets.

securityname *security-string*: Specifies an SNMPv1 or SNMPv2c community name, or SNMPv3 username, a case-sensitive string of 1 to 32 characters.

syslog: Uses a log message to send the poweroff alarm.

Usage guidelines

The device can send the poweroff alarm by using either or both of an SNMP notification and a log message.

The device can send the poweroff alarm to multiple destination hosts at the same time.

When you configure the device to send poweroff alarms in SNMP v3 traps to the NMS, execute the **snmp-agent usm-user** command to create an SNMP v3 user. Make sure the authentication mode for the group to which the SNMP v3 user belongs is the same as the authentication mode configured by the **dying-gasp host** command. In addition, the authentication and encryption parameters must match those configured on the NMS side. If you fail to do so, the device cannot send poweroff alarms in SNMP v3 traps to the NMS.

Examples

Configure the device to send the poweroff alarm to the host at 1.1.1.1 by using an SNMPv1 notification. The community name is **public**.

```
<Sysname> system-view
[Sysname] dying-gasp host 1.1.1.1 snmp-trap version v1 securityname public
```

Related commands

dying-gasp source

10.1.31. dying-gasp source

Use **dying-gasp source** to specify the source interface for sending the poweroff alarm.

Use **undo dying-gasp source** to restore the default.

Syntax

dying-gasp source *interface-type* { *interface-number* | *interface-number.subnumber* }

undo dying-gasp source

Default

No source interface is specified. On an IPv4 network, the device uses the primary IPv4 address of the output interface for the route to the destination host as the source address. On an IPv6 network, the device selects a source IPv6 address as defined in RFC 3484.

Views

System view

Predefined user roles

network-admin

Parameters

interface-type { *interface-number* | *interface-number.subnumber* }: Specifies a Layer 3 interface. The *interface-type* argument specifies the interface type. The *interface-number* argument specifies the interface number. The *subnumber* argument specifies the subinterface number and is in the range of 1 to 4094. Support for the *interface-number.subnumber* argument depends on the device model.

Usage guidelines

The device uses the IPv6 address or primary IPv4 address of the specified source interface as the source address for outgoing poweroff alarm packets. The destination hosts use this address to identify SNMP notifications or log messages received from the device.

If no address is configured for the specified source interface, this command does not take effect. For this command to take effect, assign an address to the source interface.

Examples

Use the Vlan-interface 1 interface as the source interface for sending the poweroff alarm.

```
<Sysname> system-view
[Sysname] dying-gasp source vlan-interface 1
```

Related commands

dying-gasp host

10.1.32. fan prefer-direction

Use **fan prefer-direction** to specify the preferred airflow direction for the device.

Use **undo fan prefer-direction** to restore the default.

Syntax

fan prefer-direction slot *slot-number* { **port-to-power** | **power-to-port** }

undo fan prefer-direction slot *slot-number*

Default

The preferred airflow direction is from the port side to the power supply side.

Views

System view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID.

port-to-power: Specifies the airflow direction from the port side to the power supply side.

power-to-port: Specifies the airflow direction from the power supply side to the port side.

Usage guidelines

QX-S5628GT-4X2Q and QX-S5648GT-4X2Q switches do not support this command.

Examples

Set the preferred airflow direction to **port-to-power** for member device 1.

```
<Switch> system-view
[Switch] fan prefer-direction slot 1 port-to-power
```

Related commands

display fan

10.1.33. header

Use **header** to configure a banner.

Use **undo header** to delete a banner.

Syntax

header { **legal** | **login** | **motd** | **shell** } *text*

undo header { **legal** | **login** | **motd** | **shell** }

Default

The device does not have banners.

Views

System view

Predefined user roles

network-admin

Parameters

legal: Configures the banner to be displayed before a user inputs the username and password to access the CLI.

login: Configures the banner to be displayed before password or scheme authentication is performed for a login user.

motd: Configures the greeting banner to be displayed before the legal banner appears.

shell: Configures the banner to be displayed before a user accesses user view.

text: Specifies the banner message. You can enter the banner message on the same line as the keywords or on different lines. For more information, see *Fundamentals Configuration Guide*.

Examples

Configure the legal banner.

```
<Switch> system-view
```

```
[Switch] header legal
Please input banner content, and quit with the character '%'.
Welcome to use the legal banner%
```

10.1.34. job

Use **job** to assign a job to a schedule.

Use **undo job** to revoke a job.

Syntax

job *job-name*

undo job *job-name*

Default

No job is assigned to a schedule.

Views

Schedule view

Predefined user roles

network-admin

Parameters

job-name: Specifies the job name, a case-sensitive string of 1 to 47 characters.

Usage guidelines

You can assign multiple jobs to a schedule. The jobs in a schedule are executed concurrently.

The jobs to be assigned to a schedule must already exist. To create a job, use the **scheduler job** command.

Examples

Assign job **save-job** to schedule **saveconfig**.

```
<Switch> system-view
[Switch] scheduler schedule saveconfig
[Switch-schedule-saveconfig] job save-job
```

Related commands

scheduler job

scheduler schedule

10.1.35. memory-threshold

Use **memory-threshold** to set free-memory thresholds.

Use **undo memory-threshold** to restore the defaults.

Syntax

memory-threshold [**slot** *slot-number* [**cpu** *cpu-number*]] **minor** *minor-value* **severe** *severe-value* **critical** *critical-value* **normal** *normal-value*

undo memory-threshold [**slot** *slot-number* [**cpu** *cpu-number*]]

Default

Minor alarm threshold: 96 MB.

Severe alarm threshold: 64 MB.

Critical alarm threshold: 48 MB.

Normal state threshold: 128 MB.

Views

System view

Predefined user roles

network-admin

Parameters

minor *minor-value*: Specifies the minor alarm threshold. To view the value range for this threshold, enter a question mark (?) in the place of the *minor-value* argument. Setting this threshold to 0 disables the minor alarm feature.

severe *severe-value*: Specifies the severe alarm threshold. To view the value range for this threshold, enter a question mark (?) in the place of the *severe-value* argument. Setting this threshold to 0 disables the severe alarm feature.

critical *critical-value*: Specifies the critical alarm threshold. To view the value range for this threshold, enter a question mark (?) in the place of the *critical-value* argument. Setting this threshold to 0 disables the critical alarm feature.

normal *normal-value*: Specifies the normal state threshold. To view the value range for this threshold, enter a question mark (?) in the place of the *normal-value* argument.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command sets free-memory thresholds for the master device.

cpu *cpu-number*: Specifies a CPU by its number. The *cpu-number* argument must be 0.

Usage guidelines

To ensure correct operation and improve memory efficiency, the system monitors the amount of free memory space in real time. If the amount of free memory space decreases to or below the minor, severe, or critical alarm threshold, the system issues an alarm to affected service modules or processes.

The early warning feature warns you of an approaching insufficient-memory condition.

For more information about the thresholds, see *Fundamentals Configuration Guide*.

Examples

Set the minor alarm, severe alarm, critical alarm, and normal state thresholds to 64 MB, 48 MB, 32 MB, and 96 MB, respectively.

```
<Switch> system-view
[Switch] memory-threshold minor 64 severe 48 critical 32 normal 96
```

Set the minor alarm, severe alarm, critical alarm, and normal state thresholds to 3%, 2%, 1%, and 5% of the total memory size, respectively.

```
<Switch> system-view
[Switch] memory-threshold ratio minor 3 severe 2 critical 1 normal 5
```

Related commands

display memory-threshold

10.1.36. monitor cpu-usage enable

Use **monitor cpu-usage enable** to enable CPU usage monitoring.

Use **undo monitor cpu-usage enable** to disable CPU usage monitoring.

Syntax

monitor cpu-usage enable [**slot** *slot-number* [**cpu** *cpu-number*]]

undo monitor cpu-usage enable [**slot** *slot-number* [**cpu** *cpu-number*]]

Default

CPU usage monitoring is enabled.

Views

System view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command enables CPU usage monitoring for the master device.

cpu *cpu-number*: Specifies a CPU by its number. The *cpu-number* argument must be 0.

Usage guidelines

After CPU usage monitoring is enabled, the system samples and saves CPU usage at the interval specified by the **monitor cpu-usage interval** command. You can use the **display cpu-usage history** command to view recent CPU usage.

Examples

Enable CPU usage monitoring.

```
<Switch> system-view
[Switch] monitor cpu-usage enable
```

Related commands

display cpu-usage configuration

display cpu-usage history

monitor cpu-usage interval

10.1.37. monitor cpu-usage interval

Use **monitor cpu-usage interval** to set the sampling interval for CPU usage monitoring.

Use **undo monitor cpu-usage interval** to restore default settings.

Syntax

monitor cpu-usage interval *interval* [**slot** *slot-number* [**cpu** *cpu-number*]]

undo monitor cpu-usage interval [**slot** *slot-number* [**cpu** *cpu-number*]]

Default

The system samples CPU usage every 1 minute.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the sampling interval for CPU usage monitoring. Valid values include **5Sec** (5 seconds), **1Min** (1 minute), and **5Min** (5 minutes), case insensitive.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command sets the interval for the master device.

cpu *cpu-number*: Specifies a CPU by its number. The *cpu-number* argument must be 0.

Usage guidelines

After CPU usage monitoring is enabled, the system samples and saves CPU usage at the specified interval. You can use the **display cpu-usage history** command to view recent CPU usage.

Examples

Set the sampling interval for CPU usage monitoring to 5 seconds.

```
<Switch> system-view
[Switch] monitor cpu-usage interval 5Sec
```

Related commands

display cpu-usage configuration

display cpu-usage history

monitor cpu-usage enable

10.1.38. monitor cpu-usage threshold

Use **monitor cpu-usage threshold** to set CPU usage alarm thresholds.

Use **undo monitor cpu-usage threshold** to restore default settings.

IMPORTANT:

- The **monitor cpu-usage threshold** command checks total CPU usage statistics.
- Maximum of the total CPU usage statistics is 100%.
- If control-plane is 45% and data-plane is 5%, total CPU usage statistics is 25%.

Syntax

monitor cpu-usage threshold *severe-threshold* **minor-threshold** *minor-threshold* **recovery-threshold** *recovery-threshold* [**slot** *slot-number* [**cpu** *cpu-number*]]

undo monitor cpu-usage threshold minor-threshold recovery-threshold [**slot** *slot-number* [**cpu** *cpu-number*]]

Default

The default settings are as follows:

- **Severe CPU usage alarm threshold**—99%.
- **Minor CPU usage alarm threshold**—80%.
- **CPU usage recovery threshold**—60%.

Views

System view

Predefined user roles

network-admin

Parameters

severe-threshold: Specifies the severe CPU usage alarm threshold in percentage. The value range for this argument is 2 to 100.

minor-threshold *minor-threshold*: Specifies the minor CPU usage alarm threshold in percentage. The value range for this argument is 1 to the severe CPU usage alarm threshold minus 1.

recovery-threshold *recovery-threshold*: Specifies the CPU usage recovery threshold in percentage. The value range for this argument is 0 to the minor CPU usage alarm threshold minus 1.

cpu-threshold: Specifies the CPU usage threshold in percentage. The value range is 0 to 100.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command sets the CPU usage threshold for the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Usage guidelines

The device samples CPU usage at 1-minute intervals. If the sample is greater than the CPU usage threshold, the device sends a trap.

Examples

Set the severe CPU usage alarm threshold to 90%, minor CPU usage alarm threshold to 80%, and CPU usage recovery threshold to 70%.

```
<Switch> system-view
[Switch] monitor cpu-usage threshold 90 minor-threshold 80 recovery-threshold 70
```

Related commands

display cpu-usage configuration

10.1.39. monitor resend cpu-usage

Use **monitor resend cpu-usage** to set CPU usage alarm resending intervals.

Use **undo monitor resend cpu-usage** to restore default settings.

Syntax

monitor resend cpu-usage { **minor-interval** *minor-interval* | **severe-interval** *severe-interval* } * [**slot** *slot-number* [**cpu** *cpu-number*]]

undo monitor resend cpu-usage [**minor-interval** | **severe-interval**] [**slot** *slot-number* [**cpu** *cpu-number*]]

Default

The minor alarm resending interval is 300 seconds. The severe alarm resending interval is 60 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

minor-interval *minor-interval*: Specifies the minor alarm resending interval in seconds, a multiple of five in the range of 10 to 3600.

severe-interval *severe-interval*: Specifies the severe alarm resending interval in seconds, a multiple of five in the range of 10 to 3600.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command sets alarm resending intervals for the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Usage guidelines

The device samples CPU usage periodically and compares the sample with the CPU usage threshold. If the sample increases above an alarm threshold, the CPU usage enters an alarm state and the device sends an alarm.

While the CPU usage is in minor alarm state, the device sends minor alarms periodically until the CPU usage increases above the severe threshold or the minor alarm is removed.

While the CPU usage is in severe alarm state, the device sends severe alarms periodically until the severe alarm is removed.

You can use this command to change CPU usage alarm resending intervals.

If you do not specify the **minor-interval** or **severe-interval** keyword, the **undo monitor resend cpu-usage** command restores default settings for both the minor and severe alarm resending intervals.

Examples

Set the CPU usage minor alarm resending interval to 60 seconds for CPU 0 in slot 1.

```
<Switch> system-view
[Switch] monitor resend cpu-usage minor-interval 60 slot 1 cpu 0
```

10.1.40. monitor resend memory-threshold

Use **monitor resend memory-threshold** to set memory depletion alarm resending intervals.

Use **undo monitor resend memory-threshold** to restore default settings.

Syntax

monitor resend memory-threshold { **critical-interval** *critical-interval* | **early-warning-interval** *early-warning-interval* | **minor-interval** *minor-interval* | **severe-interval** *severe-interval* } * [**slot** *slot-number* [**cpu** *cpu-number*]]

undo monitor resend memory-threshold [**critical-interval** | **early-warning-interval** | **minor-interval** | **severe-interval**] * [**slot** *slot-number* [**cpu** *cpu-number*]]

Default

- Early warning resending interval: 1 hour.
- Minor alarm resending interval: 12 hours.
- Severe alarm resending interval: 3 hours.
- Critical alarm resending interval: 1 hour.

Views

System view

Predefined user roles

network-admin

Parameters

critical-interval *critical-interval*: Specifies the critical alarm resending interval in hours, in the range of 1 to 48.

early-warning-interval *early-warning-interval*: Specifies the early warning resending interval in hours, in the range of 1 to 48.

minor-interval *minor-interval*: Specifies the minor alarm resending interval in hours, in the range of 1 to 48.

severe-interval *severe-interval*: Specifies the severe alarm resending interval in hours, in the range of 1 to 48.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command sets alarm resending intervals for the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Usage guidelines

The device samples the amount of free memory space periodically and compares the sample with free-memory thresholds. If the sample decreases to or below a threshold, the device enters a memory depletion alarm state and sends an alarm.

In critical alarm state, the device sends critical alarm notifications periodically until the critical alarm is removed.

In a lower alarm state, the device sends notifications for the alarm state periodically until it enters a higher alarm state or the current alarm is removed.

You can use this command to change the alarm resending intervals.

Examples

Set the minor memory depletion alarm resending interval to 12 hours for CPU 0 in slot 1.

```
<Switch> system-view
[Switch] monitor resend memory-threshold minor-interval 12 slot 1 cpu 0
```

10.1.41. parity-error monitor log enable

Use **parity-error monitor log enable** to enable parity error logging for entries on forwarding chips.

Use **undo parity-error monitor log enable** to disable parity error logging for entries on forwarding chips.

Syntax

parity-error monitor log enable

undo parity-error monitor log enable

Default

Parity error logging is enabled for entries on forwarding chips.

Views

System view

Predefined user roles

network-admin

Usage guidelines

The device detects parity errors in entries on forwarding chips. The parity error logging feature generates logs for the detected parity errors.

Examples

Enable parity error logging for entries on forwarding chips.

```
<Switch> system-view
[Switch] parity-error monitor log enable
```

10.1.42. parity-error monitor period

Use **parity-error monitor period** to set the parity error statistics interval for entries on forwarding chips.

Use **undo parity-error monitor period** to restore the default.

Syntax

parity-error monitor period *value*

undo parity-error monitor period

Default

The parity error statistics interval is 60 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

value: Specifies the parity error statistics interval in the range of 1 to 86400 seconds.

Usage guidelines

The device detects parity errors in entries on forwarding chips, and collects parity error statistics at the interval set by using this command.

Examples

Set the parity error statistics interval to 120 seconds.

```
<Switch> system-view
[Switch] parity-error monitor period 120
```

Related commands

parity-error monitor threshold

10.1.43. parity-error monitor threshold

Use **parity-error monitor threshold** to set the parity error alarm threshold for entries on forwarding chips.

Use **undo parity-error monitor threshold** to restore the default.

Syntax

parity-error monitor threshold *value*

undo parity-error monitor threshold

Default

The parity error alarm threshold is 5000.

Views

System view

Predefined user roles

network-admin

Parameters

value: Specifies the parity error alarm threshold in the range of 1 to 1000000.

Usage guidelines

The device detects and collects statistics for parity errors in entries on forwarding chips. If the number of parity errors in a parity error statistics interval exceeds the parity error alarm threshold, the system issues an alarm.

Examples

Set the parity error alarm threshold to 8000.

```
<Switch> system-view
[Switch] parity-error monitor threshold 8000
```

Related commands

parity-error monitor period

10.1.44. password-recovery enable

Use **password-recovery enable** to enable password recovery capability.

Use **undo password-recovery enable** to disable password recovery capability.

Syntax

password-recovery enable

undo password-recovery enable

Default

Password recovery capability is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Password recovery capability controls console user access to the device configuration and SDRAM from BootWare menus.

If password recovery capability is enabled, a console user can access the device configuration without authentication to configure new passwords.

If password recovery capability is disabled, console users must restore the factory-default configuration before they can configure new passwords. Restoring the factory-default configuration deletes the next-startup configuration files.

To enhance system security, disable password recovery capability.

Availability of BootWare menu options depends on the password recovery capability setting. For more information, see the release notes.

Examples

Disable password recovery capability.

```
<Switch> system-view
[Switch] undo password-recovery enable
```

10.1.45. reboot

Use **reboot** to reboot the device.

Syntax

reboot [**slot** *slot-number*] [**force**]

Views

User view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify an IRF member device, the command reboots all IRF member devices.

force: Reboots the device immediately without performing software or hard disk check. If this keyword is not specified, the system first identifies whether the reboot might result in data loss or a system failure. For example, the system identifies whether the main system software image file exists and whether a write operation is in progress on a storage medium. If the reboot might cause problems, the system does not reboot the device.

Usage guidelines

CAUTION:

- A reboot might interrupt network services.
- Use the **force** keyword only when the device fails or a **reboot** command without the **force** keyword cannot perform a reboot correctly. A **reboot** command with the **force** keyword might result in file system corruption because it does not perform data protection.

If the main startup software images are corrupt or missing, you must re-specify a set of main startup software images before executing the **reboot** command.

For data security, the device does not reboot if you reboot the device while the device is performing file operations.

If the IRF fabric has only one member device, rebooting the member device reboots the entire IRF fabric. If the IRF fabric has a subordinate member and the member is operating correctly, rebooting the master triggers a master/subordinate switchover.

To ensure correct operation of the IRF fabric and member devices, do not trigger a switchover by rebooting the master if no subordinate member devices are in **Stable** state. To view the status of subordinate member devices, execute the **display system stable state** command.

Examples

Reboot the device. Save the running configuration at prompt.

```
<Switch> reboot
Start to check configuration with next startup configuration file, please
wait.........DONE!
Current configuration will be lost after the reboot, save current configuration? [Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
flash:/startup.cfg exists, overwrite? [Y/N]:y
Validating file. Please wait...
Configuration is saved to mainboard device successfully.
This command will reboot the device. Continue? [Y/N]:y
Now rebooting, please wait...
```

Reboot the device immediately without performing software check.

```
<Switch> reboot force
A forced reboot might cause the storage medium to be corrupted. Continue? [Y/N]:y
Now rebooting, please wait...
```

Related commands

display system stable state

10.1.46. reset scheduler logfile

Use **reset scheduler logfile** to clear job execution log information.

Syntax

reset scheduler logfile

Views

User view

Predefined user roles

network-admin

Examples

Clear job execution log information.

```
<Switch> reset scheduler logfile
```

Related commands

display scheduler logfile

10.1.47. resource-monitor minor resend enable

Use **resource-monitor minor resend enable** to enable resending of minor resource depletion alarms.

Use **undo resource-monitor minor resend enable** to disable resending of minor resource depletion alarms.

Syntax

resource-monitor minor resend enable

undo resource-monitor minor resend enable

Default

Resending of minor resource depletion alarms is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

When a resource type enters minor alarm state, the device issues a minor alarm. If the resource type stays in minor alarm state or changes from severe alarm state to minor alarm state, the device identifies whether resending of minor resource depletion alarms is enabled. If the feature is disabled, the device does not issue additional minor alarms. If the feature is enabled, the device resends minor alarms periodically.

Examples

Enable resending of minor resource depletion alarms.

```
<Switch> system-view
[Switch] resource-monitor minor resend enable
```

Related commands

display resource-monitor

resource-monitor output

resource-monitor resource

10.1.48. resource-monitor output

Use **resource-monitor output** to specify destinations for resource depletion alarms.

Use **undo resource-monitor output** to remove destinations for resource depletion alarms.

Syntax

resource-monitor output { **netconf-event** | **snmp-notification** | **syslog** } *

undo resource-monitor output [**netconf-event** | **snmp-notification** | **syslog**] *

Default

Resource depletion alarms are sent to NETCONF, SNMP, and the information center.

Views

System view

Predefined user roles

network-admin

Parameters

netconf-event: Sends resource depletion alarms to the NETCONF feature to encapsulate the alarms in NETCONF events. For more information, see NETCONF in *Network Management and Monitoring Configuration Guide*.

snmp-notification: Sends resource depletion alarms to the SNMP feature to encapsulate the alarms in SNMP traps and informs. For more information, see SNMP in *Network Management and Monitoring Configuration Guide*.

syslog: Sends resource depletion alarms to the information center to encapsulate the alarms in log messages. For more information, see information center in *Network Management and Monitoring Configuration Guide*.

Usage guidelines

If you do not specify any keywords for the **undo resource-monitor output** command, the command disables resource depletion alarm output.

Examples

Specify the information center module as the output destination for resource depletion alarms.

```
<Switch> system-view
[Switch] resource-monitor output syslog
```

Related commands

resource-monitor minor resend enable

resource-monitor resource

10.1.49. resource-monitor resource

Use **resource-monitor resource** to set resource depletion thresholds.

Use **undo resource-monitor resource** to disable resource depletion thresholds.

Syntax

resource-monitor resource *resource-name* **slot** *slot-number* **cpu** *cpu-number* **by-percent minor-threshold** *minor-threshold* **severe-threshold** *severe-threshold*

undo resource-monitor resource *resource-name* **slot** *slot-number* **cpu** *cpu-number*

Default

The default settings vary by resource type. Use the **display resource-monitor** command to display the resource depletion thresholds.

Views

System view

Predefined user roles

network-admin

Parameters

resource-name: Specifies a resource type by its name. The values for this argument are case insensitive and cannot be abbreviated. Table 10-13 lists the resource types that can be monitored.

Table 10-13 Resource types that can be monitored

Resource type	Description
ac	Ethernet service instances.
agg_group	Aggregation group resources.

Resource type	Description
arp	ARP resources.
ecmpgroup	ECMP group resources.
mac	MAC address table resources.
mqcin	Inbound MQC resources.
mqcout	Outbound MQC resources.
nexthoppool1	Next-hop pool resources for the underlay network.
openflowin	OpenFlow resources.
pbr	PBR resources.
pfilterin	Inbound packet filter resources.
pfilterout	Outbound packet filter resources.
rport	Layer 3 Ethernet interface resources.
subrport	Layer 3 Ethernet subinterface resources.
vlan	VLANs.
vlaninterface	VLAN interface resources.
vrf	VPN instance resources.
vsi	VSIs.
vsiintf	VSI interface resources.

slot *slot-number*: Specifies an IRF member device by its member ID.

cpu *cpu-number*: Specifies a CPU by its number.

by-percent: Specifies resource depletion thresholds in percentage.

minor-threshold *minor-threshold*: Specifies the minor resource depletion threshold. To view the value range, enter a question mark (?) in the place of the *minor-threshold* argument.

severe-threshold *severe-threshold*: Specifies the severe resource depletion threshold. To view the value range, enter a question mark (?) in the place of the *severe-threshold* argument.

Usage guidelines

After you execute this command for a resource type, the device monitors the available amount of the type of resources. The device samples the available amount at intervals, compares the sample with the resource depletion thresholds to identify the resource depletion status, and sends alarms as configured.

Examples

Set the minor resource depletion threshold to 30% and the severe resource depletion threshold to 10% for ARP entry resources on slot 1.

```
<Switch> system-view
[Switch] resource-monitor resource arp slot 1 cpu 0 by-percent minor-threshold 30
severe-threshold 10
```

Related commands

display resource-monitor

resource-monitor minor resend enable

resource-monitor output

10.1.50. scheduler job

Use **scheduler job** to create a job and enter its view, or enter the view of an existing job.

Use **undo scheduler job** to delete a job.

Syntax

scheduler job *job-name*

undo scheduler job *job-name*

Default

No job exists.

Views

System view

Predefined user roles

network-admin

Parameters

job-name: Specifies the job name, a case-sensitive string of 1 to 47 characters.

Usage guidelines

A job can be referenced by multiple schedules. In job view, you can assign commands to the job.

Examples

Create a job named **backupconfig** and enter job view.

```
<Switch> system-view
[Switch] scheduler job backupconfig
[Switch-job-backupconfig]
```

Related commands

command

scheduler schedule

10.1.51. scheduler logfile size

Use **scheduler logfile size** to set the size of the job execution log file.

Syntax

scheduler logfile size *value*

Default

The size of the job execution log file is 16 KB.

Views

System view

Predefined user roles

network-admin

Parameters

value: Specifies the size of the job execution log file, in KB. The value range is 16 to 1024.

Usage guidelines

The job execution log file saves the execution information of jobs. If the file is full, old records are deleted to make room for new records. If the size of the log information to be written to the file is greater than the file size, the excessive information is not written to the file.

Examples

Set the size of the job execution log file to 32 KB.

```
<Switch> system-view
[Switch] scheduler logfile size 32
```

Related commands

display scheduler logfile

10.1.52. scheduler reboot at

Use **scheduler reboot at** to specify the reboot date and time.

Use **undo scheduler reboot** to delete the reboot schedule configuration.

Syntax

scheduler reboot at *time* [*date*]

undo scheduler reboot

Default

No reboot date or time is specified.

Views

User view

Predefined user roles

network-admin

Parameters

time: Specifies the reboot time in the *hh:mm* format. The value range for *hh* is 0 to 23. The value range for *mm* is 0 to 59.

date: Specifies the reboot date in the *MM/DD/YYYY* or *YYYY/MM/DD* format. The value range for *YYYY* is 2000 to 2035. The value range for *MM* is 1 to 12. The value range for *DD* varies by month.

Usage guidelines

CAUTION:
Device reboot interrupts network services.

When the *date* argument is not specified, the system uses the following rules to determine the reboot time:

- If the reboot time is later than the current time, a reboot occurs at the reboot time of the current day.
- If the reboot time is earlier than the current time, a reboot occurs at the reboot time the next day.

The device supports only one device reboot schedule. If you execute both the **scheduler reboot delay** and **scheduler reboot at** commands or execute one of the commands multiple times, the most recent configuration takes effect.

For data security, the system does not reboot at the reboot time if a file operation is being performed.

Examples

Configure the device to reboot at 12:00 p.m. This example assumes that the current time is 11:43 a.m. on June 6, 2015.

```
<Switch> scheduler reboot at 12:00
Reboot system at 12:00:00 06/06/2015 (in 0 hours and 16 minutes). Confirm? [Y/N]:
```

Related commands

scheduler reboot delay

10.1.53. scheduler reboot delay

Use **scheduler reboot delay** to specify the reboot delay time.

Use **undo scheduler reboot** to delete the reboot schedule configuration.

Syntax

scheduler reboot delay *time*

undo scheduler reboot

Default

No reboot delay time is specified.

Views

User view

Predefined user roles

network-admin

Parameters

time: Specifies the reboot delay time in the *hh:mm* or *mm* format. This argument can contain up to six characters. When in the *hh:mm* format, *mm* must be in the range of 0 to 59.

Usage guidelines

CAUTION:
Device reboot interrupts network services.

The device supports only one device reboot schedule. If you execute both the **scheduler reboot delay** and **schedule reboot at** commands or execute one of the commands multiple times, the most recent configuration takes effect.

For data security, the system does not reboot at the reboot time if a file operation is being performed.

Examples

Configure the device to reboot after 88 minutes. This example assumes that the current time is 11:48 a.m. on June 6, 2015.

```
<Switch> scheduler reboot delay 88
Reboot system at 13:16 06/06/2015(in 1 hours and 28 minutes). Confirm? [Y/N]:
```

10.1.54. scheduler schedule

Use **scheduler schedule** to create a schedule and enter its view, or enter the view of an existing schedule.

Use **undo scheduler schedule** to delete a schedule.

Syntax

scheduler schedule *schedule-name*

undo scheduler schedule *schedule-name*

Default

No schedule exists.

Views

System view

Predefined user roles

network-admin

Parameters

schedule-name: Specifies the schedule name, a case-sensitive string of 1 to 47 characters.

Usage guidelines

You can configure a schedule to have the device automatically run a command or a set of commands without administrative interference.

To configure a schedule:

1. Use the **scheduler job** command to create a job and enter job view.
2. Use the **command** command to assign commands to the job.
3. Use the **scheduler schedule** command to create a schedule and enter schedule view.
4. Use the **job** command to assign the job to the schedule. You can assign multiple jobs to a schedule. The jobs must already exist.
5. Use the **user-role** command to assign user roles to the schedule. You can assign up to 64 user roles to a schedule.
6. Use the **time at**, **time once**, or **time repeating** command to specify an execution time for the schedule. You can specify only one execution time for a schedule.

Examples

Create a schedule named **saveconfig**.

```
<Switch> system-view
[Switch] scheduler schedule saveconfig
```

Related commands

job

time at

time once

10.1.55. shutdown-interval

Use **shutdown-interval** to set the port status detection timer.

Use **undo shutdown-interval** to restore the default.

Syntax

shutdown-interval *interval*

undo shutdown-interval

Default

The port status detection timer setting is 30 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the port status detection timer value in seconds. The value range is 0 to 300. To disable port status detection, set this argument to 0.

Usage guidelines

The device starts a port status detection timer when a port is shut down by a protocol. Once the timer expires, the device brings up the port so the port status reflects the port's physical status.

If you change the timer setting during port detection, the device compares the new setting (T1) with the time that elapsed since the port was shut down (T).

If T < T1, the port will be brought up after T1 – T seconds.

If T ≥ T1, the port is brought up immediately.

For example, the timer setting is 30 seconds. If you change it to 10 seconds 2 seconds after the port is shut down, the port will come up 8 seconds later. If you change the timer setting to 2 seconds 10 seconds after the port is shut down, the port comes up immediately.

Examples

Set the port status detection timer to 100 seconds.

```
<Switch> system-view
[Switch] shutdown-interval 100
```

10.1.56. switch-mode

Use **switch-mode** to specify an operating mode for the device.

Syntax

switch-mode { **0** | **1** }

Default

The device operates in standard mode.

Views

System view

Predefined user roles

network-admin

Parameters

0: Specifies the standard mode.

1: Specifies the VXLAN mode.

Usage guidelines

Change to the operating mode takes effect after you reboot the device.

Examples

Set the operating mode to VXLAN mode for the device.

<Switch> system-view

[Switch] switch-mode 1

```
Reboot device to make the configuration take effect.
```

Related commands

display switch-mode status

10.1.57. sysname

Use **sysname** to set the device name.

Use **undo sysname** to restore the default.

Syntax

sysname *sysname*

undo sysname

Default

The default device name is the device name.

Views

System view

Predefined user roles

network-admin

Parameters

sysname: Specifies a name for the device, a string of 1 to 64 characters.

Usage guidelines

A device name identifies a device in a network and is used in CLI view prompts. For example, if the device name is **Sysname**, the user view prompt is <Sysname>.

Examples

Set the name of the device to **R2000**.

```
<Switch> system-view
[Switch] sysname R2000
[R2000]
```

10.1.58. temperature-limit

Use **temperature-limit** to set the temperature alarm thresholds.

Use **undo temperature-limit** to restore the default.

Syntax

temperature-limit slot *slot-number* **hotspot** *sensor-number lowlimit warninglimit* [*alarmlimit*]

undo temperature-limit slot *slot-number* **hotspot** *sensor-number*

Default

Switch	Sensor	Recommended value of warning temperature	Default value of warning temperature	Recommended value of alarm temperature	Default value of alarm temperature
QX-S5628GT-4X2Q	Hotspot 1	53	60	58	65
QX-S5648GT-4X2Q	Hotspot 1	59	60	64	65
QX-S5624GT-4X1C	Hotspot 1	52	66	57	71
QX-S5648GT-4X1C	Hotspot 1	56	61	61	66
QX-S5624GP-4X1C	Hotspot 1	54	62	59	68

NOTE:

It's recommended to change the preset temperature to a threshold value of the recommendation temperature from a threshold value of default.

Views

System view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID.

hotspot: Configures temperature alarm thresholds for hotspot sensors. A hotspot sensor is typically near the chip that generates a great amount of heat and used to monitor the chip.

sensor-number: Specifies a sensor by its number. To view the value range, enter a question mark (?) in the place of this argument.

lowlimit: Specifies the low-temperature threshold in Celsius degrees. The value range varies by temperature sensor. To view the value range, enter a question mark (?) in the place of this argument.

warninglimit: Specifies the high-temperature warning threshold in Celsius degrees. This threshold must be greater than the low-temperature threshold. To view the value range, enter a question mark (?) in the place of this argument.

alarmlimit: Specifies the high-temperature alarming threshold in Celsius degrees. This threshold must be greater than the warning threshold. To view the value range, a enter question mark (?) in the place of this argument.

Usage guidelines

When the device temperature drops below the low-temperature threshold or reaches the high-temperature warning or alarming threshold, the device performs the following operations:

- Sends log messages and traps.
- Sets LEDs on the device panel.

Examples

Set temperature alarm thresholds for hotspot sensor 1 in a slot.

```
<Sysname> system-view
[Switch] temperature-limit slot 1 hotspot 1 -10 50 60
```

Related commands

display environment

10.1.59. time at

Use **time at** to specify an execution date and time for a non-periodic schedule.

Use **undo time** to delete the execution date and time configuration for a non-periodic schedule.

Syntax

time at *time date*

undo time

Default

No execution time or date is specified for a non-periodic schedule.

Views

Schedule view

Predefined user roles

network-admin

Parameters

time: Specifies the schedule execution time in the *hh:mm* format. The value range for *hh* is 0 to 23. The value range for *mm* is 0 to 59.

date: Specifies the schedule execution date in the *MM/DD/YYYY* or *YYYY/MM/DD* format. The value range for *YYYY* is 2000 to 2035. The value range for *MM* is 1 to 12. The value range for *DD* varies by month.

Usage guidelines

The specified time (date plus time) must be later than the current system time.

The **time at** command, the **time once** command, and the **time repeating** command overwrite one another. The most recently configured command takes effect.

Examples

Configure the device to execute schedule **saveconfig** at 01:01 a.m. on May 11, 2015.

```
<Switch> system-view
[Switch] scheduler schedule saveconfig
[Switch-schedule-saveconfig] time at 1:1 2015/05/11
```

Related commands

scheduler schedule

10.1.60. time once

Use **time once** to specify one or more execution days and the execution time for a non-periodic schedule.

Use **undo time** to delete the execution day and time configuration for a non-periodic schedule.

Syntax

time once at *time* [**month-date** *month-day* | **week-day** *week-day*&<1-7>]

time once delay *time*

undo time

Default

No execution time or day is specified for a non-periodic schedule.

Views

Schedule view

Predefined user roles

network-admin

Parameters

at *time*: Specifies the execution time in the *hh:mm* format. The value range for *hh* is 0 to 23. The value range for *mm* is 0 to 59.

month-date *month-day*: Specifies a day in the current month, in the range of 1 to 31. If you specify a day that does not exist in the current month, the configuration takes effect on that day in the next month.

week-day *week-day*&<1-7>: Specifies a space-separated list of up to seven week days for the schedule. Valid week day values include **Mon**, **Tue**, **Wed**, **Thu**, **Fri**, **Sat**, and **Sun**.

delay *time*: Specifies the delay time for executing the schedule, in the *hh:mm* or *mm* format. This argument can have up to six characters. When in the *hh:mm* format, *mm* must be in the range of 0 to 59.

Usage guidelines

If the specified time has already occurred, the schedule will be executed at the specified time the following day.

If the day in the month has already occurred, the schedule will be executed at the specified day in the following month.

If the specified day in a week has already occurred, the schedule will be executed at the specified day in the following week.

The **time at** command, the **time once** command, and the **time repeating** command overwrite one another. The most recently configured command takes effect.

Examples

Configure the device to execute schedule **saveconfig** once at 15:00.

```
<Switch> system-view
[Switch] scheduler schedule saveconfig
[Switch-schedule-saveconfig] time once at 15:00
```

```
Schedule starts at 15:00 5/11/2011.
```

Configure the device to execute schedule **saveconfig** once at 15:00 on the coming 15th day in a month.

```
<Switch> system-view
[Switch] scheduler schedule saveconfig
[Switch-schedule-saveconfig] time once at 15:00 month-date 15
```

Configure the device to execute schedule **saveconfig** at 12:00 p.m. on the coming Monday and Friday.

```
<Switch> system-view
[Switch] scheduler schedule saveconfig
[Switch-schedule-saveconfig] time once at 12:00 week-day mon fri
```

Configure the device to execute schedule **saveconfig** after 10 minutes.

```
<Switch> system-view
[Switch] scheduler schedule saveconfig
[Switch-schedule-saveconfig] time once delay 10
```

Related commands

scheduler schedule

10.1.61. time repeating

Use **time repeating** to specify an execution time table for a periodic schedule.

Use **undo time** to delete the execution time table configuration for a periodic schedule.

Syntax

time repeating [**at** *time* [*date*]] **interval** *interval*

time repeating at *time* [**month-date** [*month-day* | **last**] | **week-day** *week-day*&<1-7>]

undo time

Default

No execution time table is specified for a periodic schedule.

Views

Schedule view

Predefined user roles

network-admin

Parameters

at *time*: Specifies the execution time in the *hh:mm* format. The value range for *hh* is 0 to 23. The value range for *mm* is 0 to 59. If you do not specify this option, the current system time is used as the execution time.

date: Specifies the start date for the periodic schedule, in the *MM/DD/YYYY* or *YYYY/MM/DD* format. The value range for *YYYY* is 2000 to 2035. The value range for *MM* is 1 to 12. The value range for *DD* varies by month. If you do not specify this argument, the execution start date is the first day when the specified time arrives.

interval *interval*: Specifies the execution time interval in the *hh:mm or mm* format. This argument can have up to six characters. When in the *hh:mm* format, *mm* must be in the range of 0 to 59. When in the *mm* format, this argument must be equal to or greater than 1 minute.

month-date [*month-day* | **last**]: Specifies a day in a month, in the range 1 to 31. The **last** keyword indicates the last day of a month. If you specify a day that does not exist in a month, the configuration takes effect on that day in the next month.

week-day *week-day&<1-7>*: Specifies a space-separated list of up to seven week days for the schedule. Valid week day values include **Mon**, **Tue**, **Wed**, **Thu**, **Fri**, **Sat**, and **Sun**.

Usage guidelines

The **time repeating** [**at** *time* [*date*]] **interval** *interval* command configures the device to execute a schedule at intervals from the specified time on.

The **time repeating at** *time* [**month-date** [*month-day* | **last**] | **week-day** *week-day&<1-7>*] command configures the device to execute a schedule at the specified time on every specified day in a month or week.

The **time at** command, the **time once** command, and the **time repeating** command overwrite one another, whichever is configured most recently takes effect.

Examples

Configure the device to execute schedule **saveconfig** once an hour from 8:00 a.m. on.

```
<Switch> system-view
[Switch] scheduler schedule saveconfig
[Switch-schedule-saveconfig] time repeating at 8:00 interval 60
```

Configure the device to execute schedule **saveconfig** at 12:00 p.m. every day.

```
<Switch> system-view
[Switch] scheduler schedule saveconfig
[Switch-schedule-saveconfig] time repeating at 12:00
```

Configure the device to execute schedule **saveconfig** at 8:00 a.m. on the 5th of every month.

```
<Switch> system-view
[Switch] scheduler schedule saveconfig
[Switch-schedule-saveconfig] time repeating at 8:00 month-date 5
```

Configure the device to execute schedule **saveconfig** at 8:00 a.m. on the last day of every month.

```
<Switch> system-view
[Switch] scheduler schedule saveconfig
[Switch-schedule-saveconfig] time repeating at 8:00 month-date last
```

Configure the device to execute schedule **saveconfig** at 8:00 a.m. every Friday and Saturday.

```
<Switch> system-view
[Switch] scheduler schedule saveconfig
[Switch-schedule-saveconfig] time repeating at 8:00 week-day fri sat
```

Related commands

scheduler schedule

10.1.62. usb disable

Use **usb disable** to disable USB interfaces.

Use **undo usb disable** to enable USB interfaces.

Syntax

usb disable

undo usb disable

Default

All USB interfaces are enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

You can use USB interfaces to upload or download files. By default, all USB interfaces are enabled.

Before executing this command, use the **umount** command to unmount all USB file systems.

Examples

Enable USB interfaces.

```
<Switch> system-view
[Switch] undo usb disable
```

10.1.63. user-role

Use **user-role** to assign user roles to a schedule.

Use **undo user-role** to remove user roles from a schedule.

Syntax

user-role *role-name*

undo user-role *role-name*

Default

A schedule has the user roles of the schedule creator.

Views

Schedule view

Predefined user roles

network-admin

Parameters

role-name: Specifies a user role name, a case-sensitive string of 1 to 63 characters. The user role can be user-defined or predefined. Predefined user roles include network-admin, network-operator, and level-0 to level-15.

Usage guidelines

A schedule must have one or more user roles. A command in a schedule can be executed if it is permitted by one or more user roles of the schedule. For more information about user roles, see the RBAC configuration in *Fundamentals Configuration Guide*.

A schedule can have a maximum of 64 user roles. After the limit is reached, you cannot assign additional user roles to the schedule.

Examples

Assign user role **rolename** to schedule **test**.

```
<Switch> system-view
[Switch] scheduler schedule test
```

```
[Switch-schedule-test] user-role rolename
```

Related commands

command

scheduler schedule

Contents

A page of this section is **1-x-x**

11. Python commands 11-1
11.1. Python commands 11-1
11.1.1. exit() 11-1
11.1.2. python 11-1
11.1.3. python *filename* 11-2

11. Python commands

11.1. Python commands

11.1.1. exit()

Use **exit()** to exit the Python shell.

Syntax

exit()

Views

Python shell

Predefined user roles

network-admin

Usage guidelines

To return to user view from the Python shell, you cannot use the **quit** command. You must use the **exit()** command.

Examples

Exit the Python shell.

```
Python 2.7.3 (default)
[GCC 4.4.1] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>>
>>> exit()
<Switch>
```

11.1.2. python

Use **python** to enter the Python shell.

Syntax

python

Views

User view

Predefined user roles

network-admin

Usage guidelines

In the Python shell, you can use the following items:

- Python 2.7 commands.
- Python 2.7 standard API.
- Comware 7 extended API.

Examples

Enter the Python shell.

```
<Switch> python
Python 2.7.3 (default)
[GCC 4.4.1] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

11.1.3. python *filename*

Use **python** *filename* to execute a Python script.

Syntax

python *filename* [*param*]

Views

User view

Predefined user roles

network-admin

Parameters

filename: Specifies the name of a Python script on a storage medium of the device. The script name is case sensitive and must use the extension .py. The extension .py is case insensitive.

param: Specifies the parameters to be passed to the script. To enter multiple parameters, use spaces as the delimiter.

Usage guidelines

You cannot perform any operations while you are executing a Python script.

Make sure the statements in the script meet the syntax requirements. The system stops executing a Python script if it finds a statement with syntax errors.

When executing a script, the system uses the defaults for interactive statements. The system does not stop for human input.

Examples

Execute Python script **test.py**.

```
<Switch> python test.py 1 2
['/flash:/test.py', '1', '2']
```

Contents

A page of this section is **1-x-x**

12. Automatic configuration commands 12-1
12.1. Automatic configuration commands 12-1
12.1.1. autodeploy udisk enable 12-1

12. Automatic configuration commands

12.1. Automatic configuration commands

12.1.1. autodeploy udisk enable

Use **autodeploy udisk enable** to enable USB-based automatic configuration.

Use **undo autodeploy udisk enable** to disable USB-based automatic configuration.

Syntax

autodeploy udisk enable

undo autodeploy udisk enable

Default

USB-based automatic configuration is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command is supported only if the device has a USB interface.

Examples

Disable USB-based automatic configuration.

```
<Sysname> system-view
[Sysname] undo autodeploy udisk enable
```

QX-S5600G Series Ethernet Switches

Command References

2. IRF

This manual is including the following chapters.

01-IRF commands

Contents

A page of this section is **2-x-x**

1. IRF commands ····· 1-1
1.1. IRF commands ····· 1-1
1.1.1. display irf ····· 1-1
1.1.2. display irf configuration ····· 1-2
1.1.3. display irf link ····· 1-3
1.1.4. display irf topology ····· 1-4
1.1.5. display mad ····· 1-4
1.1.6. irf auto-update enable ····· 1-7
1.1.7. irf domain ····· 1-8
1.1.8. irf link-delay ····· 1-9
1.1.9. irf mac-address persistent ····· 1-9
1.1.10. irf member description ····· 1-10
1.1.11. irf member priority ····· 1-11
1.1.12. irf member renumber ····· 1-12
1.1.13. irf-port ····· 1-13
1.1.14. irf-port-configuration active ····· 1-13
1.1.15. mad arp enable ····· 1-14
1.1.16. mad bfd enable ····· 1-16
1.1.17. mad enable ····· 1-17
1.1.18. mad exclude interface ····· 1-18
1.1.19. mad ip address ····· 1-19
1.1.20. mad restore ····· 1-20
1.1.21. port group interface ····· 1-21

1. IRF commands

1.1. IRF commands

1.1.1. display irf

Use **display irf** to display IRF fabric information.

Syntax

display irf

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Table 1-1 shows the fields of IRF fabric information.

Table 1-1 Command output

Field	Description
MemberID	IRF member ID: • ID of the master is prefixed with an asterisk (*) sign. • ID of the device where you are logged in is prefixed with a plus (+) sign.
Role	Role of the member device in the IRF fabric: • **Standby**—Subordinate device. • **Master**—Master device. • **Loading**—The device is loading software images.
Priority	IRF member priority.
CPU-MAC	MAC address of the CPU in the device.
Description	Description you have configured for the member device. • If no description is configured, this field displays a dashed line (-----). • If the description exceeds the maximum number of characters that can be displayed, an ellipsis (…) is displayed in place of the exceeding text. To display the complete description, use the **display current-configuration** command.
Auto upgrade	Status of the software auto-update feature: • **yes**—Enabled. • **no**—Disabled.
MAC persistent	IRF bridge MAC persistence setting: • **6 min**—Bridge MAC address of the IRF fabric remains unchanged for 6 minutes after the address owner leaves. • **always**—Bridge MAC address of the IRF fabric does not

Field	Description
	change after the address owner leaves. • **no**—Bridge MAC address of the current master replaces the original bridge MAC address as soon as the owner of the original address leaves.
Domain ID	Domain ID of the IRF fabric. The domain ID you assign to an IRF fabric must uniquely identify the fabric in a multi-IRF fabric network.

Related commands

display irf configuration

display irf topology

1.1.2. display irf configuration

Use **display irf configuration** to display basic IRF settings for each member device.

Syntax

display irf configuration

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display basic IRF settings for all members.

```
<Switch> display irf configuration
 MemberID  NewID    IRF-Port1                    IRF-Port2
 1         1        Ten-GigabitEthernet1/0/49    Ten-GigabitEthernet1/0/51
 2         2        Ten-GigabitEthernet2/0/49    Ten-GigabitEthernet2/0/51
                    Ten-GigabitEthernet2/0/50
 4         4        Ten-GigabitEthernet4/0/49    Ten-GigabitEthernet4/0/51
                                                 Ten-GigabitEthernet4/0/52
```

Table 1-2 Command output

Field	Description
MemberID	Current member ID of the device.
NewID	Member ID assigned to the device. This member ID takes effect at reboot.
IRF-Port1	Physical interfaces bound to IRF-port 1. This field displays **disable** if no physical interfaces are bound to the IRF port.
IRF-Port2	Physical interfaces bound to IRF-port 2. This field displays **disable** if no physical interfaces are bound to the IRF port.

Related commands

display irf

display irf topology

1.1.3. display irf link

Use **display irf link** to display IRF link information.

Syntax

display irf link

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display IRF link information.

```
<Switch> display irf link
Member 1
 IRF Port     Interface                           Status
 1            disable                             --
 2            Ten-GigabitEthernet1/0/49           UP
              Ten-GigabitEthernet1/0/50           ADM
Member 2
 IRF Port     Interface                          Status
 1            Ten-GigabitEthernet2/0/49           UP
              Ten-GigabitEthernet2/0/50           DOWN
 2            disable                            --
```

Table 1-3 Command output

Field	Description
Member *ID*	IRF member ID.
IRF Port	IRF port number: • **1**—IRF-port 1. • **2**—IRF-port 2.
Interface	Physical interfaces bound to the IRF port. This field displays **disable** if no physical interfaces have been bound to the IRF port.
Status	Link state of the IRF physical interface: • **UP**—The link is up. • **DOWN**—The link is down. • **ADM**—The interface has been manually shut down by using the **shutdown** command. • **ABSENT**—Expansion interface card that hosts the interface is not present.

1.1.4. display irf topology

Use **display irf topology** to display IRF fabric topology information.

Syntax

display irf topology

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Table 1-4 shows the fields of IRF fabric information.

Table 1-4 Command output

Field	Description
IRF-Port1	Information about IRF-port 1, including its link state and neighbor.
IRF-Port2	Information about IRF-port 2, including its link state and neighbor.
MemberID	IRF member ID.

Link	Link state of the IRF port:
	• **UP**—The IRF link is up.
	• **DOWN**—The IRF link is down because the port has no physical link or has not been activated by the **irf-port-configuration active** command.
	• **DIS**—No physical interfaces have been bound to the IRF port.
	• **TIMEOUT**—IRF hello interval has timed out.
	• **ISOLATE**—The device is isolated from the IRF fabric. This issue might be caused by the following reasons:
	  ○ The IRF fabric does not support the device model.
	  ○ The maximum number of member devices has exceeded the upper limit.

neighbor	IRF member ID of the device connected to the IRF port. This field displays three hyphens (---) if no device is connected to the port.
Belong To	IRF fabric that has the device, represented by the CPU MAC address of the master in the IRF fabric.

Related commands

display irf

display irf configuration

1.1.5. display mad

Use **display mad** to display MAD status and settings.

Syntax

display mad [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

verbose: Displays detailed MAD information. If you do not specify this keyword, the command only displays whether a MAD mechanism is enabled or disabled.

Examples

Display brief MAD information.

```
<Switch> display mad
MAD ARP enabled.
MAD ND disabled.
MAD LACP disabled.
MAD BFD disabled.
```

Display detailed MAD information.

```
<Switch> display mad verbose
Multi-active recovery state: No
Excluded ports (user-configured):
  Bridge-Aggregation4
  Vlan-interface999
Excluded ports (system-configured):
  IRF physical interfaces:
    Ten-GigabitEthernet1/0/49
    Ten-GigabitEthernet1/0/50
    Ten-GigabitEthernet1/0/51
    Ten-GigabitEthernet1/0/52
  BFD MAD interfaces:
    GigabitEthernet1/0/10
    GigabitEthernet2/0/10
    Vlan-interface3
  Member interfaces of excluded interface Bridge-Aggregation 4:
    GigabitEthernet1/0/11
    GigabitEthernet2/0/11
MAD ARP enabled interface:
  Vlan-interface2
MAD ND enabled interface:
  Vlan-interface2
MAD LACP enabled interface: Bridge-Aggregation 1
  MAD status                 : Normal
  Member ID       Port                       MAD status
  1               GigabitEthernet1/0/1       Normal
  2               GigabitEthernet2/0/1       Normal
```

```
MAD BFD enabled interface: VLAN-interface 3
  MAD status                 : Normal
  Member ID   MAD IP address       Neighbor    MAD status
  1           192.168.1.1/24       2           Normal
  2           192.168.1.2/24       1           Normal
```

Table 1-5 Command output

Field	Description
MAD ARP enabled.	Status of ARP MAD. This field displays **MAD ARP disabled** if ARP MAD is disabled.
MAD ND disabled.	Status of ND MAD. This field displays **MAD ND enabled** if ND MAD is enabled.
MAD LACP disabled.	Status of LACP MAD. This field displays **MAD LACP enabled** if LACP MAD is enabled.
MAD BFD disabled.	Status of BFD MAD. This field displays **MAD BFD enabled** if BFD MAD is enabled.
Multi-active recovery state	Whether the IRF fabric is in Recovery state: • **Yes**—The IRF fabric is in Recovery state. When MAD detects that an IRF fabric has split into multiple IRF fabrics, it allows one fabric to forward traffic. All the other IRF fabrics are set to the Recovery state. In Recovery state, MAD shuts down all service interfaces in the fabric except for the system- and user-excluded service interfaces. • **No**—The IRF fabric is not in Recovery state. It is active and can forward traffic.
Excluded ports (user-configured)	Service interfaces manually configured to not shut down when the IRF fabric transits to the Recovery state.

Excluded ports (system-configured)	Service interfaces set to not shut down by the system when the IRF fabric transits to the Recovery state. These service interfaces are not manually configured.
	• IRF physical interfaces.
	• BFD MAD interfaces:
	  ○ VLAN interfaces used for BFD MAD and the Layer 2 Ethernet ports in the VLANs.
	  ○ Management Ethernet ports used for BFD MAD.
	• Member interfaces of a Layer 2 aggregate interface if the aggregate interface is excluded from the MAD shutdown action.

MAD ARP enabled interface:	Interfaces on which ARP MAD is enabled.
MAD ND enabled interface:	Interfaces on which ND MAD is enabled.
MAD LACP enabled interface	Interface on which LACP MAD is enabled. This field is displayed for each interface enabled with LACP MAD.
MAD status	LACP MAD operating status: • **Normal**—LACP MAD is operating correctly. • **Faulty**—LACP MAD is not operating correctly. Verify the following items: ○ Verify that the ports on LACP MAD links are up.

Field	Description
	○ Verify that the intermediate device supports extended LACPDUs. ○ Verify that all member devices have member ports used for LACP MAD.
Member ID Port MAD status	LACP MAD details: • **Member ID**—IRF member ID of a device. • **Port**—Member ports of the aggregate interface used for LACP MAD. • **MAD status**—LACP MAD operating state on a member port. Options include **Normal** and **Faulty**.
MAD BFD enabled interface:	Layer 3 interface on which BFD MAD is enabled.
MAD status	BFD MAD operating status: • **Normal**—BFD MAD is operating correctly. • **Faulty**—BFD MAD is not operating correctly. Check the BFD MAD link connectivity. • **N/A**—BFD MAD link status cannot be detected. If BFD MAD is enabled on a management Ethernet port, it is normal that this field displays **N/A**.
Member ID MAD IP address Neighbor MAD status	BFD MAD details: • **Member ID**—IRF member ID of the local device. • **MAD IP address**—MAD IP address of a member device. • **Neighbor**—IRF member ID of the neighboring member device. • **MAD status**—BFD MAD link state. Options include **Normal** and **Faulty**. • **N/A**—BFD MAD link status cannot be detected. If BFD MAD is enabled on a management Ethernet port, it is normal that this field displays **N/A**.

1.1.6. irf auto-update enable

Use **irf auto-update enable** to enable the software auto-update feature.

Use **undo irf auto-update enable** to disable the software auto-update feature.

Syntax

irf auto-update enable

undo irf auto-update enable

Default

Software auto-update is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command automatically propagates the current software images of the master device in the IRF fabric to any devices you are adding to the IRF fabric.

To ensure a successful software update, verify that the new device you are adding to the IRF fabric has sufficient storage space for the new software images. If sufficient storage space is not available, the device automatically deletes the current software images. If the reclaimed space is still insufficient, the device cannot complete the auto-update. You must reboot the device, and then access the BootWare menu to delete files.

Examples

Enable the software auto-update feature.

```
<Switch> system-view
[Switch] irf auto-update enable
```

1.1.7. irf domain

Use **irf domain** to assign a domain ID to the IRF fabric.

Use **undo irf domain** to restore the default.

Syntax

irf domain *domain-id*

undo irf domain

Default

The IRF domain ID is 0.

Views

System view

Predefined user roles

network-admin

Parameters

domain-id: Specifies a domain ID for the IRF fabric. The value range is 0 to 4294967295.

Usage guidelines

One IRF fabric forms one IRF domain. IRF uses IRF domain IDs to uniquely identify IRF fabrics and prevent IRF fabrics from interfering with one another.

If one IRF fabric uses another IRF fabric as the intermediate device for LACP MAD, or ARP MAD, you must assign the two IRF fabrics different domain IDs for correct split detection. False detection causes IRF split.

An IRF fabric has only one IRF domain ID. You can change the IRF domain ID by using the following commands: **irf domain**, **mad enable**, **mad arp enable**, or **mad nd enable**. The IRF domain IDs configured by using these commands overwrite each other.

Examples

Set the IRF domain ID to 10.

```
<Switch> system-view
[Switch] irf domain 10
```

1.1.8. irf link-delay

Use **irf link-delay** to set a delay for the IRF ports to report a link down event.

Use **undo irf link-delay** to set 4 seconds.

Syntax

irf link-delay *interval*

undo irf link-delay

Default

The delay time is 500 milliseconds.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Sets the IRF link down report delay, in the range of 0 to 10000 milliseconds. If the interval is set to 0, link down events are reported without any delay.

Usage guidelines

When you configure the IRF link down report delay, follow these restrictions and guidelines:

- Make sure the IRF link down report delay is shorter than the heartbeat or hello timeout settings of upper-layer protocols (for example, CFD and OSPF). If the report delay is longer than the timeout setting of a protocol, unnecessary recalculations might occur.
- Set the delay to 0 seconds in the following situations:
  - The IRF fabric requires a fast master/subordinate or IRF link switchover.
  - The RRPP, BFD, or GR feature is used.
  - You want to shut down an IRF physical interface or reboot an IRF member device. (After you complete the operation, reconfigure the delay depending on the network condition.)

Using **undo irf link-delay interval** cannot restore the default. You must use the **irf link-delay interval 500** command to reconfigure the irf link-delay.

Examples

Set the IRF link down report delay to 300 milliseconds.

```
<Switch> system-view
[Switch] irf link-delay 300
```

1.1.9. irf mac-address persistent

Use **irf mac-address persistent** to configure IRF bridge MAC persistence.

Use **undo irf mac-address persistent** to disable IRF bridge MAC persistence.

Syntax

irf mac-address persistent { **always** | **timer** }

undo irf mac-address persistent

Default

The IRF bridge MAC address remains unchanged for 6 minutes after the address owner leaves.

Views

System view

Predefined user roles

network-admin

Parameters

always: Enables the IRF bridge MAC address to be permanent. The IRF bridge MAC address does not change after the address owner leaves the fabric.

timer: Enables the IRF bridge MAC address to remain unchanged for 6 minutes after the address owner leaves. If the owner rejoins the IRF fabric with the time limit, the IRF bridge MAC address does not change. If the owner does not rejoin the IRF fabric within the time limit, the IRF fabric uses the bridge MAC address of the current master as the bridge MAC address.

Usage guidelines

If the **undo** form of this command is used, bridge MAC address of the current master replaces the original IRF bridge MAC as soon as the original address owner leaves.

This command does not take effect if the IRF bridge MAC address is configured by using the **irf mac-address** *mac-address* command.

If ARP MAD is used with the spanning tree feature, disable IRF bridge MAC persistence by using the **undo irf mac-address persistent** command. In addition, do not specify an IRF bridge MAC address by using the **irf mac-address** *mac-address* command.

If the IRF fabric uses a daisy-chain topology and has aggregate links with upstream or downstream devices, do not execute the **undo irf mac-address persistent** command. Any violation results in transmission delay or packet loss after the address owner leaves or reboots.

If the IRF fabric has multichassis aggregate links, do not use the **undo irf mac-address persistent** command. A violation might cause traffic disruption.

By default, an IRF fabric uses the bridge MAC address of the master device as its bridge MAC address.

On a switched LAN, the IRF bridge MAC address must be unique for correct traffic transmission.

When IRF fabrics merge, IRF ignores the IRF bridge MAC address and checks the bridge MAC address of each member device in the IRF fabrics. IRF merge fails if any two member devices have the same bridge MAC address.

Examples

Enable the IRF bridge MAC address to persist forever.

```
<Switch> system-view
[Switch] irf mac-address persistent always
```

1.1.10. irf member description

Use **irf member description** to configure a description for an IRF member device.

Use **undo irf member description** to restore the default.

Syntax

irf member *member-id* **description** *text*

undo irf member *member-id* **description**

Default

No description is configured for an IRF member device.

Views

System view

Predefined user roles

network-admin

Parameters

member-id: Specifies the ID of an IRF member.

text: Specifies a description, a string of 1 to 127 characters.

Examples

Configure the description as **F1Num001** for IRF member 1.

```
<Switch> system-view
[Switch] irf member 1 description F1Num001
```

1.1.11. irf member priority

Use **irf member priority** to change the priority of an IRF member device.

Use **undo irf member priority** to restore the default.

Syntax

irf member *member-id* **priority** *priority*

undo irf member *member-id* **priority**

Default

The IRF member priority is 1.

Views

System view

Predefined user roles

network-admin

Parameters

member-id: Specifies an IRF member ID. The value range for IRF member IDs is 1 to 10.

priority: Sets priority in the range of 1 to 32. The greater the priority value, the higher the priority. A member with higher priority is more likely to be the master.

Usage guidelines

The new priority setting takes effect at the next master election, but it does not trigger a master election.

Examples

Set the priority of IRF member 2 to 32.

```
<Switch> system-view
[Switch] irf member 2 priority 32
```

1.1.12. irf member renumber

Use **irf member renumber** to change the member ID of an IRF member device.

Use **undo irf member renumber** to restore the previous IRF member ID of the device.

Syntax

irf member *member-id* **renumber** *new-member-id*

undo irf member *member-id* **renumber**

Default

The IRF member ID is 1.

Views

System view

Predefined user roles

network-admin

Parameters

member-id: Specifies the ID of an IRF member. The value range for IRF member IDs is 1 to 10.

new-member-id: Assigns a new ID to the IRF member. The value range for IRF member IDs is 1 to 10.

Usage guidelines

CAUTION:
IRF member ID change can invalidate member ID-related settings, including interface and file path settings, and cause data loss. Make sure you fully understand its impact on your live network.

To have the new ID take effect, you must reboot the IRF member. To cancel the member ID change before you reboot the member device, use the **undo irf member renumber** command. In the command, set the new member ID to be the same as the old member ID.

When adding a device into an IRF fabric, you must assign a unique IRF member ID to the device. If its IRF member ID has been used in the IRF fabric, the device cannot join the IRF fabric.

Interchanging member IDs between IRF member devices might cause undesirable configuration changes and data loss. For example, the IRF member IDs of Device A and Device B are 2 and 3, respectively. After you interchange their member IDs, their port settings also interchange.

Examples

Change the ID of an IRF member device from 1 to 2.

```
<Switch> display irf
[Switch] irf member 1 renumber 2
Renumbering the member ID may result in configuration change or loss. Continue?[Y/N]Y
```

Before rebooting the device, cancel the change in the preceding example.

```
[Switch] undo irf member 1 renumber
Renumbering the member ID may result in configuration change or loss. Continue?[Y/N]y
```

If you reboot the device after executing the **irf member 1 renumber 2** command, the device member ID changes to 2 at system reboot. Using **undo irf member 1 renumber** cannot restore the member ID to 1. You must use the **irf member 2 renumber 1** command to reconfigure the member ID.

1.1.13. irf-port

Use **irf-port** to enter IRF port view.

Use **undo irf-port** to remove all port bindings on an IRF port.

Syntax

irf-port *member-id/irf-port-number*

undo irf-port *member-id/irf-port-number*

Views

System view

Predefined user roles

network-admin

Parameters

member-id: Specifies an IRF member device by its member ID.

irf-port-number: Specifies an IRF port on the member device. The *irf-port-number* argument represents the IRF port index and must be 1 or 2.

Usage guidelines

To bind physical interfaces to an IRF port, you must enter IRF port view.

Examples

Enter IRF-port 2/1 view.

```
<Switch> system-view
[Switch] irf-port 2/1
[Switch-irf-port2/1]
```

Related commands

port group interface

1.1.14. irf-port-configuration active

Use **irf-port-configuration active** to activate IRF ports.

Syntax

irf-port-configuration active

Views

System view

Predefined user roles

network-admin

Usage guidelines

After connecting the physical interfaces between two devices and binding them to the correct IRF ports, you must use this command to activate the settings on the IRF ports. This command merges the two devices into one IRF fabric.

The system activates the IRF port settings automatically in the following situations:

- The configuration file that the device starts with contains IRF port bindings.

- You are binding physical interfaces to an IRF port after an IRF fabric is formed.

Examples

To configure and activate IRF-port 1/2 when the port is in DIS state:

Bind Ten-GigabitEthernet 1/0/49 to IRF-port 1/2.

```
<Switch> system-view
[Switch] interface ten-gigabitethernet 1/0/49
[Switch-Ten-GigabitEthernet1/0/49] shutdown
[Switch-Ten-GigabitEthernet1/0/49] quit
[Switch] irf-port 1/2
[Switch-irf-port1/2] port group interface ten-gigabitethernet 1/0/49
You must perform the following tasks for a successful IRF setup:
Save the configuration after completing IRF configuration.
Execute the "irf-port-configuration active" command to activate the IRF ports.
[Switch-irf-port1/2] quit
[Switch] interface ten-gigabitethernet 1/0/49
[Switch-Ten-GigabitEthernet1/0/49] undo shutdown
[Switch-Ten-GigabitEthernet1/0/49] quit
```

Save the configuration so the IRF port settings can take effect after the device reboots.

```
[Switch] save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
flash:/startup.cfg exists, overwrite? [Y/N]:y
Validating file. Please wait.....................
Saved the current configuration to mainboard device successfully.
```

Activate the IRF port.

```
[Switch] irf-port-configuration active
```

1.1.15. mad arp enable

Use **mad arp enable** to enable ARP MAD.

Use **undo mad arp enable** to disable ARP MAD.

Syntax

mad arp enable

undo mad arp enable

Default

ARP MAD is disabled.

Views

Management Ethernet interface view

VLAN interface view

Predefined user roles

network-admin

Usage guidelines

Do not configure ARP MAD together with LACP MAD or BFD MAD, because they handle collisions differently.

When you configure ARP MAD on a VLAN interface, follow these restrictions and guidelines:

Category	Restrictions and guidelines

ARP MAD VLAN	• Do not enable ARP MAD on VLAN-interface 1.
	• If you are using an intermediate device, perform the following tasks:
	  ○ On both the IRF fabric and the intermediate device, create a VLAN for ARP MAD.
	  ○ On both the IRF fabric and the intermediate device, assign the ports of ARP MAD links to the ARP MAD VLAN.
	  ○ On the IRF fabric, create a VLAN interface for the ARP MAD VLAN.
	• As a best practice, do not use the ARP MAD VLAN for any other purposes.

ARP MAD and feature configuration	If an intermediate device is used, make sure the following requirements are met: • Run the spanning tree feature between the IRF fabric and the intermediate device to ensure that there is only one ARP MAD link in forwarding state. For more information about the spanning tree feature and its configuration, see *Layer 2—LAN Switching Configuration Guide*. • Enable the IRF fabric to change its bridge MAC address as soon as the address owner leaves. • If the intermediate device is also an IRF fabric, assign the two IRF fabrics different domain IDs for correct split detection.

When you configure ARP MAD that uses management Ethernet ports, follow these restrictions and guidelines:

Category	Restrictions and guidelines
Management Ethernet ports for ARP MAD	Connect a management Ethernet port on each member device to the common Ethernet ports on the intermediate device.
ARP MAD VLAN	On the intermediate device, create a VLAN for ARP MAD, and assign the ports used for ARP MAD to the VLAN. On the IRF fabric, you do not need to assign the management Ethernet ports to the VLAN.
ARP MAD and feature configuration	• Enable the IRF fabric to change its bridge MAC address as soon as the address owner leaves. • If the intermediate device is also an IRF fabric, assign the two IRF fabrics different domain IDs for correct split detection.

When you use the **mad arp enable** command, the system prompts you to enter a domain ID. If you do not want to change the current domain ID, press **enter** at the prompt.

An IRF fabric has only one IRF domain ID. You can change the IRF domain ID by using the following commands: **irf domain**, **mad enable**, **mad arp enable**, or **mad nd enable**. The IRF domain IDs configured by using these commands overwrite each other.

Examples

Enable ARP MAD on VLAN-interface 3.

```
<Switch> system-view
[Switch] interface vlan-interface 3
[Switch-Vlan-interface3] mad arp enable
You need to assign a domain ID (range: 0-4294967295)
[Current domain is: 0]: 1
The assigned domain ID is: 1
```

Related commands

irf domain

1.1.16. mad bfd enable

Use **mad bfd enable** to enable BFD MAD.

Use **undo mad bfd enable** to disable BFD MAD.

Syntax

mad bfd enable

undo mad bfd enable

Default

BFD MAD is disabled.

Views

VLAN interface view

Management Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

Do not configure BFD MAD together with ARP MAD, because they handle collisions differently.

When you configure BFD MAD on a VLAN interface, follow these guidelines:

Category	Restrictions and guidelines

BFD MAD VLAN	• Do not enable BFD MAD on VLAN-interface 1.
	• If you are using an intermediate device, perform the following tasks:
	  ○ On both the IRF fabric and the intermediate device, create a VLAN for BFD MAD.
	  ○ On both the IRF fabric and the intermediate device, assign the ports of BFD MAD links to the BFD MAD VLAN.
	  ○ On the IRF fabric, create a VLAN interface for the BFD MAD VLAN.
	  ○ Make sure the IRF fabrics on the network use different BFD MAD VLANs.
	• Make sure the BFD MAD VLAN contains only ports on the BFD MAD links. Exclude a port from the BFD MAD VLAN if the port is not on the BFD MAD link. For example, if you have assigned the port to all VLANs by using the **port trunk**

Category	Restrictions and guidelines
	permit vlan all command, use the **undo port trunk permit** command to exclude the port from the BFD MAD VLAN.
BFD MAD VLAN and feature compatibility	Do not use the BFD MAD VLAN for any purposes other than configuring BFD MAD. • Configure only the **mad bfd enable** and **mad ip address** commands on the BFD MAD-enabled VLAN interface. If you configure other features, both BFD MAD and other features on the interface might run incorrectly. • Disable the spanning tree feature on any Layer 2 Ethernet ports in the BFD MAD VLAN. The MAD feature is mutually exclusive with the spanning tree feature.
MAD IP address	• To avoid problems, only use the **mad ip address** command to configure IP addresses on the BFD MAD-enabled VLAN interface. Do not configure an IP address by using the **ip address** command or configure a VRRP virtual address on the BFD MAD-enabled VLAN interface. • Make sure all the MAD IP addresses are on the same subnet.

When you configure BFD MAD that uses management Ethernet ports, follow these restrictions and guidelines:

Category	Restrictions and guidelines
Management Ethernet ports for BFD MAD	Connect a management Ethernet port on each member device to the common Ethernet ports on the intermediate device.
BFD MAD VLAN	• On the intermediate device, create a VLAN for BFD MAD, and assign the ports used for BFD MAD to the VLAN. On the IRF fabric, you do not need to assign the management Ethernet ports to the VLAN. • Make sure the IRF fabrics on the network use different BFD MAD VLANs. • Make sure the BFD MAD VLAN on the intermediate device contains only ports on the BFD MAD links.
MAD IP address	• Use the **mad ip address** command instead of the **ip address** command to configure MAD IP addresses on the BFD MAD-enabled management Ethernet ports. • Make sure all the MAD IP addresses are on the same subnet.

Examples

Enable BFD MAD on VLAN-interface 3.

```
<Switch> system-view
[Switch] interface vlan-interface 3
[Switch-Vlan-interface3] mad bfd enable
```

1.1.17. mad enable

Use **mad enable** to enable LACP MAD.

Use **undo mad enable** to disable LACP MAD.

Syntax

mad enable

undo mad enable

Default

LACP MAD is disabled.

Views

Aggregate interface view

Predefined user roles

network-admin

Usage guidelines

LACP MAD handles collisions differently than ARP MAD. To avoid conflicts, do not enable LACP MAD together with ARP MAD on an IRF fabric.

LACP MAD requires an NEC device that supports extended LACPDUs to act as the intermediate device. You must configure all IRF stack member devices to participate in a single dynamic link aggregation group when connected to the intermediate device. To enable dynamic link aggregation, configure the **link-aggregation mode dynamic** command on the aggregate interface.

If one IRF fabric uses another IRF fabric as the intermediate device for LACP MAD, you must assign the two IRF fabrics different domain IDs for correct split detection. False detection causes IRF split.

When you use the **mad enable** command, the system prompts you to enter a domain ID. If you do not want to change the current domain ID, press **enter** at the prompt.

An IRF fabric has only one IRF domain ID. You can change the IRF domain ID by using the following commands: **irf domain**, **mad enable**, **mad arp enable**, or **mad nd enable**. The IRF domain IDs configured by using these commands overwrite each other.

Examples

Enable LACP MAD on Bridge-Aggregation 1, a Layer 2 dynamic aggregate interface.

```
<Switch> system-view
[Switch] interface bridge-aggregation 1
[Switch-Bridge-Aggregation1] link-aggregation mode dynamic
[Switch-Bridge-Aggregation1] mad enable
You need to assign a domain ID (range: 0-4294967295)
[Current domain is: 0]: 1
The assigned domain ID is: 1
MAD LACP only enable on dynamic aggregation interface.
```

Related commands

irf domain

1.1.18. mad exclude interface

Use **mad exclude interface** to exclude a service interface from being shut down when the IRF fabric transits to the Recovery state upon detection of a multi-active collision.

Use **undo mad exclude interface** to configure the IRF fabric to shut down a service interface when it transits to the Recovery state upon detection of a multi-active collision.

Syntax

mad exclude interface *interface-type interface-number*

undo mad exclude interface *interface-type interface-number*

Default

Except for the service interfaces automatically excluded by the system, all service interfaces are shut down when the IRF fabric transits to the Recovery state. The system automatically excludes the following service interfaces from being shut down:

- IRF physical interfaces.
- Interfaces used for BFD MAD.
- Member interfaces of an aggregate interface if the aggregate interface is excluded from being shut down.

Views

System view

Predefined user roles

network-admin

Parameters

interface-type interface-number: Specifies a service interface by its type and number.

Usage guidelines

If a service interface must be kept in up state for special purposes such as Telnet connection, exclude the service interface from the shutdown action. As a best practice to avoid incorrect traffic forwarding, do not exclude any service interfaces except for the interfaces used for Telnet.

The service interfaces that have been shut down by MAD come up when the member devices reboot to join the recovered IRF fabric. If the active IRF fabric fails before the IRF link is recovered, use the **mad restore** command on the inactive IRF fabric to recover the inactive IRF fabric. This command also brings up all service interfaces that were shut down by MAD.

Examples

Exclude GigabitEthernet 1/0/1 from being shut down when the MAD status transits to Recovery.

```
<Switch> system-view
[Switch] mad exclude interface gigabitethernet 1/0/1
```

Related commands

mad restore

1.1.19. mad ip address

Use **mad ip address** to assign a MAD IP address to an IRF member device for BFD MAD.

Use **undo mad ip address** to delete the MAD IP address for an IRF member device.

Syntax

mad ip address *ip-address* { *mask* | *mask-length* } **member** *member-id*

undo mad ip address *ip-address* { *mask* | *mask-length* } **member** *member-id*

Default

No MAD IP address is configured for an IRF member device.

Views

VLAN interface view

Management Ethernet interface view

Predefined user roles

network-admin

Parameters

ip-address: Specifies an IP address in dotted decimal notation.

mask: Specifies a subnet mask in decimal dotted notation.

mask-length: Specifies a subnet mask in length, in the range of 0 to 32.

member *member-id*: Specifies the ID of an IRF member.

Usage guidelines

To use BFD MAD, configure a MAD IP address for each IRF member. Make sure all the MAD IP addresses are on the same subnet.

Do not configure a MAD IP address by using the **ip address** command or configure a VRRP virtual address on the BFD MAD-enabled port or interface.

The master attempts to establish BFD sessions with other member devices by using its MAD IP address as the source IP address.

- If the IRF fabric is integrated, only the MAD IP address of the master takes effect. The master cannot establish a BFD session with any other member. If you execute the **display bfd session** command, the state of the BFD sessions is **Down**.
- When the IRF fabric splits, the IP addresses of the masters in the partitioned IRF fabrics take effect. The masters can establish a BFD session. If you execute the **display bfd session** command, the state of the BFD session between the two devices is **Up**.

Examples

Assign a MAD IP address to IRF member 1 on VLAN-interface 3.

```
<Switch> system-view
[Switch] interface vlan-interface 3
[Switch-Vlan-interface3] mad ip address 192.168.0.1 255.255.255.0 member 1
```

Assign a MAD IP address to IRF member 2 on VLAN-interface 3.

```
[Switch-Vlan-interface3] mad ip address 192.168.0.2 255.255.255.0 member 2
```

Related commands

mad bfd enable

1.1.20. mad restore

Use **mad restore** to restore the normal MAD state of the IRF fabric in Recovery state.

Syntax

mad restore

Views

System view

Predefined user roles

network-admin

Usage guidelines

If the active IRF fabric has failed to work before the IRF split problem is fixed, use this command to restore an IRF fabric in Recovery state. The recovered IRF fabric will take over the active IRF fabric role.

Examples

Restore the normal MAD state of the IRF fabric in Recovery state.

```
<Switch> system-view
[Switch] mad restore
This command will restore the device from multi-active conflict state. Continue? [Y/N]:Y
Restoring from multi-active conflict state, please wait...
```

1.1.21. port group interface

Use **port group interface** to bind a physical interface to an IRF port.

Use **undo port group interface** to remove the binding of a physical interface to an IRF port.

Syntax

port group interface *interface-type interface-number*

undo port group interface *interface-name*

Default

No physical interfaces are bound to an IRF port.

Views

IRF port view

Predefined user roles

network-admin

Parameters

interface-type interface-number: Specifies a physical interface by its type and number.

interface-name: Specifies a physical interface in the *interface-typeinterface-number* format. No space is allowed between the *interface-type* and *interface-number* arguments.

Usage guidelines

Execute this command multiple times to bind multiple physical interfaces to an IRF port. You can bind a maximum of four physical interfaces to an IRF port.

Use the **shutdown** command to shut down a physical interface before you bind it to or remove it from an IRF port. To bring up the physical interface after a binding or binding removal operation, use the **undo shutdown** command.

The system does not dynamically remove IRF port bindings when IRF links are lost, for example, because an interface card is removed. To remove IRF port bindings, you must use the **undo port group interface** command.

For more information about IRF port binding requirements, see *Virtual Technologies Configuration Guide*.

Examples

Bind Ten-GigabitEthernet 1/0/49 to IRF-port 1/1 on IRF member 1.

```
<Switch> system-view
[Switch] interface ten-gigabitethernet 1/0/49
[Switch-Ten-GigabitEthernet1/0/49] shutdown
[Switch-Ten-GigabitEthernet1/0/49] quit
[Switch] irf-port 1/1
[Switch-irf-port1/1] port group interface ten-gigabitethernet 1/0/49
[Switch-irf-port1/1] quit
[Switch] interface ten-gigabitethernet 1/0/49
[Switch-Ten-GigabitEthernet1/0/49] undo shutdown
```

Related commands

irf-port

QX-S5600G Series Ethernet Switches

Command References

3.Layer 2 - LAN Switching

This manual is including the following chapters.

01-Ethernet interface commands

02-Loopback, null interface commands

03-Bulk interface configuration commands

04-MAC address table commands

05-MAC Information commands

06-Ethernet link aggregation commands

07-Port isolation commands

08-Spanning tree commands

09-Loop detection commands

10-VLAN commands

11-Private VLAN commands

12-Voice VLAN commands

13-QinQ commands

14-VLAN mapping commands

15-LLDP commands

16-L2PT commands

17-M-LAG commands

Contents

A page of this section is **3-x-x**

1. Ethernet interface commands 1-1
1.1. Common Ethernet interface commands 1-1
1.1.1. broadcast-suppression 1-1
1.1.2. combo enable 1-2
1.1.3. description 1-3
1.1.4. display counters 1-3
1.1.5. display counters rate 1-5
1.1.6. display interface 1-6
1.1.7. duplex 1-16
1.1.8. eee enable 1-17
1.1.9. flow-control 1-18
1.1.10. flow-interval 1-18
1.1.11. interface 1-19
1.1.12. jumboframe enable 1-19
1.1.13. link-delay 1-20
1.1.14. loopback 1-22
1.1.15. multicast-suppression 1-23
1.1.16. port auto-power-down 1-24
1.1.17. port link-mode 1-25
1.1.18. reset counters interface 1-26
1.1.19. shutdown 1-27
1.1.20. speed 1-27
1.1.21. unicast-suppression 1-28
1.1.22. using fortygige 1-29
1.1.23. using tengige 1-30
1.2. Layer 2 Ethernet interface commands 1-31
1.2.1. display storm-constrain 1-31
1.2.2. mdix-mode 1-32
1.2.3. speed auto 1-33
1.2.4. storm-constrain 1-34
1.2.5. storm-constrain control 1-36
1.2.6. storm-constrain enable log 1-36
1.2.7. storm-constrain enable trap 1-37
1.2.8. storm-constrain interval 1-37
1.2.9. virtual-cable-test 1-38

1. Ethernet interface commands

1.1. Common Ethernet interface commands

1.1.1. broadcast-suppression

Use **broadcast-suppression** to enable broadcast suppression and set the broadcast suppression threshold.

Use **undo broadcast-suppression** to disable broadcast suppression.

Syntax

broadcast-suppression { *ratio* | **pps** *max-pps* | **kbps** *max-kbps* }

undo broadcast-suppression

Default

Ethernet interfaces do not suppress broadcast traffic.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

ratio: Sets the broadcast suppression threshold as a percentage of the interface bandwidth. The value range for this argument is 0 to 100. A smaller value means that less broadcast traffic is allowed to pass through.

pps *max-pps*: Specifies the maximum number of broadcast packets that the interface can forward per second. The value range for the *max-pps* argument (in pps) is 0 to 1.4881 × the interface bandwidth.

kbps *max-kbps*: Specifies the maximum number of kilobits of broadcast traffic that the Ethernet interface can forward per second. The value range for this argument (in kbps) is 0 to the interface bandwidth.

Usage guidelines

The broadcast storm suppression features limits the size of broadcast traffic to a threshold on an interface. When the broadcast traffic on the interface exceeds this threshold, the system drops packets until the traffic drops below this threshold.

Both the **storm-constrain** command and the **broadcast-suppression** command can suppress broadcast storms on a port. The **broadcast-suppression** command uses the chip to physically suppress broadcast traffic. It has less influence on the device performance than the **storm-constrain** command, which uses software to suppress broadcast traffic.

For the traffic suppression result to be determined, do not configure both the **storm-constrain broadcast** command and the **broadcast-suppression** command on an interface.

When you configure the suppression threshold in kbps, the actual suppression threshold might be different from the configured one as follows:

- If the configured value is smaller than 64, the value of 64 takes effect.

- If the configured value is greater than 64 but not an integer multiple of 64, the integer multiple of 64 that is greater than and closest to the configured value takes effect.

For the suppression threshold that takes effect, see the prompt on the device.

Examples

Set the broadcast suppression threshold to 10000 kbps on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] broadcast-suppression kbps 10000
The actual value is 10048 on port GigabitEthernet1/0/1 currently.
```

The output shows that the value that takes effect is 10048 kbps (157 times of 64), because the chip only supports step 64.

Related commands

multicast-suppression

unicast-suppression

1.1.2. combo enable

Use **combo enable** to activate the copper or fiber combo port of a combo interface.

Syntax

combo enable { **auto** | **copper** | **fiber** }

Default

Before v7.1.8

The copper combo port of a combo interface is activated.

After v7.2.16

The copper or fiber combo port is automatically activated depending on the medium inserted in the combo interface.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

auto: Automatically identifies the media inserted and activates the corresponding combo port.

copper: Activates the copper combo port. In this case, use twisted pairs to connect the port.

fiber: Activates the fiber combo port. In this case, use optical fibers to connect the port.

Usage guidelines

A combo interface is a logical interface that physically contains one fiber combo port and one copper combo port on the device panel. The two ports share one forwarding interface. As a result, they cannot work simultaneously. When you activate either port, the other port is automatically disabled. You can select to activate the copper combo port or fiber combo port.

Before using this command, perform the following tasks according to the marks on the device panel:

- Determine the combo interfaces on your device.

- Identify the two physical interfaces that belong to each combo interface.

Examples

Activate the copper combo port of combo interface GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] combo enable copper
```

Activate the fiber combo port of combo interface GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] combo enable fiber
```

1.1.3. description

Use **description** to configure the description of an interface.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

The description of an interface is the interface name plus **Interface** (for example, **GigabitEthernet1/0/1 Interface**).

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

text: Specifies the interface description, a case-sensitive string of 1 to 255 characters.

Examples

Set the description of GigabitEthernet 1/0/1 to **lan-interface**.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] description lan-interface
```

1.1.4. display counters

Use **display counters** to display interface traffic statistics.

Syntax

display counters { **inbound** | **outbound** } **interface** [*interface-type* [*interface-number*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

inbound: Displays inbound traffic statistics.

outbound: Displays outbound traffic statistics.

interface-type: Specifies an interface type.

interface-number: Specifies an interface number.

Usage guidelines

This command displays traffic statistics within a statistics polling interval specified by using the **flow-interval** command.

To clear the Ethernet interface traffic statistics, use the **reset counters interface** command.

If you do not specify an interface type, this command displays traffic statistics for all interfaces that have traffic counters.

If you specify an interface type but do not specify an interface number, this command displays traffic statistics for all interfaces of the specified type.

If you specify an interface type and number, this command displays traffic statistics for the specified interface.

Examples

Display inbound traffic statistics for all interfaces.

```
<Switch> display counters inbound interface
Interface            Total (pkts)    Broadcast (pkts)    Multicast (pkts)  Err (pkts)
GE1/0/1                       100                 100                   0           0
GE1/0/2                  Overflow            Overflow            Overflow    Overflow

 Overflow: More than 14 digits (7 digits for column "Err").
       --: Not supported.
```

Table 1-1 Command output

Field	Description
Interface	Abbreviated interface name.
Total (pkts)	Total number of packets received or sent through the interface.
Broadcast (pkts)	Total number of broadcast packets received or sent through the interface.
Multicast (pkts)	Total number of multicast packets received or sent through the interface.
Err (pkts)	Total number of error packets received or sent through the interface.
Overflow: More than 14 digits (7 digits for column "Err")	The command displays **Overflow** when any of the following conditions exist: • The data length of an **Err** field value is greater than 7 decimal digits. • The data length of a non-Err field value is greater than 14 decimal digits.

Field	Description
--: Not supported	The statistical item is not supported.

Related commands

flow-interval

reset counters interface

1.1.5. display counters rate

Use **display counters rate** to display traffic rate statistics for interfaces in up state for the most recent statistics polling interval.

Syntax

display counters rate { **inbound** | **outbound** } **interface** [*interface-type* [*interface-number*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

inbound: Displays inbound traffic rate statistics.

outbound: Displays outbound traffic rate statistics.

interface-type: Specifies an interface type.

interface-number: Specifies an interface number.

Usage guidelines

If you do not specify an interface type, this command displays traffic rate statistics for all up interfaces that have traffic counters.

If you specify an interface type but do not specify an interface number, this command displays traffic rate statistics for all up interfaces of the specified type.

If you specify an interface type and an interface, this command displays traffic rate statistics for the specified interface.

If an interface that you specify is always down for the most recent statistics polling interval, the system prompts that the interface does not support the command.

To set the statistics polling interval, use the **flow-interval** command.

Examples

Display the inbound traffic rate statistics for all interfaces.

```
<Switch> display counters rate inbound interface
Usage: Bandwidth utilization in percentage
Interface            Usage (%)    Total (pps)    Broadcast (pps)    Multicast (pps)
GE1/0/1                      0              0                 --                 --


 Overflow: More than 14 digits.
```

```
--: Not supported.
```

Table 1-2 Command output

Field	Description
Interface	Abbreviated interface name.
Usage (%)	Bandwidth usage (in percentage) of the interface for the last statistics polling interval.
Total (pkts/sec)	Average receiving or sending rate (in pps) for unicast packets for the last statistics polling interval.
Broadcast (pkts/sec)	Average receiving or sending rate (in pps) for broadcast packets for the last statistics polling interval.
Multicast (pkts/sec)	Average receiving or sending rate (in pps) for multicast packets for the last statistics polling interval. .
Overflow: more than 14 decimal digits	The command displays **Overflow** if the data length of a statistical item is greater than 14 decimal digits.
--: not supported	The statistical item is not supported.

Related commands

flow-interval

reset counters interface

1.1.6. display interface

Use **display interface** to display interface information.

Syntax

display interface [*interface-type* [*interface-number*]] [**brief** [**description** | **down**]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type: Specifies an interface type.

interface-number: Specifies an interface number.

brief: Displays brief interface information. If you do not specify this keyword, the command displays detailed interface information.

description: Displays complete interface descriptions. If you do not specify this keyword, the command displays only the first 27 characters of each interface description.

down: Displays information about interfaces in down state and the causes. If you do not specify this keyword, the command displays information about interfaces in all states.

Usage guidelines

If you do not specify an interface type, this command displays information about all interfaces.

If you specify an interface type but do not specify an interface number, this command displays information about all interfaces of the specified type.

Examples

Display information about Layer 3 interface GigabitEthernet 1/0/1.

```
<Switch> display interface gigabitethernet 1/0/1
GigabitEthernet1/0/1
Current state: Administratively DOWN
Line protocol state: DOWN
Description: GigabitEthernet1/0/1 Interface
Bandwidth: 1000000 kbps
Maximum transmission unit: 1500
Allow jumbo frames to pass
Broadcast max-ratio: 100%
Multicast max-ratio: 100%
Unicast max-ratio: 100%
Internet protocol processing: Disabled
IP packet frame type: Ethernet II, hardware address: 3822-d666-bd0c
IPv6 packet frame type: Ethernet II, hardware address: 3822-d666-bd0c
Loopback is not set
Media type is twisted pair, port hardware type is 1000_BASE_T
Port priority: 2
Unknown-speed mode, unknown-duplex mode
Link speed type is autonegotiation, link duplex type is autonegotiation
Flow-control is not enabled
Maximum frame length: 9216
Last link flapping: 6 hours 39 minutes 28 seconds
Last clearing of counters: Never
 Peak input rate: 0 bytes/sec, at 2013-07-07 16:07:11
 Peak output rate: 0 bytes/sec, at 2013-07-07 16:07:11
 Last 300 second input:  0 packets/sec 0 bytes/sec  0%
 Last 300 second output: 0 packets/sec 0 bytes/sec  0%
 Input  (total): 0 packets, 0 bytes
          0 unicasts, 0 broadcasts, 0 multicasts, - pauses
 Input  (normal): 0 packets, 0 bytes
          0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
 Input: 0 input errors, 0 runts, 0 giants, 0 throttles
          0 CRC, 0 frame, 0 overruns, - aborts
          - ignored, - parity errors
 Output  (total): 0 packets, 0 bytes
          0 unicasts, 0 broadcasts, 0 multicasts, - pauses
 Output  (normal): 0 packets, 0 bytes
          0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
 Output: 0 output errors, - underruns, - buffer failures
          0 aborts, 0 deferred, 0 collisions, 0 late collisions
          - lost carrier, - no carrier
```

Display detailed information about Layer 2 interface GigabitEthernet 1/0/1.

```
<Switch> display interface gigabitethernet 1/0/1
```

```
GigabitEthernet1/0/1
Current state: DOWN
Line protocol state: DOWN
IP packet frame type: Ethernet II, hardware address: 000c-2963-b767
Description: GigabitEthernet1/0/1 Interface
Bandwidth: 100000 kbps
Loopback is not set
Media type is twisted pair, port hardware type is 1000_BASE_T_AN_SFP
Unknown-speed mode, unknown-duplex mode
Link speed type is autonegotiation, link duplex type is autonegotiation
Flow-control is not enabled
Maximum frame length: 9216
Allow jumbo frame to pass
Broadcast max-ratio: 100%
Multicast max-ratio: 100%
Unicast max-ratio: 100%
PVID: 1
MDI type: Automdix
Port link-type: Access
 Tagged VLANs:   None
 UnTagged VLANs: 1
Port priority: 2
Last link flapping: 6 hours 39 minutes 25 seconds
Last clearing of counters:  14:34:09 Tue 11/01/2011
 Peak input rate: 0 bytes/sec, at 2013-07-17 22:06:19
 Peak output rate: 0 bytes/sec, at 2013-07-17 22:06:19
 Last 300 second input:  0 packets/sec 0 bytes/sec -%
 Last 300 second output:  0 packets/sec 0 bytes/sec -%
 Input (total):  0 packets, 0 bytes
          0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
 Input (normal):  0 packets, 0 bytes
          0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
 Input:  0 input errors, 0 runts, 0 giants, 0 throttles
          0 CRC, 0 frame, 0 overruns, 0 aborts
          0 ignored, 0 parity errors
 Output (total): 0 packets, 0 bytes
          0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
 Output (normal): 0 packets, 0 bytes
          0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
 Output: 0 output errors, 0 underruns, 0 buffer failures
          0 aborts, 0 deferred, 0 collisions, 0 late collisions
          0 lost carrier, 0 no carrier
```

Table 1-3 Command output

Field	Description
Current state	Physical link state of the interface: • **Administratively DOWN**—The interface has been

Field	Description
	shut down by using the **shutdown** command. • **DOWN**—The interface is administratively up, but its physical state is down (possibly because no physical link exists or the link has failed). • **DOWN (Link-Aggregation interface down)**—The aggregate interface to which the interface belongs has been shut down by using the **shutdown** command. • **Link-Flap DOWN**—The interface has been shut down by the link flapping protection feature. • **mac-address moving down**—The interface has been shut down by the MAC address move suppression feature. • **MAD ShutDown**—The interface has been shut down by IRF MAD. This state occurs if the interface is on an IRF fabric placed in Recovery state after an IRF split. • **Storm-Constrain**—The interface has been shut down because the storm control feature detected that unknown unicast traffic, multicast traffic, or broadcast traffic exceeded the upper threshold. • **STP DOWN**—The interface has been shut down by the BPDU guard feature. • **UP**—The interface is both administratively and physically up.

Line protocol state	Data link layer state of the interface. The state is determined through automatic parameter negotiation at the data link layer.
	• **UP**—The data link layer protocol is up.
	• **UP (spoofing)**—The data link layer protocol is up, but the link is an on-demand link or does not exist. This attribute is typical of null interfaces and loopback interfaces.
	• **DOWN**—The data link layer protocol is down.
	• **DOWN (***protocols***)** —The data link layer has been shut down by protocols included in the parentheses. Available protocols include:
	  ○ **DLDP**—Shuts down the data link layer when it detects that the link is unidirectional.
	  ○ **OAM**—Shuts down the data link layer when it detects a remote link failure.
	  ○ **LAGG**—Shuts down the data link layer when it detects that the aggregate interface does not have Selected ports.
	  ○ **BFD**—Shuts down the data link layer when it detects a link failure.

Bandwidth	Expected bandwidth of the interface.
Maximum transmission unit	MTU of the interface.
Internet protocol processing: Disabled	The interface is not assigned an IP address and cannot process IP packets.
Internet address	IP address of the interface. The **primary** attribute indicates that the address is the primary IP address.
IP packet frame type	IPv4 packet framing format.

Field	Description
hardware address	MAC address of the interface.
IPv6 packet frame type	IPv6 packet framing format.
Port priority	Port priority of the interface.
Loopback is set internal	An internal loopback test is running on the interface. This field depends on your configuration.
Loopback is set external	An external loopback test is running on the interface. This field depends on your configuration.
Loopback is not set	No loopback test is running on the interface. This field depends on your configuration.
10Mbps-speed mode	The interface is operating at 10 Mbps. This field depends on your configuration and the link parameter negotiation result.
100Mbps-speed mode	The interface is operating at 100 Mbps. This field depends on your configuration and the link parameter negotiation result.
1000Mbps-speed mode	The interface is operating at 1000 Mbps. This field depends on your configuration and the link parameter negotiation result.
10Gbps-speed mode	The interface is operating at 10 Gbps. This field depends on your configuration and the link parameter negotiation result.
40Gbps-speed mode	The interface is operating at 40 Gbps. This field depends on your configuration and the link parameter negotiation result.
Unknown-speed mode	The speed of the interface is unknown because the speed negotiation fails or the interface is physically disconnected.
half-duplex mode	The interface is operating in half duplex mode. This field depends on your configuration and the link parameter negotiation result.
full-duplex mode	The interface is operating in full duplex mode. This field depends on your configuration and the link parameter negotiation result.
unknown-duplex mode	The duplex mode of the interface is unknown because the duplex mode negotiation fails or the interface is physically disconnected.
Link speed type is autonegotiation	The interface is configured with the **speed auto** command.
Link speed type is force link	The interface is manually configured with a speed (for example, 1000 Mbps) by using the **speed** command.
link duplex type is autonegotiation	The interface is configured with the **duplex auto** command.
link duplex type is force link	The interface is manually configured with a duplex mode (for example, half or full) by using the **duplex** command.
Flow-control is not enabled	Generic flow control is disabled on the interface. This field depends on your configuration and the link

Field	Description
	parameter negotiation result.
Maximum frame length	Maximum length of Ethernet frames allowed to pass through the interface.
Allow jumbo frame to pass	The interface allows jumbo frames to pass through.
Broadcast max-	Broadcast storm suppression threshold in ratio, pps, or kbps. The unit of the threshold depends on your configuration.
Multicast max-	Multicast storm suppression threshold in ratio, pps, or kbps. The unit of the threshold depends on your configuration.
Unicast max-	Unknown unicast storm suppression threshold in ratio, pps, or kbps. The unit of the threshold depends on your configuration.
PVID	Port VLAN ID (PVID) of the interface.
MDI type	MDIX mode of the interface: • automdix. • mdi. • mdix.
Port link-type	Link type of the interface: • access. • trunk. • hybrid.
Tagged VLANs	VLANs for which the interface sends packets without removing VLAN tags.
Untagged VLANs	VLANs for which the interface sends packets after removing VLAN tags.
VLAN Passing	VLANs whose packets can be forwarded by the port. The VLANs must have been created.
VLAN permitted	VLANs whose packets are permitted by the port.
Trunk port encapsulation	Encapsulation protocol type for the trunk port.
Last link flapping	The amount of time that has elapsed since the most recent physical state change of the interface. This field displays **Never** if the interface has been physically down since device startup.
Last clearing of counters	Time when the **reset counters interface** command was last used to clear the interface statistics. This field displays **Never** if the **reset counters interface** command has never been used on the interface since device startup.
Last 300 second input: 0 packets/sec 0 bytes/sec 0% Last 300 second output: 0 packets/sec 0 bytes/sec 0%	Average inbound or outbound traffic rate (in pps and Bps) in the last 300 seconds, and the ratio of the actual rate to the interface bandwidth. A hyphen (-) indicates that the statistical item is not supported.
Input(total): 0 packets, 0 bytes 0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses	The two fields on the first line represent the inbound traffic statistics (in packets and bytes) for the interface. All inbound normal packets, abnormal packets, and

Field	Description
	normal pause frames were counted. The four fields on the second line represent: • Number of inbound unicast packets. • Number of inbound broadcasts. • Number of inbound multicasts. • Number of inbound pause frames. A hyphen (-) indicates that the statistical item is not supported.
Input(normal): 0 packets, 0 bytes 0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses	The two fields on the first line represent the inbound normal traffic and pause frame statistics (in packets and bytes) for the interface. The four fields on the second line represent: • Number of inbound normal unicast packets. • Number of inbound normal broadcasts. • Number of inbound normal multicasts. • Number of inbound normal pause frames. A hyphen (-) indicates that the statistical item is not supported.
input errors	Statistics of incoming error packets.
runts	Number of inbound frames meeting the following conditions: • Shorter than 64 bytes. • In correct format. • Containing valid CRCs.
giants	Number of inbound giants. Giants refer to frames larger than the maximum frame length supported on the interface. For an Ethernet interface that does not permit jumbo frames, the maximum frame length is as follows: • 1518 bytes (without VLAN tags). • 1522 bytes (with VLAN tags). For an Ethernet interface that permits jumbo frames, the maximum Ethernet frame length is set when you configure jumbo frame support on the interface.
throttles	Number of inbound frames that had a non-integer number of bytes.
CRC	Total number of inbound frames that had a normal length, but contained CRC errors.
frame	Total number of inbound frames that contained CRC errors and a non-integer number of bytes.
overruns	Number of packets dropped because the input rate of the port exceeded the queuing capability.
aborts	Total number of illegal inbound packets: • **Fragment frames**—CRC error frames shorter than 64 bytes. The length (in bytes) can be an integral or non-integral value. • **Jabber frames**—CRC error frames greater than the maximum frame length supported on the Ethernet interface (with an integral or non-integral

Field	Description
	length). ○ For an Ethernet interface that does not permit jumbo frames, the maximum frame length is 1518 bytes (without VLAN tags) or 1522 bytes (with VLAN tags). ○ For an Ethernet interface that permits jumbo frames, the maximum Ethernet frame length is set when you configure jumbo frame support on the interface. • **Symbol error frames**—Frames that contained a minimum of one undefined symbol. • **Unknown operation code frames**—Non-pause MAC control frames. • **Length error frames**—Frames whose 802.3 length fields did not match the actual frame length (46 to 1500 bytes).
ignored	Number of inbound frames dropped because the receiving buffer of the port ran low.
parity errors	Total number of frames with parity errors.
Output(total): 0 packets, 0 bytes 0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses	The two fields on the first line represent the outbound traffic statistics (in packets and bytes) for the interface. All outbound normal packets, abnormal packets, and normal pause frames were counted. The four fields on the second line represent: • Number of outbound unicast packets. • Number of outbound broadcasts. • Number of outbound multicasts. • Number of outbound pause frames. A hyphen (-) indicates that the statistical item is not supported.
Output(normal): 0 packets, 0 bytes 0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses	The two fields on the first line represent the outbound normal traffic and pause frame statistics (in packets and bytes) for the interface. The four fields on the second line represent: • Number of outbound normal unicast packets. • Number of outbound normal broadcasts. • Number of outbound normal multicasts. • Number of outbound normal pause frames. A hyphen (-) indicates that the statistical item is not supported.
output errors	Number of outbound packets with errors.
underruns	Number of packets dropped because the output rate of the interface exceeded the output queuing capability. This is a low-probability hardware anomaly.
buffer failures	Number of packets dropped because the transmitting buffer of the interface ran low.
aborts	Number of packets that failed to be transmitted, for example, because of Ethernet collisions.
deferred	Number of frames that the interface deferred to transmit because of detected collisions.

Field	Description
collisions	Number of frames that the interface stopped transmitting because Ethernet collisions were detected during transmission.
late collisions	Number of frames that the interface deferred to transmit after transmitting their first 512 bits because of detected collisions.
lost carrier	Number of carrier losses during transmission. This counter increases by one when a carrier is lost, and applies to serial WAN interfaces.
no carrier	Number of times that the port failed to detect the carrier when attempting to send frames. This counter increases by one when a port failed to detect the carrier, and applies to serial WAN interfaces.
Peak input rate	Peak rate of inbound traffic in Bps, and the time when the peak inbound traffic rate occurred.
Peak output rate	Peak rate of outbound traffic in Bps, and the time when the peak outbound traffic rate occurred.

Display brief information about all interfaces.

```
<Switch> display interface brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) – spoofing

Interface            Link Protocol Primary IP      Description
GE1/0/1              DOWN DOWN     --
Loop0                UP   UP(s)    2.2.2.9
NULL0                UP   UP(s)    --
Vlan1                UP   DOWN     --
Vlan999              UP   UP       192.168.1.42

Brief information on interfaces in bridge mode:
Link: ADM - administratively down; Stby - standby
Speed: (a) - auto
Duplex: (a)/A - auto; H - half; F - full
Type: A - access; T - trunk; H - hybrid
Interface            Link Speed   Duplex Type PVID Description
GE1/0/2              DOWN auto    A      A    1
GE1/0/3              UP   auto    F(a)   A    1    aaaaaaaaaaaaaaaaaaaaaaaaaa
```

Display brief information about GigabitEthernet 1/0/3, including the complete description of the interface.

```
<Switch> display interface gigabitethernet 1/0/3 brief description
Brief information on interfaces in bridge mode:
Link: ADM - administratively down; Stby - standby
Speed: (a) - auto
Duplex: (a)/A - auto; H - half; F - full
Type: A - access; T - trunk; H - hybrid
```

```
Interface            Link Speed   Duplex Type PVID Description
GE1/0/3              UP   auto    F(a)   A    1    aaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

Display information about interfaces in DOWN state and the causes.

```
<Switch> display interface brief down
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Interface            Link Cause
GE1/0/1              DOWN Not connected
Vlan2                DOWN Not connected

Brief information on interfaces in bridge mode:
Link: ADM - administratively down; Stby - standby
Interface            Link Cause
GE1/0/2              DOWN Not connected
```

Table 1-4 Command output

Field	Description
Brief information on interfaces in route mode:	Brief information about Layer 3 interfaces.
Interface	Interface name.
Link	Physical link state of the interface: • **UP**—The interface is physically up. • **DOWN**—The interface is physically down. • **ADM**—The interface has been shut down by using the **shutdown** command. To restore the physical state of the interface, use the **undo shutdown** command. • **Stby**—The interface is a backup interface in standby state.
Protocol	Data link layer protocol state of the interface: • **UP**—The data link layer protocol of the interface is up. • **DOWN**—The data link layer protocol of the interface is down. • **UP(s)**—The data link layer protocol of the interface is up, but the link is an on-demand link or does not exist. The **(s)** attribute represents the spoofing flag. This value is typical of null interfaces and loopback interfaces.
Primary IP	Primary IP address of the interface. This field displays two hyphens (**--**) if the interface does not have an IP address.
Description	Description of the interface.
Brief information of interfaces in bridge mode:	Brief information about Layer 2 interfaces.
Type: A - access; T - trunk; H – hybrid	Link type options for interfaces.
Speed	Speed of the interface, in bps. This field displays the **(a)** flag next to the speed if the speed is automatically negotiated.

Field	Description
	This field displays **auto** if the interface is configured to autonegotiate its speed but the autonegotiation has not started.
Duplex	Duplex mode of the interface: • **A**—Autonegotiation. The interface is configured to autonegotiate its duplex mode but the autonegotiation has not started. • **F**—Full duplex. • **F(a)**—Autonegotiated full duplex. • **H**—Half duplex. • **H(a)**—Autonegotiated half duplex.
Type	Link type of the interface: • **A**—Access. • **H**—Hybrid. • **T**—Trunk.
PVID	Port VLAN ID.
Cause	Cause for the physical link state of an interface to be **DOWN**: • **Administratively**—The interface has been manually shut down by using the **shutdown** command. To restore the physical state of the interface, use the **undo shutdown** command. • **DOWN (Link-Aggregation interface down)**—The interface is a member port of an aggregate interface, and the aggregate interface is down. • **DOWN (Loopback detection down)**—The loopback detection module has detected loops. • **DOWN (Monitor-Link uplink down)**—The monitor link module has detected that the uplink is down. • **MAD ShutDown**—The interface is on an IRF fabric placed by IRF MAD in Recovery state after an IRF split. • **Not connected**—No physical connection exists (possibly because the network cable is disconnected or faulty). • **Storm-Constrain**—The storm control feature has detected that unknown unicast traffic, multicast traffic, or broadcast traffic exceeded the upper threshold. • **STP DOWN**—The interface has been shut down by the BPDU guard feature. • **Port Security Disabled**—The interface has been shut down by the intrusion detection mechanism because the interface received illegal packets. • **Standby**—The interface is a backup interface in standby state.

Related commands

reset counters interface

1.1.7. duplex

Use **duplex** to set the duplex mode for an Ethernet interface.

Use **undo duplex** to restore the default.

Syntax

duplex { **auto** | **full** | **half** }

undo duplex

Default

An Ethernet interface operates in autonegotiation mode.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

auto: Configures the interface to autonegotiate the duplex mode with the peer.

full: Configures the interface to operate in full duplex mode. In this mode, the interface can receive and transmit packets simultaneously.

half: Configures the interface to operate in half duplex mode. In this mode, the interface can only receive or transmit packets at a given time. Fiber ports, 1000-Mbps Ethernet interfaces, and 10000-Mbps Ethernet interfaces do not support this keyword.

Examples

Configure GigabitEthernet 1/0/1 to operate in full duplex mode.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] duplex full
```

1.1.8. eee enable

IMPORTANT:
Fiber ports do not support this command.

Use **eee enable** to enable Energy Efficient Ethernet (EEE) on an interface.

Use **undo eee enable** to disable EEE on an interface.

Syntax

eee enable

undo eee enable

Default

EEE is disabled.

Views

Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

With EEE enabled, a link-up interface enters low power state if it has not received any packet for a period of time. The time period depends on the chip specifications and is not configurable. When a packet arrives later, the interface restores to the normal state.

Examples

Enable EEE on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] eee enable
```

1.1.9. flow-control

Use **flow-control** to enable TxRx-mode generic flow control on an Ethernet interface.

Use **undo flow-control** to disable TxRx-mode generic flow control on the Ethernet interface.

Syntax

flow-control

undo flow-control

Default

TxRx-mode generic flow control is disabled on an Ethernet interface.

Views

Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

With TxRx-mode generic flow control configured, an interface can both send and receive flow control frames:

- When congested, the interface sends a flow control frame to its peer.
- Upon receiving a flow control frame from the peer, the interface suspends sending packets.

To implement flow control on a link, enable generic flow control at both ends of the link.

Examples

Enable TxRx-mode generic flow control on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] flow-control
```

1.1.10. flow-interval

Use **flow-interval** to set the statistics polling interval.

Use **undo flow-interval** to restore the default.

Syntax

flow-interval *interval*

undo flow-interval

Default

The statistics polling interval is 300 seconds.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

interval: Sets the statistics polling interval in seconds. The interval is in the range of 5 to 300 and must be a multiple of 5.

Examples

Set the statistics polling interval to 100 seconds on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] flow-interval 100
```

1.1.11. interface

Use **interface** to enter interface view.

Syntax

interface *interface-type interface-number*

Views

System view

Predefined user roles

network-admin

Parameters

interface-type: Specifies an interface type.

interface-number: Specifies an interface number.

Examples

Enter the view of GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1]
```

1.1.12. jumboframe enable

Use **jumboframe enable** to allow jumbo frames within the specified length to pass through.

Use **undo jumboframe enable** to prevent jumbo frames from passing through.

Use **undo jumboframe enable** *size* to restore the default.

Syntax

jumboframe enable [*size*]

undo jumboframe enable [*size*]

Default

The device allows jumbo frames within 10000 bytes to pass through.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Predefined user roles

network-admin

Parameters

size: Sets the maximum length (in bytes) of Ethernet frames that are allowed to pass through. The value range for this argument is 1536 to 10000. The value must be an even integer.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Allow jumbo frames to pass through GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] jumboframe enable
```

1.1.13. link-delay

Use **link-delay** to set the physical state change suppression interval on an Ethernet interface.

Use **undo link-delay** to restore the default.

Syntax

Before v7.1.6

link-delay [**msec**] *delay-time* [**mode** { **up** | **updown** }]

undo link-delay [**msec**] *delay-time* [**mode** { **up** | **updown** }]

After v7.2.16

link-delay { **down** | **up** } [**msec**] *delay-time*

undo link-delay { **down** | **up** }

Default

Each time the physical link of a port goes up or comes down, the interface immediately reports the change to the CPU.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

Before v7.1.6

msec: Enables the physical state change suppression interval to be accurate to milliseconds. If you do not specify this keyword, the suppression interval is accurate to seconds.

delay-time: Sets the physical state change suppression interval on the Ethernet interface. A value of 0 means that physical state changes are immediately reported to the CPU and are not suppressed.

- If you do not specify the **msec** keyword, the value range is 0 to 30 seconds.
- If you specify the **msec** keyword, the value range is 0 to 10000 milliseconds, and the value must be a multiple of 100.

mode up: Suppresses the link-up events.

mode updown: Suppresses both the link-up and link-down events.

After v7.2.16

down: Suppresses link-down events.

up: Suppresses link-up events.

msec: Enables the physical state change suppression interval to be accurate to milliseconds. If you do not specify this keyword, the suppression interval is accurate to seconds.

delay-time: Sets the physical state change suppression interval on the Ethernet interface. A value of 0 means that physical state changes are immediately reported to the CPU and are not suppressed.

- If you do not specify the **msec** keyword, the value range is 0 to 120 seconds.

If you specify the **msec** keyword, the value range is 0 to 10000 milliseconds, and the value must be a multiple of 100.

Usage guidelines

Before v7.1.6

You can configure this feature to suppress only link-down events, only link-up events, or both. If an event of the specified type still exists when the suppression interval expires, the system reports the event.

When you configure this feature, follow these guidelines:

- To suppress only link-down events, configure the **link-delay** [**msec**] *delay-time* command.
- To suppress only link-up events, configure the **link-delay** [**msec**] *delay-time* **mode up** command.
- To suppress both link-down and link-up events, configure the **link-delay** [**msec**] *delay-time* **mode updown** command.

On an interface, you can configure different suppression intervals for link-up and link-down events. If you configure the **link-delay** command multiple times for link-up or link-down events, the most recent configuration takes effect.

Do not configure this command on an interface that has RRPP, spanning tree protocols, or Smart Link enabled.

After v7.2.16

You can configure this feature to suppress only link-down events, only link-up events, or both. If an event of the specified type still exists when the suppression interval expires, the system reports the event.

When you configure this feature, follow these guidelines:

- To suppress link-down events, configure the **link-delay down** command.
- To suppress link-up events, configure the **link-delay up** command.

On an interface, you can configure different suppression intervals for link-up and link-down events. If you execute the **link-delay** command multiple times on an interface, the following rules apply:

- You can configure the suppression intervals for link-up and link-down events separately.
- If you configure the suppression interval multiple times for link-up or link-down events, the most recent configuration takes effect.
- Do not execute this command on an interface that has RRPP, spanning tree protocols, or Smart Link enabled.

Examples

Before v7.1.6

Set the link-down event suppression interval to 8 seconds on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] link-delay 8
```

Set the link-up event suppression interval to 800 milliseconds on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
```

[Switch-GigabitEthernet1/0/1] link-delay msec 800 mode up

After v7.2.16

Set the link-down event suppression interval to 8 seconds on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] link-delay down 8
```

Set the link-up event suppression interval to 800 milliseconds on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] link-delay up msec 800
```

1.1.14. loopback

CAUTION:
After you enable loopback testing on an Ethernet interface, the interface does not forward data traffic.

Use **loopback** to enable loopback testing on an Ethernet interface.

Use **undo loopback** to disable loopback testing on an Ethernet interface.

Syntax

loopback { **external** | **internal** }

undo loopback

Default

Loopback testing is disabled on an Ethernet interface.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

external: Enables external loopback testing on the Ethernet interface.

internal: Enables internal loopback testing on the Ethernet interface.

Usage guidelines

After you enable loopback testing on an Ethernet interface, the Ethernet interface switches to full duplex mode. After you disable loopback testing, the Ethernet interface restores to its duplex setting.

An Ethernet interface in a loopback test cannot correctly forward data packets.

You cannot perform a loopback test on the following Ethernet interfaces:

- Ethernet interfaces manually brought down (displayed as in **ADM** or **Administratively DOWN** state).
- Ethernet interfaces configured with the **port up-mode** command.

The **speed**, **duplex**, and **shutdown** commands cannot be configured on an Ethernet interface in a loopback test.

Examples

Enable internal loopback testing on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] loopback internal
```

1.1.15. multicast-suppression

Use **multicast-suppression** to enable multicast storm suppression and set the multicast storm suppression threshold.

Use **undo multicast-suppression** to disable multicast storm suppression.

Syntax

multicast-suppression { *ratio* | **pps** *max-pps* | **kbps** *max-kbps* }

undo multicast-suppression

Default

Ethernet interfaces do not suppress multicast traffic.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

ratio: Sets the multicast suppression threshold as a percentage of the interface bandwidth. The value range for this argument (in percentage) is 0 to 100. A smaller value means that less multicast traffic is allowed to pass through.

pps *max-pps*: Specifies the maximum number of multicast packets that the interface can forward per second. The value range for the *max-pps* argument (in pps) is 0 to 1.4881 × the interface bandwidth.

kbps *max-kbps*: Specifies the maximum number of kilobits of multicast traffic that the Ethernet interface can forward per second. The value range for this argument (in kbps) is 0 to the interface bandwidth.

Usage guidelines

The multicast storm suppression feature limits the size of multicast traffic to a threshold on an interface. When the multicast traffic on the interface exceeds this threshold, the system drops packets until the traffic drops below this threshold.

Both the **storm-constrain** command and the **multicast-suppression** command can suppress multicast storms on a port. The **multicast-suppression** command uses the chip to physically suppress multicast traffic. It has less influence on the device performance than the **storm-constrain** command, which uses software to suppress multicast traffic.

For the traffic suppression result to be determined, do not configure both the **storm-constrain multicast** command and the **multicast-suppression** command on an interface.

When you configure the suppression threshold in kbps, the actual suppression threshold might be different from the configured one as follows:

- If the configured value is smaller than 64, the value of 64 takes effect.
- If the configured value is greater than 64 but not an integer multiple of 64, the integer multiple of 64 that is greater than and closest to the configured value takes effect.

To determine the suppression threshold that takes effect, see the prompts on the switch.

Examples

Set the multicast storm suppression threshold to 10000 kbps on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] multicast-suppression kbps 10000
The actual value is 10048 on port GigabitEthernet1/0/1 currently.
```

The output shows that the value that takes effect is 10048 kbps (157 times of 64), because the chip only supports step 64.

Related commands

broadcast-suppression

unicast-suppression

1.1.16. port auto-power-down

IMPORTANT:
Fiber ports do not support this command.

Use **port auto-power-down** to enable auto power-down on an Ethernet interface.

Use **undo port auto-power-down** to disable auto power-down on an Ethernet interface.

Syntax

port auto-power-down

undo port auto-power-down

Default

Auto power-down is disabled on Ethernet interfaces.

Views

Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

When an interface with auto power-down enabled has been down for a specific period of time, both of the following events occur:

- The device automatically stops supplying power to the interface.
- The interface enters the power save mode.

The time period depends on the chip specifications and is not configurable.

When the interface comes up, both of the following events occur:

- The device automatically restores the power supply to the interface.
- The interface restores to its normal state.

Examples

Enable auto power-down on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port auto-power-down
```

1.1.17. port link-mode

Use **port link-mode** to change the link mode of an Ethernet interface.

Use **undo port link-mode** to restore the default.

Syntax

port link-mode { **bridge** | **route** }

undo port link-mode

Default

Interfaces operate in bridge mode.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

bridge: Specifies the Layer 2 mode.

route: Specifies the Layer 3 mode.

Usage guidelines

Interfaces on the device can operate either as Layer 2 or Layer 3 Ethernet interfaces.

You can use commands to set the link mode to bridge or route.

Changing the link mode of an Ethernet interface also restores all commands (except **shutdown** and **combo enable**) on the Ethernet interface to their defaults in the new link mode.

For a device supporting interface grouping, changing the link mode of interfaces in a group restores all interfaces in the group to the default speed.

Examples

Configure GigabitEthernet 1/0/1 to operate in Layer 2 mode.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-mode bridge
```

1.1.18. reset counters interface

Use **reset counters interface** to clear the interface statistics.

Syntax

reset counters interface [*interface-type* [*interface-number*]]

Views

User view

Predefined user roles

network-admin

Parameters

interface-type: Specifies an interface type.

interface-number: Specifies an interface number.

Usage guidelines

Use this command to clear history statistics if you want to collect traffic statistics for a specific time period.

If you do not specify an interface type, this command clears statistics for all interfaces.

If you specify an interface type but do not specify an interface number, this command clears statistics for all interfaces of the specified type.

Examples

Clear the statistics for GigabitEthernet 1/0/1.

```
<Switch> reset counters interface gigabitethernet 1/0/1
```

Related commands

display counters interface

display counters rate interface

display interface

1.1.19. shutdown

Use **shutdown** to shut down an Ethernet interface.

Use **undo shutdown** to bring up an Ethernet interface.

Syntax

shutdown

undo shutdown

Default

Ethernet interfaces are in up state.

Views

Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

Some interface configurations might require an interface restart before taking effect.

The **shutdown** and **port up-mode** commands are mutually exclusive.

Examples

Shut down and then bring up GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] shutdown
[Switch-GigabitEthernet1/0/1] undo shutdown
```

1.1.20. speed

Use **speed** to set the speed of an Ethernet interface.

Use **undo speed** to restore the default.

Syntax

speed { **10** | **100** | **1000** | **10000** | **40000** | **auto** }

undo speed

Default

An Ethernet interface negotiates a speed with its peer.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

10: Sets the interface speed to 10 Mbps.

100: Sets the interface speed to 100 Mbps.

1000: Sets the interface speed to 1000 Mbps.

10000: Sets the interface speed to 10000 Mbps.

40000: Sets the interface speed to 40000 Mbps.

auto: Enables the interface to negotiate a speed with its peer.

Usage guidelines

For an Ethernet copper port, use the **speed** command to set its speed to match the speed of the peer interface.

For a fiber port, use the **speed** command to set its speed to match the rate of a transceiver module.

Support of an interface for the keywords depends on the interface type. For more information, use the **speed ?** command in interface view.

When an LSWM5SP2PM or LSWM5XGT2PM interface card is installed on the switch, interfaces on the card can operate only at 10 Gbps.

Examples

Configure GigabitEthernet 1/0/1 to autonegotiate the speed.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] speed auto
```

Related commands

speed auto

1.1.21. unicast-suppression

Use **unicast-suppression** to enable unknown unicast storm suppression and set the unknown unicast storm suppression threshold.

Use **undo unicast-suppression** to disable unknown unicast storm suppression.

Syntax

unicast-suppression { *ratio* | **pps** *max-pps* | **kbps** *max-kbps* }

undo unicast-suppression

Default

Ethernet interfaces do not suppress unknown unicast traffic.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

ratio: Sets the unknown unicast suppression threshold as a percentage of the interface bandwidth. The value range for this argument (in percentage) is 0 to 100. A smaller value means that less unknown unicast traffic is allowed to pass through.

pps *max-pps*: Specifies the maximum number of unknown unicast packets that the interface can forward per second. The value range for the *max-pps* argument (in pps) is 0 to 1.4881 × the interface bandwidth.

kbps *max-kbps*: Specifies the maximum number of kilobits of unknown unicast traffic that the Ethernet interface can forward per second. The value range for this argument (in kbps) is 0 to the interface bandwidth.

Usage guidelines

The unknown unicast storm suppression feature limits the size of unknown unicast traffic to a threshold on an interface. When the unknown unicast traffic on the interface exceeds this threshold, the system discards packets until the unknown unicast traffic drops below this threshold.

Both the **storm-constrain** command and the **unicast-suppression** command can suppress unknown unicast storms on a port. The **unicast-suppression** command uses the chip to physically suppress unknown unicast traffic. It has less influence on the device performance than the **storm-constrain** command, which uses software to suppress unknown unicast traffic.

For the unknown unicast traffic suppression result to be determined, do not configure both the **storm-constrain unicast** command and the **unicast-suppression** command on an interface.

When you configure the suppression threshold in kbps, the actual suppression threshold might be different from the configured one as follows:

- If the configured value is smaller than 64, the value of 64 takes effect.
- If the configured value is greater than 64 but not an integer multiple of 64, the integer multiple of 64 that is greater than and closest to the configured value takes effect.

To determine the suppression threshold that takes effect, see the prompts on the switch.

Examples

Set the unknown unicast storm suppression threshold to 10000 kbps on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] unicast-suppression kbps 10000
The actual value is 10048 on port GigabitEthernet1/0/1 currently.
```

The output shows that the value that takes effect is 10048 kbps (157 times of 64), because the chip only supports step 64.

Related commands

broadcast-suppression

multicast-suppression

1.1.22. using fortygige

Use **using fortygige** to combine 10-GE breakout interfaces split from a 40-GE interface into a 40-GE interface.

Use **undo using fortygige** to cancel the configuration.

Syntax

using fortygige

undo using fortygige

Default

The 10-GE breakout interfaces are not combined and operate as single interfaces.

Views

10-GE breakout interface view

Predefined user roles

network-admin

Usage guidelines

If you need higher bandwidth on a single interface, you can combine four 10-GE breakout interfaces split from a 40-GE interface into a 40-GE interface. To do so, execute this command on any of these 10-GE breakout interfaces.

Examples

Combine Ten-GigabitEthernet 1/0/1:1 through Ten-GigabitEthernet 1/0/1:4 into a 40-GE interface.

```
<System> system-view
[System] interface ten-gigabitethernet1/0/1:1
[System-Ten-GigabitEthernet1/0/1:1] using fortygige
The interfaces Ten-GigabitEthernet1/0/1:1 through Ten-GigabitEthernet1/0/1:4 will be
deleted. Continue? [Y/N]:y
```

Related commands

using tengige

1.1.23. using tengige

Use **using tengige** to split a high bandwidth interface into multiple 10-GE breakout interfaces.

Use **undo using tengige** to cancel the configuration.

Syntax

using tengige

undo using tengige

Default

A high bandwidth interface is not split and operates as a single interface.

Views

40-GE interface view

Predefined user roles

network-admin

Usage guidelines

To improve port density, reduce costs, and improve network flexibility, you can split a high bandwidth interface into multiple 10-GE breakout interfaces. For example, split a 40-GE interface FortyGigE 1/0/1 into four 10-GE breakout interfaces Ten-GigabitEthernet 1/0/1:1 through Ten-GigabitEthernet 1/0/1:4.

The 10-GE breakout interfaces support the same configuration and attributes as common 10-GE interfaces, except that they are numbered in a different way.

Examples

Split FortyGigE 1/0/1 into four 10-GE breakout interfaces.

```
<System> system-view
[System] interface fortygige 1/0/1
[System-FortyGigE1/0/1] using tengige
The interface FortyGigE1/0/1 will be deleted. Continue? [Y/N]:y
```

Related commands

using fortygige

1.2. Layer 2 Ethernet interface commands

1.2.1. display storm-constrain

Use **display storm-constrain** to display storm control settings and statistics.

Syntax

display storm-constrain [**broadcast** | **multicast** | **unicast**] [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

broadcast: Displays broadcast storm control settings and statistics.

multicast: Displays multicast storm control settings and statistics.

unicast: Displays unknown unicast storm control settings and statistics.

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify this option, the command displays storm control settings and statistics for all storm control-enabled interfaces.

Usage guidelines

If you do not specify any keywords, this command displays all storm control settings on all storm control-enabled interfaces.

Examples

Display the storm control settings on all storm control-enabled ports.

```
<Switch> display storm-constrain
Abbreviation: BC - broadcast; MC - multicast; UC - unicast
              KNUC - known unicast; FW - forwarding
Flow Statistic Interval: 5 (in seconds)
Port          Type Lower     Upper     Unit CtrlMode Status   Trap Log SwitchNum
--------------------------------------------------------------------------------
GE1/0/1       MC   100       200       kbps shutdown shutdown off  on  10
```

Table 1-5 Command output

Field	Description
Flow Statistic Interval	Traffic polling interval (in seconds) of the storm control module.
Port	Abbreviated interface name.
Type	Type of traffic subjected to storm control: • **BC**—Broadcast packets.

Field	Description
	• **MC**—Multicast packets. • **UC**—Unknown unicast packets. • **KNUC**—Known unicast packets. This field is not supported in the current software version.
Lower	Lower storm control threshold, in pps, kbps, or percentage.
Upper	Upper storm control threshold, in pps, kbps, or percentage.
Unit	Storm control threshold unit: • pps. • kbps. • percentage.
CtrlMode	Action (block or shutdown) taken on the interface when the upper threshold is reached. N/A indicates that no action is configured.
Status	Packet forwarding status: • **forwarding**—The port is forwarding traffic correctly. • **shutdown**—The port has been shut down. • **block**—The port drops the type of traffic.
Trap	Status of the storm control threshold event trap switch: • **on**—The port sends threshold event traps. • **off**—The port does not send threshold event traps.
Log	Status of the storm control threshold event log switch: • **on**—The port sends threshold event log messages. • **off**—The port does not send threshold event log messages.
SwitchNum	Number of forwarding state changes of the interface. When the **SwitchNum** field reaches 65535, it resets automatically.

1.2.2. mdix-mode

IMPORTANT:
Fiber ports do not support this command.

Use **mdix-mode** to configure the Medium Dependent Interface Cross-Over (MDIX) mode of an Ethernet interface.

Use **undo mdix-mode** to restore the default.

Syntax

mdix-mode { **automdix** | **mdi** | **mdix** }

undo mdix-mode

Default

Ethernet interfaces operate in **automdix** mode.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

automdix: Specifies that the interface negotiates pin roles with its peer.

mdi: Specifies that pins 1 and 2 are transmit pins and pins 3 and 6 are receive pins.

mdix: Specifies that pins 1 and 2 are receive pins and pins 3 and 6 are transmit pins.

Examples

Configure GigabitEthernet 1/0/1 to operate in **automdix** mode.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] mdix-mode automdix
```

1.2.3. speed auto

Use **speed auto** to set options for speed autonegotiation.

Use **undo speed** to restore the default.

Syntax

speed auto { **10** | **100** | **1000** } *

undo speed

Default

No option is set for speed autonegotiation.

Views

100-Mbps or 1000-Mbps Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

10: Configures 10 Mbps as an option for speed autonegotiation.

100: Configures 100 Mbps as an option for speed autonegotiation.

1000: Configures 1000 Mbps as an option for speed autonegotiation.

Usage guidelines

The **speed** command and the **speed auto** command supersede each other. The most recent command that you configure takes effect. For example:

- If you configure **speed auto 100 1000** and then **speed 100** on the interface, the interface speed is forcibly set to 100 Mbps.
- If you configure **speed 100** and then **speed auto 100 1000** on the interface, the interface negotiates with its peer for a speed. The negotiated speed is either 100 Mbps or 1000 Mbps.

Speed autonegotiation enables an Ethernet interface to negotiate with its peer for the highest speed that both ends support. You can narrow down the speed option list for negotiation. To avoid negotiation failures, make sure a minimum of one speed option is supported at both ends.

Examples

Configure GigabitEthernet 1/0/1 to use 10 Mbps and 1000 Mbps for speed negotiation.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] speed auto 10 1000
```

Related commands

speed

1.2.4. storm-constrain

Use **storm-constrain** to enable storm control and set thresholds for broadcast, multicast, or unknown unicast packets on an Ethernet interface.

Use **undo storm-constrain** to disable storm control for broadcast, multicast, unknown unicast, or all types of traffic.

Syntax

storm-constrain { **broadcast** | **multicast** | **unicast** } { **pps** | **kbps** | **ratio** } *upperlimit lowerlimit*

undo storm-constrain { **all** | **broadcast** | **multicast** | **unicast** }

Default

Traffic storm control is disabled.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

all: Disables storm control for all types of traffic: broadcast, known unicast, multicast, and unknown unicast.

broadcast: Enables or disables broadcast storm control.

multicast: Enables or disables multicast storm control.

unicast: Enables or disables unknown unicast storm control.

pps: Sets storm control thresholds in pps.

kbps: Sets storm control thresholds in kbps.

ratio: Sets storm control thresholds as a percentage of the transmission capacity of the interface.

upperlimit: Sets the upper threshold, in pps, kbps, or percentage.

- If you specify the **pps** keyword, the value range for the *upperlimit* argument is 1 to 1.4881 × the interface bandwidth（kbps）.

  For example, if the interface bandwidth is 1 Gbps (1,000,000 kbps), the range that can be controlled by this setting is 1 to 1.4881 × 1,000,000 kbps = 1 to 1,488,100 pps.

  For example, if the interface bandwidth is 10 Gbps (10,000,000 kbps), the range that can be controlled by this setting is 1 to 1.4881 × 10,000,000 kbps = 1 to 14,881,000 pps.

  For example, if the interface bandwidth is 40 Gbps (40,000,000 kbps), the range that can be controlled by this setting is 1 to 1.4881 × 40,000,000 kbps = 1 to 59,524,000 pps.

- If you specify the **kbps** keyword, the value range for the *upperlimit* argument is 1 to the interface bandwidth.
- If you specify the **ratio** keyword, the value range for the *upperlimit* argument is 1 to 100.

lowerlimit: Sets the lower threshold, in pps, kbps, or percentage.

- If you specify the **pps** keyword, the value range for the *lowerlimit* argument is 1 to 1.4881 × the interface bandwidth（kbps）.

  For example, if the interface bandwidth is 1 Gbps (1,000,000 kbps), the range that can be controlled by this setting is 1 to 1.4881 × 1,000,000 kbps = 1 to 1,488,100 pps.

  For example, if the interface bandwidth is 10 Gbps (10,000,000 kbps), the range that can be controlled by this setting is 1 to 1.4881 × 10,000,000 kbps = 1 to 14,881,000 pps.

  For example, if the interface bandwidth is 40 Gbps (40,000,000 kbps), the range that can be controlled by this setting is 1 to 1.4881 × 40,000,000 kbps = 1 to 59,524,000 pps.
- If you specify the **kbps** keyword, the value range for the *lowerlimit* argument is 1 to the interface bandwidth.
- If you specify the **ratio** keyword, the value range for the *lowerlimit* argument is 1 to 100.

Usage guidelines

After you configure storm control for a type of traffic, the device collects the statistics for the type of traffic at the interval configured by using the **storm-constrain interval** command. When the type of traffic exceeds its upper threshold, the interface takes an action configured by using the **storm-constrain control** command.

The **storm-constrain**, **broadcast-suppression**, **multicast-suppression**, and **unicast-suppression** commands can suppress storms on an interface. The **broadcast-suppression**, **multicast-suppression**, and **unicast-suppression** commands use the chip to physically suppress traffic. They have less influence on the device performance than the **storm-constrain** command, which uses software to suppress traffic.

For the traffic suppression result to be determined, do not configure both storm control and storm suppression for the same type of traffic.

When configuring this command, make sure *upperlimit* is greater than *lowerlimit*.

Examples

Enable unknown unicast storm control on GigabitEthernet 1/0/1 and set the upper and lower thresholds to 200 pps and 150 pps, respectively.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] storm-constrain unicast pps 200 150
```

Enable broadcast storm control on GigabitEthernet 1/0/2, and set the upper and lower thresholds to 2000 kbps and 1500 kbps, respectively.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] storm-constrain broadcast kbps 2000 1500
```

Enable multicast storm control on GigabitEthernet 1/0/3, and set the upper and lower thresholds to 80% and 15%, respectively.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/3
[Switch-GigabitEthernet1/0/3] storm-constrain multicast ratio 80 15
```

Related commands

storm-constrain control

storm-constrain interval

1.2.5. storm-constrain control

Use **storm-constrain control** to set the action to take on an Ethernet interface when a type of traffic (unknown unicast, multicast, or broadcast) exceeds the upper storm control threshold.

Use **undo storm-constrain control** to restore the default.

Syntax

storm-constrain control { **block** | **shutdown** }

undo storm-constrain control

Default

No action is taken on an Ethernet interface when a type of traffic exceeds the upper storm control threshold.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

block: Blocks this type of traffic and forwards other types of traffic. Even though the interface does not forward the blocked traffic, it still counts the traffic. When the blocked traffic drops below the lower threshold, the port begins to forward the traffic.

shutdown: Goes down automatically. The interface goes down automatically and stops forwarding any traffic. When the blocked traffic drops below the lower threshold, the interface does not forward the traffic. To bring up the interface, use the **undo shutdown** command or disable storm control on the interface.

Examples

Configure GigabitEthernet 1/0/1 to block a specific type of traffic when the type of traffic exceeds the upper storm control threshold.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] storm-constrain control block
```

Related commands

storm-constrain

storm-constrain control

1.2.6. storm-constrain enable log

Use **storm-constrain enable log** to enable an Ethernet interface to output log messages when it detects storm control threshold events.

Use **undo storm-constrain enable log** to disable an Ethernet interface from outputting log messages for storm control threshold events.

Syntax

storm-constrain enable log

undo storm-constrain enable log

Default

An Ethernet interface outputs log messages when monitored traffic exceeds the upper threshold or drops below the lower threshold.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Examples

Enable GigabitEthernet 1/0/1 to output log messages when it detects storm control threshold events.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] storm-constrain enable log
```

1.2.7. storm-constrain enable trap

Use **storm-constrain enable trap** to enable an Ethernet interface to send storm control threshold event traps.

Use **undo storm-constrain enable trap** to disable an Ethernet interface from sending storm control threshold event traps.

Syntax

storm-constrain enable trap

undo storm-constrain enable trap

Default

An interface sends out storm control threshold event traps when monitored traffic exceeds the upper threshold or drops below the lower threshold.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Examples

Enable GigabitEthernet 1/0/1 to send traps when it detects storm control threshold events.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] storm-constrain enable trap
```

1.2.8. storm-constrain interval

Use **storm-constrain interval** to set the traffic polling interval of the storm control module.

Use **undo storm-constrain interval** to restore the default.

Syntax

storm-constrain interval *interval*

undo storm-constrain interval

Default

The storm control module polls traffic statistics every 10 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Sets the traffic polling interval of the storm control module. The value range is 1 to 300 seconds. To ensure network stability, as a best practice, do not use a traffic polling interval shorter than 10 seconds.

Usage guidelines

The traffic polling interval set by using the **storm-constrain interval** command is specific to storm control. To set the statistics polling interval of an interface, use the **flow-interval** command.

Examples

Set the traffic statistics polling interval of the storm control module to 60 seconds.

```
<Switch> system-view
[Switch] storm-constrain interval 60
```

Related commands

storm-constrain

storm-constrain control

1.2.9. virtual-cable-test

IMPORTANT:
This command is not available on fiber ports.
It's not supported at the port link up by 10M and 100M.

Use **virtual-cable-test** to test the cable connection of an Ethernet interface and display the test result.

Syntax

virtual-cable-test

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

The test result is for reference only. The cable length detection error is up to 5 m (about 16 ft).

If a test item is not available, a hyphen (-) is displayed.

Examples

Test the cable connection of GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] virtual-cable-test
Cable status: abnormal(open), 140 metre(s)
Pair Impedance mismatch: -
Pair skew: - ns
Pair swap: -
Pair polarity: -
Insertion loss: - db
Return loss: - db
Near-end crosstalk: - db
```

Table 1-6 Command output

Field	Description
Cable status	Cable status: • **Normal**—The cable is in good condition. • **Abnormal**—The cable is abnormal. • **Abnormal (open)**—An open circuit is detected. • **Abnormal (short)**—A short circuit is detected. • **Failure**—The test failed.
n metre(s)	If the cable connection is working correctly, this field displays the total length of the cable. If the cable connection fails, this field displays the length from the local port to the faulty point.

Contents

A page of this section is **3-x-x**

2. Loopback, null interface commands 2-1
2.1. Loopback, null interface commands 2-1
2.1.1. description 2-1
2.1.2. display interface loopback 2-1
2.1.3. display interface null 2-4
2.1.4. interface loopback 2-5
2.1.5. interface null 2-6
2.1.6. reset counters interface loopback 2-6
2.1.7. reset counters interface null 2-7
2.1.8. shutdown 2-8

2. Loopback, null interface commands

2.1. Loopback, null interface commands

2.1.1. description

Use **description** to configure the description of an interface.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

The interface description uses the *interface name* **Interface** format, for example, LoopBack1 **Interface**.

Views

Loopback interface view

Null interface view

Predefined user roles

network-admin

Parameters

text: Specifies the description, a case-sensitive string of 1 to 255 characters.

Usage guidelines

Configure a description for an interface for easy identification and management purposes.

You can use the **display interface** command to view the configured description.

Examples

Configure the description of Loopback 1 as **for RouterID**.

```
<Switch> system-view
[Switch] interface loopback 1
[Switch-LoopBack1] description for RouterID
```

2.1.2. display interface loopback

Use **display interface loopback** to display information about the specified or all existing loopback interfaces.

Syntax

display interface loopback [*interface-number*] [**brief** [**description** | **down**]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

loopback *interface-number*: Specifies a loopback interface by its number, which can be the number of any existing loopback interface. If you do not specify this argument, the command displays information about all existing loopback interfaces on the device.

brief: Displays brief interface information. If you do not specify this keyword, the command displays detailed interface information.

description: Displays complete interface descriptions. If you do not specify this keyword, the command displays only the first 27 characters of interface descriptions.

down: Displays information about interfaces in down state and the causes. If you do not specify this keyword, the command displays information about interfaces in all states.

Usage guidelines

This command is supported only after a loopback interface is created.

Examples

Display detailed information about Loopback 0.

```
<Switch> display interface loopback 0
LoopBack0
Current state: UP
Line protocol state: UP(spoofing)
Description: LoopBack0 Interface
Bandwidth: 1000 kbps
Maximum transmission unit: 1536
Internet protocol processing: Disabled
Physical: Loopback
Last clearing of counters:  Never
Last 300 seconds input rate:  0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate:  0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops
```

Table 2-1 Command output

Field	Description
Current state	Physical link state of the interface: • **UP**—The loopback interface can receive and transmit packets. • **Administratively DOWN**—The interface has been shut down by using the **shutdown** command.
Line protocol state	Data link layer state of the interface. **UP (spoofing)** means that the data link layer protocol of the interface is up, but the link is an on-demand link or does not exist. This attribute is typical of null interfaces and loopback interfaces.
Description	Description of the interface.
Bandwidth	Expected bandwidth of the interface. This field is not displayed when the value is 0.

Field	Description
Maximum transmission unit	MTU of the interface.
Internet protocol processing: Disabled	The interface is not assigned an IP address and cannot process IP packets.
Internet address: 1.1.1.1/32 (primary)	IP address of the interface. The **primary** attribute indicates that the address is the primary IP address.
Physical: Loopback	The physical type of the interface is loopback.
Last clearing of counters	Time when statistics on the logical interface were last cleared by using the **reset counters interface** command. If the statistics of the interface have never been cleared by using the **reset counters interface** command since the device started, this field displays **Never**.
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec	Average input rate during the last 300 seconds (displayed when the interface supports traffic statistics collection): **bytes/sec**—Average number of bytes received per second. **bits/sec**—Average number of bits received per second. **packets/sec**—Average number of packets received per second.
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec	Average output rate over the last 300 seconds (displayed when the interface supports traffic statistics collection): • **bytes/sec**—Average number of bytes sent per second. • **bits/sec**—Average number of bits sent per second. • **packets/sec**—Average number of packets sent per second.
Input: 0 packets, 0 bytes, 0 drops	Total number and size (in bytes) of incoming packets of the interface and the number of dropped packets (displayed when the interface supports traffic statistics collection).
Output: 0 packets, 0 bytes, 0 drops	Total number and size (in bytes) of outgoing packets of the interface and the number of dropped packets (displayed when the interface supports traffic statistics collection).

Display brief information about all loopback interfaces.

```
<Switch> display interface loopback brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Primary IP         Description
Loop1                UP   UP(s)    --              forLAN1
```

Display information about all loopback interfaces in down state and the causes.

```
<Switch> display interface loopback brief down
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Interface            Link Cause
Loop1                ADM  Administratively
```

Table 2-2 Command output

Field	Description
Link	Physical link state of the interface: • **UP**—The interface is physically up. • **DOWN**—The interface is physically down. • **ADM**—The interface has been shut down by using the **shutdown** command. To restore the physical state of the interface, use the **undo shutdown** command. • **Stby**—The interface is a backup interface in standby state.
Protocol	Data link layer protocol state of the interface, which is always **UP(s)**. **UP(s)** represents that the data link layer protocol of the interface is up, but the link is an on-demand link or does not exist. The **(s)** attribute represents the spoofing flag. This value is typical of null interfaces and loopback interfaces.
Primary IP	Primary IP address of the interface.
Description	Description of the interface.
Cause	Cause for the physical link state of the interface to be **DOWN**. **Administratively** represents that the interface has been manually shut down by using the **shutdown** command. To restore the physical state of the interface, use the **undo shutdown** command.

Related commands

interface loopback

reset counters interface loopback

2.1.3. display interface null

Use **display interface null** to display information about the null interface.

Syntax

display interface null [**0**] [**brief** [**description** | **down**]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

0: Specifies Null 0.

brief: Displays brief interface information. If you do not specify this keyword, the command displays detailed interface information.

description: Displays complete interface descriptions. If you do not specify this keyword, the command displays only the first 27 characters of interface descriptions.

down: Displays information about interfaces in down state and the causes. If you do not specify this keyword, the command displays information about interfaces in all states.

Usage guidelines

The device has only one null interface Null 0. If you specify the **null** keyword, the command displays information about the interface Null 0 regardless of whether you specify the **0** keyword.

Examples

Display detailed information about Null 0.

```
<Switch> display interface null 0
NULL0
Current state: UP
Line protocol state: UP(spoofing)
Description: NULL0 Interface
Bandwidth: 1000000 kbps
Maximum transmission unit: 1500
Internet protocol processing: Disabled
Physical: NULL DEV
Last clearing of counters: Never
Last 300 seconds input rate:  0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate:  0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops
```

Display brief information about Null 0.

```
<Switch> display interface null 0 brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Primary IP         Description
NULL0                UP   UP(s)     --
```

For the command output, see Table 2-1 and Table 2-2 .

Related commands

interface null

reset counters interface null

2.1.4. interface loopback

Use **interface loopback** to create a loopback interface and enter its view, or enter the view of an existing loopback interface.

Use **undo interface loopback** to remove a loopback interface.

Syntax

interface loopback *interface-number*

undo interface loopback *interface-number*

Default

No loopback interfaces exist.

Views

System view

Predefined user roles

network-admin

Parameters

interface-number: Specifies a loopback interface by its number. The value range for this argument is 0 to 127.

Usage guidelines

The physical layer state and link layer protocols of a loopback interface are always up unless the loopback interface is manually shut down. You can use a loopback interface to achieve the following purposes:

- Prevent the connection from being affected by the physical state of the interface.
- Improve the reliability of the connection.

For example, you can configure a loopback interface as the source interface for establishing an FTP connection, or use the loopback interface address as the Router ID in BGP.

Examples

Create Loopback 1.

```
<Switch> system-view
[Switch] interface loopback 1
[Switch-LoopBack1]
```

2.1.5. interface null

Use **interface null** to enter null interface view.

Syntax

interface null 0

Default

A device has only one null interface (Null 0), which cannot be created or deleted.

Views

System view

Predefined user roles

network-admin

Parameters

0: Specifies Null 0. The null interface number is always 0.

Examples

Enter Null 0 interface view.

```
<Switch> system-view
[Switch] interface null 0
[Switch-NULL0]
```

2.1.6. reset counters interface loopback

Use **reset counters interface loopback** to clear the statistics on the specified or all loopback interfaces.

Syntax

reset counters interface loopback [*interface-number*]

Views

User view

Predefined user roles

network-admin

Parameters

interface-number: Specifies a loopback interface by its number, which can be the number of any existing loopback interface. If you do not specify the *interface-number* argument, the command clears the statistics on all loopback interfaces.

Usage guidelines

To determine whether a loopback interface works correctly within a period by collecting the traffic statistics within that period, first use the **reset counters interface** [**loopback** [*interface-number*]] command to clear the statistics. Then have the interface automatically collect the statistics.

This command is available only if a minimum of one loopback interface has been created.

Examples

Clear the statistics on Loopback 1.

```
<Switch> reset counters interface loopback 1
```

Related commands

display interface loopback

2.1.7. reset counters interface null

Use **reset counters interface null** to clear the statistics on the null interface.

Syntax

reset counters interface null [**0**]

Views

User view

Predefined user roles

network-admin

Parameters

0: Specifies the number of the null interface, which is always 0.

Usage guidelines

To determine whether the null interface works correctly within a period by collecting the traffic statistics within that period, first use the **reset counters interface** [**null** [**0**]] command to clear the statistics. Then have the interface automatically collect the statistics.

Examples

Clear the statistics on Null 0.

```
<Switch> reset counters interface null 0
```

Related commands

display interface null

2.1.8. shutdown

Use **shutdown** to shut down a loopback interface.

Use **undo shutdown** to bring up a loopback interface.

Syntax

shutdown

undo shutdown

Default

A loopback interface is up.

Views

Loopback interface view

Predefined user roles

network-admin

Usage guidelines

Use the **shutdown** command with caution, because the command disconnects the connection of the interface and disables the interface from communicating.

Examples

Shut down Loopback 1.

```
<Switch> system-view
[Switch] interface loopback 1
[Switch-LoopBack1] shutdown
```

Contents

A page of this section is **3-x-x**

3. Bulk interface configuration commands 3-1
3.1. Bulk interface configuration commands 3-1
3.1.1. display interface range 3-1
3.1.2. interface range 3-1
3.1.3. interface range name 3-3

3. Bulk interface configuration commands

3.1. Bulk interface configuration commands

3.1.1. display interface range

Use **display interface range** to display information about named interface ranges created by using the **interface range name** command.

Syntax

display interface range [**name** *name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

name *name*: Specifies an interface range by its name, a case-sensitive string of 1 to 32 characters. If you do not specify an interface range name, this command displays information about all interface ranges created by using the **interface range name** command.

Examples

Display information about the interface ranges created by using the **interface range name** command.

```
<Switch> display interface range
Interface range name t2 GigabitEthernet1/0/1 GigabitEthernet1/0/2
Interface range name test GigabitEthernet1/0/3 GigabitEthernet1/0/4
```

The output shows the following:

- Interfaces GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 are added to interface range **t2**.
- Interfaces GigabitEthernet 1/0/3 and GigabitEthernet 1/0/4 are added to interface range **test**.

Related commands

interface range name

3.1.2. interface range

Use **interface range** to create an interface range and enter the interface range view.

Syntax

interface range *interface-list*

Views

System view

Predefined user roles

network-admin

Parameters

interface-list: Specifies a space-separated list of up to 24 interface items. Each item specifies an interface by its type and number or specifies a subrange of interfaces in the form of *interface-type interface-number1* **to** *interface-type interface-number2*. The start interface number must be identical to or lower than the end interface number.

Usage guidelines

Use this command to bulk configure multiple interfaces with the same feature instead of configuring them one by one. For example, execute the **shutdown** command in interface range view to shut down a range of interfaces.

The interface range created by using this command is not saved to the running configuration. You cannot use the interface range repeatedly. To create an interface range that can be used repeatedly, use the **interface range name** command.

In interface range view, only the commands supported by the first interface in the specified interface list (alphabetically sorted) are available for configuration. To view available commands, enter a question mark (?) in interface range view.

After a command is executed in interface range view, one of the following situations might occur:

- The system displays an error message and stays in interface range view. It means that the execution failed on one or multiple member interfaces.
  - If the execution failed on the first member interface, the command is not executed on any member interfaces.
  - If the execution failed on a non-first member interface, the command takes effect on the remaining member interfaces.
- The system returns to system view. It means that:
  - The command is supported in both system view and interface view.
  - The execution failed on a member interface in interface range view and succeeded in system view.
  - The command is not executed on the subsequent member interfaces.

  You can use the **display this** command to verify the configuration in interface view of each member interface. In addition, if the configuration in system view is not needed, use the **undo** form of the command to remove the configuration.

To verify the configuration of the first member interface, you can execute the **display this** command in interface range view.

When you bulk configure interfaces, follow these guidelines:

- Before you configure an interface as the first interface in an interface range, make sure you can enter the view of the interface by using the **interface** *interface-type interface-number* command.
- Do not assign both an aggregate interface and any of its member interfaces to an interface range. Some commands, after being executed on both an aggregate interface and its member interfaces, can break up the aggregation.
- Understand that the more interfaces you specify, the longer the command execution time.

Examples

Shut down interfaces GigabitEthernet 1/0/1 through GigabitEthernet 1/0/5.

```
<Switch> system-view
[Switch] interface range gigabitethernet 1/0/1 to gigabitethernet 1/0/5
```

```
[Switch-if-range] shutdown
```

3.1.3. interface range name

Use **interface range name** *name* **interface** *interface-list* to create a named interface range and enter the interface range view.

Use **interface range name** *name* without the **interface** keyword to enter the view of a named interface range.

Use **undo interface range name** to delete the interface range with the specified name.

Syntax

interface range name *name* [**interface** *interface-list*]

undo interface range name *name*

Views

System view

Predefined user roles

network-admin

Parameters

name: Specifies an interface range name, a case-sensitive string of 1 to 32 characters.

interface-list: Specifies a space-separated list of up to 24 interface items. Each item specifies an interface by its type and number or a subrange of interfaces in the form of *interface-type interface-number1* **to** *interface-type interface-number2*. The start interface number must be identical to or lower than the end interface number.

Usage guidelines

A named interface range is saved in the running configuration and can be used repeatedly to bulk configure its member interfaces.

In interface range view, only the commands supported by the first interface in the specified interface list (alphabetically sorted) are available for configuration. To view available commands, enter a question mark (?) in interface range view.

After a command is executed in interface range view, one of the following situations might occur:

- The system displays an error message and stays in interface range view. It means that the execution failed on one or multiple member interfaces.
  - If the execution failed on the first member interface, the command is not executed on any member interfaces.
  - If the execution failed on a non-first member interface, the command takes effect on the remaining member interfaces.
- The system returns to system view. It means that:
  - The command is supported in both system view and interface view.
  - The execution failed on a member interface in interface range view and succeeded in system view.
  - The command is not executed on the subsequent member interfaces.

  You can use the **display this** command to verify the configuration in interface view of each member interface. In addition, if the configuration in system view is not needed, use the **undo** form of the command to remove the configuration.

To verify the configuration of the first interface, you can execute the **display this** command in interface range view.

To view the member interfaces of a named interface range, use the **display interface range** command.

When you bulk configure interfaces, follow these guidelines:

- Before you configure an interface as the first interface in an interface range, make sure you can enter the view of the interface by using the **interface** *interface-type interface-number* command.
- Do not assign both an aggregate interface and any of its member interfaces to an interface range. Some commands, after being executed on both an aggregate interface and its member interfaces, can break up the aggregation.
- Understand that the more interfaces you specify, the longer the command execution time.
- To guarantee bulk interface configuration performance, configure fewer than 1000 interface range names.

Examples

Add GigabitEthernet 1/0/1 through GigabitEthernet 1/0/5 to interface range **myEthPort**, and enter the interface range view.

```
<Switch> system-view
[Switch] interface range name myEthPort interface gigabitethernet 1/0/1 to gigabitethernet 1/0/5
[Switch-if-range-myEthPort]
```

Enter the view of interface range **myEthPort**.

```
<Switch> system-view
[Switch] interface range name myEthPort
[Switch-if-range-myEthPort]
```

Related commands

display interface range

Contents

A page of this section is **3-x-x**

4. MAC address table commands ····· 4-1
4.1. MAC address table commands ····· 4-1
4.1.1. display mac-address ····· 4-1
4.1.2. display mac-address aging-time ····· 4-2
4.1.3. display mac-address mac-learning ····· 4-3
4.1.4. display mac-address mac-move ····· 4-4
4.1.5. display mac-address statistics ····· 4-5
4.1.6. mac-address (interface view) ····· 4-6
4.1.7. mac-address (system view) ····· 4-7
4.1.8. mac-address mac-learning enable ····· 4-9
4.1.9. mac-address mac-move fast-update ····· 4-11
4.1.10. mac-address max-mac-count ····· 4-11
4.1.11. mac-address max-mac-count enable-forwarding ····· 4-12
4.1.12. mac-address notification mac-move ····· 4-12
4.1.13. mac-address notification mac-move suppression (interface view) ····· 4-14
4.1.14. mac-address notification mac-move suppression (system view) ····· 4-15
4.1.15. mac-address static source-check enable ····· 4-16
4.1.16. mac-address timer ····· 4-16
4.1.17. snmp-agent trap enable mac-address ····· 4-17

4. MAC address table commands

4.1. MAC address table commands

This document covers the configuration of unicast MAC address entries, including static, dynamic, blackhole, and multiport unicast MAC address entries. For more information about configuring static multicast MAC address entries, see IGMP snooping and IPv6 multicast routing and forwarding in *IP Multicast Configuration Guide*.

4.1.1. display mac-address

Use **display mac-address** to display MAC address entries.

Syntax

display mac-address [*mac-address* [**vlan** *vlan-id*] | [[**dynamic** | **static**] [**interface** *interface-type interface-number*] | **blackhole** | **multiport**] [**vlan** *vlan-id*] [**count**]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

mac-address: Specifies a MAC address in the format of H-H-H. When entering a MAC address, you can omit the leading zeros in each H section. For example, enter f-e2-1 for 000f-00e2-0001.

vlan *vlan-id*: Specifies a VLAN by its ID in the range of 1 to 4094.

dynamic: Displays dynamic MAC address entries.

static: Displays static MAC address entries.

interface *interface-type interface-number*: Specifies an interface by its type and number.

blackhole: Displays blackhole MAC address entries.

multiport: Displays multiport unicast MAC address entries.

count: Displays only the number of MAC address entries that match all entry attributes you specify in the command. Detailed information about MAC address entries is not displayed. For example, you can use the **display mac-address vlan 20 dynamic count** command to display the number of dynamic entries for VLAN 20. If you do not specify an entry attribute, the command displays the number of entries in the MAC address table. If you do not specify this keyword, the command displays detailed information about the specified MAC address entries.

Usage guidelines

A MAC address entry includes a destination MAC address, an outgoing interface, and a VLAN ID.

If you do not specify any parameters, the command displays all MAC address entries.

This command displays dynamic MAC address entries for an aggregate interface only when the aggregate interface has a minimum of one Selected member port.

Multiport unicast MAC address entries have no impact on the MAC address learning. When receiving a frame whose source MAC address matches a multiport unicast entry, the device can still learn the MAC address of the frame and generate a dynamic entry. However, the generated dynamic entry has lower priority. The device prefers to use the multiport unicast entry to forward frames destined for the MAC address in the entry.

Examples

Display MAC address entries for VLAN 100.

```
<Switch> display mac-address vlan 100
MAC Address      VLAN ID    State           Port/Nickname           Aging
0001-0101-0101   100        Multiport       GE1/0/1                 N
                                            GE1/0/2
0033-0033-0033   100        Blackhole       N/A                     N
0000-0000-0002   100        Static          GE1/0/3                 N
f474-8800-5829   100        Learned         GE1/0/4                 Y
```

Display the number of MAC address entries.

```
<Switch> display mac-address count
1 mac address(es) found.
```

Table 4-1 Command output

Field	Description
VLAN ID	ID of the VLAN to which the outgoing interface of the MAC address entry belongs.
State	MAC address entry state: • **Static**—Static MAC address entry. • **Learned**—Dynamic MAC address entry. Dynamic entries can be learned or manually configured. • **Blackhole**—Blackhole MAC address entry. • **Multiport**—Multiport unicast MAC address entry. • **OpenFlow**—MAC address entry for an OpenFlow instance.
Port/Nickname	When the field displays an interface name, the field indicates the outgoing interface for packets that are destined for the MAC address. This field displays **N/A** for a blackhole MAC address entry.
Aging	Whether the entry can age out: • **Y**—The entry can age out. • **N**—The entry never ages out.
mac address(es) found	Number of matching MAC address entries.

Related commands

mac-address

mac-address timer

4.1.2. display mac-address aging-time

Use **display mac-address aging-time** to display the aging timer for dynamic MAC address entries.

Syntax

display mac-address aging-time

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display the aging timer for dynamic MAC address entries.

```
<Switch> display mac-address aging-time
MAC address aging time: 300s.
```

Related commands

mac-address timer

4.1.3. display mac-address mac-learning

Use **display mac-address mac-learning** to display the global MAC address learning status and the MAC learning status of the specified interface or all interfaces.

Syntax

display mac-address mac-learning [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, the command displays the global MAC address learning status and the MAC address learning status of all interfaces.

Examples

Display the global MAC address learning status and the MAC learning status of all interfaces.

```
<Switch> display mac-address mac-learning
Global MAC address learning status: Enabled.

Port                        Learning Status
GE1/0/1                     Enabled
GE1/0/2                     Enabled
```

Table 4-2 Command output

Field	Description
Global MAC address learning status	Global MAC address learning status:

Field	Description
	• Enabled. • Disabled.
Learning Status	MAC address learning status of an interface: • Enabled. • Disabled.

Related commands

mac-address mac-learning enable

4.1.4. display mac-address mac-move

Use **display mac-address mac-move** to display the MAC address move records after the device is started.

Syntax

display mac-address mac-move [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, the command displays MAC address move records for all IRF member devices.

Usage guidelines

When a MAC address frequently moves between the specified two interfaces, Layer 2 loops might occur in the network. To discover and locate loops, you can view the MAC address move records.

In the MAC address move records, records with the same MAC address, VLAN, source port, and current port are considered to be one record.

An IRF member device can generate a maximum of 200 MAC address move records.

Examples

Display the MAC address move records for a slot.

```
<Switch> display mac-address mac-move slot 1
MAC address    VLAN Current port   Source port    Last time           Times
0000-0001-002c 1    GE1/0/1       GE1/0/2       2013-05-20 13:40:52 1
0000-0001-002c 1    GE1/0/2       GE1/0/1       2013-05-20 13:41:30 1
---  2 MAC address moving records found  ---
```

Display the MAC address move records for all slots.

```
<Switch> display mac-address mac-move
MAC address    VLAN Current port  Source port   Last time           Times
0000-0001-002c 1    GE1/0/1       GE1/0/2       2013-05-20 13:40:52 20
0000-0001-002c 1    GE1/0/2       GE1/0/1       2013-05-20 13:41:32 20
0000-0094-0001 1    GE1/0/3       GE1/0/4       2013-05-20 13:42:22 13
```

```
0000-0094-0001 1    GE1/0/4       GE1/0/3       2013-05-20 13:42:21 12
---  4 MAC address moving records found  ---
```

Table 4-3 Command output

Field	Description
VLAN	VLAN to which the outgoing interface of the MAC address entry belongs.
Current port	Interface to which the MAC address was moved.
Source port	Interface from which the MAC address was moved.
Last time	Last time when the MAC address was moved.
Times	Number of MAC address moves after the device is started. For a MAC address record, the number of MAC address moves is increased by 1 when a new MAC address move has the same **MAC address**, **VLAN**, **Current Port**, and **Source Port** fields as the MAC address record.

Related commands

mac-address notification mac-move

4.1.5. display mac-address statistics

Use **display mac-address statistics** to display MAC address table statistics.

Syntax

display mac-address statistics

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

This command displays the number of MAC address entries per type and the maximum number of MAC address entries allowed for each type.

Examples

Display MAC address table statistics.

```
<Switch> display mac-address statistics
MAC Address Count:
Dynamic Unicast Address (Learned) Count:                        3
Dynamic Unicast Address (Security-service-defined) Count:       4
Static Unicast Address (User-defined) Count:                    0
Static Unicast Address (System-defined) Count:                  3
Total Unicast MAC Addresses In Use:                             10
Total Unicast MAC Addresses Available:                          65536
Multicast and Multiport MAC Address Count:                      1
Static Multicast and Multiport MAC Address (User-defined) Count: 1
```

```
Total Multicast and Multiport MAC Addresses Available:          256
```

Table 4-4 Command output

Field	Description
Dynamic Unicast Address (Learned) Count	Number of dynamic unicast MAC address entries triggered by packets.
Dynamic Unicast Address (Security-service-defined) Count	Number of dynamic unicast MAC address entries triggered by the security service.
Static Unicast Address (User-defined) Count	Number of static unicast MAC address entries added by users.
Static Unicast Address (System-defined) Count	Number of static unicast MAC address entries added by the system.
Total Unicast MAC Addresses In Use	Number of unicast MAC address entries.
Total Unicast MAC Addresses Available	Maximum number of unicast MAC address entries allowed.
Multicast and Multiport MAC Address Count	Number of multicast and multiport unicast MAC address entries.
Static Multicast and Multiport MAC Address (User-defined) Count	Number of static multicast and multiport unicast MAC address entries added by users.
Total Multicast and Multiport MAC Addresses Available	Maximum number of multicast and multiport unicast MAC address entries allowed.

4.1.6. mac-address (interface view)

Use **mac-address** to add or modify a MAC address entry on an interface.

Use **undo mac-address** to delete a MAC address entry on an interface.

Syntax

mac-address { **dynamic** | **multiport** | **static** } *mac-address* **vlan** *vlan-id*

undo mac-address { **dynamic** | **multiport** | **static** } *mac-address* **vlan** *vlan-id*

Default

An interface is not configured with MAC address entries.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

dynamic: Specifies dynamic MAC address entries.

static: Specifies static MAC address entries.

multiport: Specifies multiport unicast MAC address entries. A frame whose destination MAC address matches a multiport unicast MAC address entry is sent out of multiple ports.

mac-address: Specifies a MAC address in the format of H-H-H, excluding multicast, all-zero, and all-F MAC addresses. When entering a MAC address, you can omit the leading zeros in each H section. For example, enter f-e2-1 for 000f-00e2-0001.

vlan *vlan-id*: Specifies an existing VLAN to which the specified interface belongs. The value range for the *vlan-id* argument is 1 to 4094.

Usage guidelines

Typically, the device automatically builds the MAC address table by learning the source MAC addresses of incoming frames on each interface. However, you can manually configure static MAC address entries. For a MAC address, a manually configured static entry takes precedence over a dynamically learned entry. To improve the security for the user device connected to an interface, manually configure a static entry to bind the user device to the interface. Then, the frames destined for the user device (for example, Host A) are always sent out of the interface. Other hosts using the forged MAC address of Host A cannot obtain the frames destined for Host A.

The MAC address entry configuration cannot survive a reboot unless you save it. The dynamic MAC address entries, however, are lost upon reboot whether or not you save the configuration.

Examples

Add a static entry for MAC address 000f-e201-0101 on GigabitEthernet 1/0/1 that belongs to VLAN 2.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] mac-address static 000f-e201-0101 vlan 2
```

Add a static entry for MAC address 000f-e201-0101 on Bridge-Aggregation 1 that belongs to VLAN 1.

```
<Switch> system-view
[Switch] interface bridge-aggregation 1
[Switch-Bridge-Aggregation1] mac-address static 000f-e201-0102 vlan 1
```

Add a multiport unicast MAC address entry for MAC address 0001-0001-0101 on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 that belong to VLAN 2.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] mac-address multiport 0001-0001-0101 vlan 2
[Switch-GigabitEthernet1/0/1] quit
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] mac-address multiport 0001-0001-0101 vlan 2
```

Related commands

display mac-address

mac-address (system view)

4.1.7. mac-address (system view)

Use **mac-address** to add or modify a MAC address entry.

Use **undo mac-address** to delete one or all MAC address entries.

Syntax

mac-address { **dynamic** | **static** } *mac-address* **interface** *interface-type interface-number* **vlan** *vlan-id*

mac-address blackhole *mac-address* **vlan** *vlan-id*

mac-address multiport *mac-address* **interface** *interface-list* **vlan** *vlan-id*

undo mac-address [[**dynamic** | **static**] *mac-address* **interface** *interface-type interface-number* **vlan** *vlan-id*]

undo mac-address [**blackhole** | **dynamic** | **static**] [*mac-address*] **vlan** *vlan-id*

undo mac-address [**dynamic** | **static**] **interface** *interface-type interface-number*

undo mac-address multiport *mac-address* **interface** *interface-list* **vlan** *vlan-id*

undo mac-address [**multiport**] [[*mac-address*] **vlan** *vlan-id*]

Default

The system is not configured with MAC address entries.

Views

System view

Predefined user roles

network-admin

Parameters

dynamic: Specifies dynamic MAC address entries.

static: Specifies static MAC address entries.

blackhole: Specifies blackhole MAC address entries. Packets whose source or destination MAC addresses match blackhole MAC address entries are dropped.

multiport: Specifies multiport unicast MAC address entries. A frame whose destination MAC address matches a multiport unicast MAC address entry is sent out of multiple ports.

mac-address: Specifies a MAC address in the format of H-H-H, excluding multicast, all-zero, and all-F MAC addresses. When entering a MAC address, you can omit the leading zeros in each H section. For example, enter f-e2-1 for 000f-00e2-0001.

vlan *vlan-id*: Specifies an existing VLAN to which the interface belongs. The value range for the *vlan-id* argument is 1 to 4094.

interface *interface-type interface-number*: Specifies an outgoing interface by its type and number.

interface *interface-list*: Specifies a list of up to four interface items. Each interface item can be an individual interface in the format of *interface-type interface-number* or a range of interfaces in the format of *interface-type interface-number1* **to** *interface-type interface-number2*. The interfaces can only be Layer 2 Ethernet interfaces or Layer 2 aggregate interfaces. The value for the *interface-number2* argument cannot be lower than the value for the *interface-number1* argument.

Usage guidelines

You can use this command to configure the following types of MAC address entries:

- Dynamic entries.

  Dynamic entries include manually configured dynamic entries and automatically learned dynamic entries.
- Static entries.

For a MAC address, a manually configured static entry takes precedence over a dynamic entry. To improve the security for the user device connected to an interface, manually configure a static entry to bind the user device to the interface. Then, the frames destined for the user device (for example, Host A) are always sent out of the interface. Other hosts using the forged MAC address of Host A cannot obtain the frames destined for Host A.

- Blackhole entries.

  To drop frames with the specified source MAC addresses or destination MAC addresses, you can configure blackhole entries.

- Multiport unicast entries.

  To send frames with a specific destination MAC address out of multiple ports, configure a multiport unicast entry. When you execute this command for the first time, the command adds an entry. When you execute the command again with the same MAC address and VLAN but with different interfaces, this command adds the specified interfaces for this entry.

A static or blackhole entry can overwrite a dynamic entry, but not vice versa.

If you execute the **undo mac-address** command without specifying any parameters, this command deletes all unicast MAC address entries and static multicast MAC address entries.

You can delete all the MAC address entries (including unicast and static multicast MAC address entries) from the specified VLAN. You can also delete only one type (dynamic, static, blackhole, or multiport unicast) of MAC address entries. You can single out an interface and delete the unicast MAC address entries on it, but not the static multicast MAC address entries.

The MAC address entry configuration cannot survive a reboot unless you save it. The dynamic MAC address entries, however, are lost upon reboot whether or not you save the configuration.

Examples

Add a static entry for MAC address 000f-e201-0101. Then, all frames that are destined for this MAC address are sent out of GigabitEthernet 1/0/1, which belongs to VLAN 2.

```
<Switch> system-view
[Switch] mac-address static 000f-e201-0101 interface gigabitethernet 1/0/1 vlan 2
```

Add a multiport unicast MAC address entry for MAC address 000f-e201-0101. Then, all frames that are destined for this MAC address are sent out of GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3, which belong to VLAN 2.

```
<Switch> system-view
[Switch] mac-address multiport 000f-e201-0101 interface gigabitethernet 1/0/1 to
gigabitethernet 1/0/3 vlan 2
```

Related commands

display mac-address

mac-address (interface view)

4.1.8. mac-address mac-learning enable

Use **mac-address mac-learning enable** to enable MAC address learning globally, on an interface, or on a VLAN.

Use **undo mac-address mac-learning enable** to disable MAC address learning globally, on an interface, or on a VLAN.

Syntax

mac-address mac-learning enable

undo mac-address mac-learning enable

Default

MAC address learning is enabled.

Views

System view

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

VLAN view

Predefined user roles

network-admin

Usage guidelines

To prevent the MAC address table from becoming saturated, you can disable MAC address learning.

For example, a number of packets with different source MAC addresses reaching a device can affect the MAC address table update. To avoid such attacks, you can disable MAC address learning by following these guidelines:

- You can disable MAC address learning on a per-interface basis. If you disable MAC address learning globally, MAC address learning is disabled for all interfaces. The device then stops learning MAC addresses and cannot dynamically update the MAC address table.
- Because disabling MAC address learning can result in broadcast storms, enable broadcast storm suppression after you disable MAC address learning on an interface. For more information about broadcast storm suppression, see *Interface Configuration Guide*.
- With MAC address learning enabled globally, you can disable MAC address learning for an interface or VLAN.
- After MAC address learning is disabled, the device immediately deletes existing dynamic MAC address entries.

This command does not take effect on a VXLAN VSI. For information about VXLAN VSIs, see *VXLAN Configuration Guide*.

Examples

Disable MAC address learning globally.

```
<Switch> system-view
[Switch] undo mac-address mac-learning enable
```

Disable MAC address learning for VLAN 10.

```
<Switch> system-view
[Switch] vlan 10
[Switch-vlan10] undo mac-address mac-learning enable
```

Disable MAC address learning on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] undo mac-address mac-learning enable
```

Disable MAC address learning on Bridge-Aggregation 1.

```
<Switch> system-view
[Switch] interface bridge-aggregation 1
[Switch-Bridge-Aggregation1] undo mac-address mac-learning enable
```

Related commands

display mac-address mac-learning

4.1.9. mac-address mac-move fast-update

Use **mac-address mac-move fast-update** to enable ARP fast update for MAC address moves.

Use **undo mac-address mac-move fast-update** to disable ARP fast update for MAC address moves.

Syntax

mac-address mac-move fast-update

undo mac-address mac-move fast-update

Default

ARP fast update is enabled for MAC address moves.

Views

System view

Predefined user roles

network-admin

Examples

Enable ARP fast update for MAC address moves.

```
<Switch> system-view
[Switch] mac-address mac-move fast-update
```

4.1.10. mac-address max-mac-count

Use **mac-address max-mac-count** to set the MAC learning limit on an interface.

Use **undo mac-address max-mac-count** to restore the default.

Syntax

mac-address max-mac-count *count*

undo mac-address max-mac-count

Default

The number of MAC addresses that can be learned on an interface is not limited.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

count: Specifies the maximum number of MAC addresses that can be learned on an interface. When the argument is set to 0, the interface is not allowed to learn MAC addresses. The value range for this argument is 0 to 4096.

Usage guidelines

This command helps limit the MAC address table size. When the number of MAC address entries learned by an interface reaches the limit, the interface stops learning MAC address entries.

Examples

Configure GigabitEthernet 1/0/1 to learn a maximum of 600 MAC address entries.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] mac-address max-mac-count 600
```

Related commands

mac-address

mac-address max-mac-count enable-forwarding

4.1.11. mac-address max-mac-count enable-forwarding

Use **mac-address max-mac-count enable-forwarding** to enable the device to forward unknown frames received on an interface after the MAC learning limit on the interface is reached. Unknown frames refer to frames whose source MAC addresses are not in the MAC address table.

Use **undo mac-address max-mac-count enable-forwarding** to disable the device from forwarding unknown frames received on an interface after the MAC learning limit on the interface is reached.

Syntax

mac-address max-mac-count enable-forwarding

undo mac-address max-mac-count enable-forwarding

Default

When the MAC learning limit on an interface is reached, the device can forward unknown frames received on the interface.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Examples

Configure GigabitEthernet 1/0/1 to learn a maximum of 600 MAC address entries.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] mac-address max-mac-count 600
```

Disable the device from forwarding unknown frames received on GigabitEthernet 1/0/1 after the MAC learning limit on GigabitEthernet 1/0/1 is reached.

```
[Switch-GigabitEthernet1/0/1] undo mac-address max-mac-count enable-forwarding
```

Related commands

mac-address

mac-address max-mac-count

4.1.12. mac-address notification mac-move

Use **mac-address notification mac-move** to enable MAC address move notifications and optionally specify a MAC move detection interval.

Use **undo mac-address notification mac-move** to disable MAC address move notifications.

Syntax

mac-address notification mac-move [**interval** *interval*]

undo mac-address notification mac-move

Default

MAC address move notifications are disabled.

Views

System view

Predefined user roles

network-admin

Parameters

interval *interval*: Specifies the interval for detecting MAC address moves, in the range of 1 to 60 minutes. If you do not specify this option, the default setting of 1 minute is used.

Usage guidelines

With MAC address move notifications enabled, the system records the MAC address move logs every MAC move detection interval. Each record of the MAC address move logs contains the following information:

- MAC address.
- VLAN ID of the MAC address entry.
- Current port and source port of the MAC address moves.
- Number of MAC address moves within a detection interval.

A MAC address can have only one MAC address move record. If a MAC address moves multiple times, the new record overrides the old record.

Within a detection interval, an IRF member device can record MAC address move information for a maximum of 20 MAC addresses. The records are ranked in descending order of MAC move counts. When the MAC move count of a new record is higher than the MAC move count of any existing record, the device performs the following operations:

- Discards the record that has the lowest MAC move count.
- Ranks the MAC address move records in descending order of MAC move count.

Then in the next detection interval, the device discards all MAC address move records generated in the previous detection interval and starts another round of MAC move record generation.

After you execute this command, the system sends only syslog messages to the information center module. If the **snmp-agent trap enable mac-address** command is also executed, the system also sends SNMP notifications to the SNMP module.

Examples

Enable MAC address move notifications.

```
<Switch> system-view
[Switch] mac-address notification mac-move
[Switch]
%May 14 17:16:45:688 2013 Switch MAC/4/MAC_FLAPPING: MAC address 0000-0012-0034 in VLAN
500 has moved from port GE1/0/1 to port GE1/0/2 for 1 times
```

The output shows that:

- The VLAN ID of MAC address 0000-0012-0034 is VLAN 500.
- The MAC address moved from GigabitEthernet 1/0/1 to GigabitEthernet 1/0/2.
- The MAC address has moved once within a MAC move detection interval.

Related commands

display mac-address mac-move

4.1.13. mac-address notification mac-move suppression (interface view)

Use **mac-address notification mac-move suppression** to enable MAC address move suppression on an interface.

Use **undo mac-address notification mac-move suppression** to disable MAC address move suppression on an interface.

Syntax

mac-address notification mac-move suppression

undo mac-address notification mac-move suppression

Default

MAC address moves are not suppressed.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

This feature shuts an interface down when a MAC address has been moved to or from the interface more than the suppression threshold within a MAC move detection interval. The shutdown interface automatically goes up after a suppression interval. Also, you can use the **shutdown** command and then the **undo shutdown** command to bring up the interface.

When MAC address move suppression shuts an interface down, the system sends only syslog messages to the information center module. If the **snmp-agent trap enable mac-address** command is also executed, the system also sends SNMP notifications to the SNMP module.

Examples

Enable MAC address move suppression on GigabitEthernet 1/0/1.

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] mac-address notification mac-move suppression
```

Related commands

mac-address notification mac-move suppression (system view)

4.1.14. mac-address notification mac-move suppression (system view)

Use **mac-address notification mac-move suppression** to set the suppression interval or the suppression threshold.

Use **undo mac-address notification mac-move suppression** to restore the default.

Syntax

mac-address notification mac-move suppression { **interval** *interval* | **threshold** *threshold* }

undo mac-address notification mac-move suppression { **interval** | **threshold** }

Default

The suppression interval is 30 seconds. The suppression threshold is 3.

Views

System view

Predefined user roles

network-admin

Parameters

interval *interval*: Specifies the MAC address move suppression interval during which a suppressed interface stays down. The value range for the *interval-value* argument is 30 to 86400 seconds. If you do not specify this option, the default suppression interval of 30 seconds is used.

threshold *threshold*: Specifies the suppression threshold for MAC address moves sourced from or destined for an interface within a MAC move detection interval. The value range for this argument is 0 to 1024. If you do not specify this option, the default suppression threshold of 3 is used.

Usage guidelines

For this command to take effect on an interface, you must also enable MAC address move suppression on the interface.

If you set the suppression interval or suppression threshold multiple times, the most recent configuration applies. The suppression interval setting is independent of the suppression threshold setting.

Examples

Set the suppression interval to 40 seconds and the suppression threshold to 1 for MAC address moves.

```
<Switch> system-view
[Switch] mac-address notification mac-move suppression interval 40
[Switch] mac-address notification mac-move suppression threshold 1
```

Related commands

mac-address notification mac-move suppression (interface view)

4.1.15. mac-address static source-check enable

Use **mac-address static source-check enable** to enable the static source check feature.

Use **undo mac-address static source-check enable** to disable the static source check feature.

Syntax

mac-address static source-check enable

undo mac-address static source-check enable

Default

The static source check feature is enabled.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Layer 3 Ethernet interface view

IRF physical interface view

System view

Predefined user roles

network-admin

Examples

Disable the static source check feature on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] undo mac-address static source-check enable
```

4.1.16. mac-address timer

Use **mac-address timer** to set the aging timer for dynamic MAC address entries.

Use **undo mac-address timer** to restore the default.

Syntax

mac-address timer { **aging** *seconds* | **no-aging** }

undo mac-address timer

Default

The aging timer is 300 seconds for dynamic MAC address entries.

Views

System view

Predefined user roles

network-admin

Parameters

aging *seconds*: Specifies an aging timer for dynamic MAC address entries, in seconds. The value range for the *seconds* argument is 10 to 1000000.

memo:

It's possible to establish 10 to 630 in Version 7.1.6.

no-aging: Configures dynamic MAC address entries not to age.

Usage guidelines

To set the aging timer appropriately, follow these guidelines:

- A long aging interval causes the MAC address table to retain outdated entries and fail to accommodate the most recent network changes.
- A short aging interval results in removal of valid entries. Then, unnecessary broadcast packets appear and affect device performance.

Examples

Set the aging time to 500 seconds for dynamic MAC address entries.

```
<Switch> system-view
[Switch] mac-address timer aging 500
```

Related commands

display mac-address aging-time

4.1.17. snmp-agent trap enable mac-address

Use **snmp-agent trap enable mac-address** to enable SNMP notifications for the MAC address table.

Use **undo snmp-agent trap enable mac-address** to disable SNMP notifications for the MAC address table.

Syntax

snmp-agent trap enable mac-address [**mac-move**]

undo snmp-agent trap enable mac-address [**mac-move**]

Default

SNMP notifications are enabled for the MAC address table.

Views

System view

Predefined user roles

network-admin

Parameters

mac-move: Specifies notifications about the MAC address moves for the MAC address table. If you do not specify this keyword, the command enables all types of SNMP notifications for the MAC address table.

Usage guidelines

To report critical MAC address move events to an NMS, enable SNMP notifications for the MAC address table. For MAC address move event notifications to be sent correctly, you must also configure SNMP on the device.

When SNMP notifications are disabled for the MAC address table, the device sends the generated logs to the information center. To display the logs, configure the log destination and output rule configuration in the information center.

For information about SNMP and information center configuration, see the network management and monitoring configuration guide for the device.

The MAC address table supports only SNMP notifications about MAC address moves. When you enable or disable SNMP notifications about MAC address moves, you enable or disable all types of SNMP notifications for the MAC address table.

Examples

Disable SNMP notifications about MAC address moves for the MAC address table.

```
<Switch> system-view
[Switch] undo snmp-agent trap enable mac-address mac-move
```

Related commands

mac-address notification mac-move

Contents

A page of this section is **3-x-x**

5. MAC Information commands ····· 5-1
5.1. MAC Information commands ····· 5-1
5.1.1. mac-address information enable (interface view) ····· 5-1
5.1.2. mac-address information enable (system view) ····· 5-1
5.1.3. mac-address information interval ····· 5-2
5.1.4. mac-address information mode ····· 5-3
5.1.5. mac-address information queue-length ····· 5-3

5. MAC Information commands

5.1. MAC Information commands

5.1.1. mac-address information enable (interface view)

Use **mac-address information enable** to enable MAC Information on an interface.

Use **undo mac-address information enable** to disable MAC Information on an interface.

Syntax

mac-address information enable { **added** | **deleted** }

undo mac-address information enable { **added** | **deleted** }

Default

MAC Information is disabled on an interface.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

added: Enables the device to record MAC change information when a new MAC address is learned on an interface.

deleted: Enables the device to record MAC change information when an existing MAC address is deleted.

Usage guidelines

Before you enable MAC Information on an interface, enable MAC Information globally.

Examples

Enable MAC Information on GigabitEthernet 1/0/1 to enable the interface to record MAC change information when learning a new MAC address.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] mac-address information enable added
```

Related commands

mac-address information enable (system view)

5.1.2. mac-address information enable (system view)

Use **mac-address information enable** to enable MAC Information globally.

Use **undo mac-address information enable** to disable MAC Information globally.

Syntax

mac-address information enable

undo mac-address information enable

Default

MAC Information is disabled globally.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Before you enable MAC Information on an interface, enable MAC Information globally.

Examples

Enable MAC Information globally.

```
<Switch> system-view
[Switch] mac-address information enable
```

Related commands

mac-address information enable (interface view)

5.1.3. mac-address information interval

Use **mac-address information interval** to set the MAC change notification interval.

Use **undo mac-address information interval** to restore the default.

Syntax

mac-address information interval *interval*

undo mac-address information interval

Default

The MAC change notification interval is 1 second.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the MAC change notification interval in the range of 1 to 20000 seconds.

Usage guidelines

To prevent syslog messages or SNMP notifications from being sent too frequently, set the MAC change notification interval to a larger value.

Examples

Set the MAC change notification interval to 200 seconds.

```
<Switch> system-view
[Switch] mac-address information interval 200
```

5.1.4. mac-address information mode

Use **mac-address information mode** to set the MAC Information mode. The MAC Information mode specifies the type of messages (syslog messages or SNMP notifications) used to notify MAC changes.

Use **undo mac-address information mode** to restore the default.

Syntax

mac-address information mode { **syslog** | **trap** }

undo mac-address information mode

Default

SNMP notifications are sent to notify MAC changes.

Views

System view

Predefined user roles

network-admin

Parameters

syslog: Specifies that the device sends syslog messages to notify MAC changes.

trap: Specifies that the device sends SNMP notifications to notify MAC changes.

Examples

Configure the MAC Information mode as **trap**.

```
<Switch> system-view
[Switch] mac-address information mode trap
```

5.1.5. mac-address information queue-length

Use **mac-address information queue-length** to set the MAC Information queue length.

Use **undo mac-address information queue-length** to restore the default.

Syntax

mac-address information queue-length *value*

undo mac-address information queue-length

Default

The MAC Information queue length is 50.

Views

System view

Predefined user roles

network-admin

Parameters

value: Specifies the MAC Information queue length in the range of 0 to 1000. The MAC Information queue length indicates the number of MAC change messages.

Usage guidelines

If the MAC Information queue length is 0, the device sends a syslog message or SNMP notification immediately after learning or deleting a MAC address.

If the MAC Information queue length is not 0, the device stores MAC changes in the queue:

- The device overwrites the oldest MAC change written into the queue with the most recent MAC change when the following conditions exist:
  - The MAC change notification interval does not expire.
  - The queue has been exhausted.
- The device sends syslog messages or SNMP notifications only if the MAC change notification interval expires.

Examples

Set the MAC Information queue length to 600.

```
<Switch> system-view
[Switch] mac-address information queue-length 600
```

Contents

A page of this section is **3-x-x**

6. Ethernet link aggregation commands 6-1
6.1. Ethernet link aggregation commands 6-1
6.1.1. description 6-1
6.1.2. display interface 6-1
6.1.3. display lacp system-id 6-5
6.1.4. display link-aggregation load-sharing mode 6-6
6.1.5. display link-aggregation member-port 6-7
6.1.6. display link-aggregation summary 6-9
6.1.7. display link-aggregation verbose 6-11
6.1.8. interface bridge-aggregation 6-13
6.1.9. lacp period short 6-14
6.1.10. lacp system-priority 6-15
6.1.11. link-aggregation global load-sharing mode 6-15
6.1.12. link-aggregation load-sharing mode local-first 6-16
6.1.13. link-aggregation mode 6-17
6.1.14. link-aggregation port-priority 6-18
6.1.15. link-aggregation selected-port maximum 6-18
6.1.16. link-aggregation selected-port minimum 6-19
6.1.17. port link-aggregation group 6-20
6.1.18. reset counters interface 6-21
6.1.19. reset lacp statistics 6-22
6.1.20. shutdown 6-22

6. Ethernet link aggregation commands

6.1. Ethernet link aggregation commands

6.1.1. description

Use **description** to configure the description of an interface.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

The description of an interface is *interface-name* **Interface**. For example, the default description of Bridge-Aggregation 1 is **Bridge-Aggregation1 Interface**.

Views

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

text: Specifies a description, a case-sensitive string of 1 to 255 characters.

Examples

Configure the description as **connect to the lab** for Layer 2 aggregate interface Bridge-Aggregation 1.

```
<Switch> system-view
[Switch] interface bridge-aggregation 1
[Switch-Bridge-Aggregation1] description connect to the lab
```

6.1.2. display interface

Use **display interface** to display aggregate interface information.

Syntax

display interface [**bridge-aggregation** [*interface-number*]] [**brief** [**description** | **down**]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

bridge-aggregation: Specifies Layer 2 aggregate interfaces.

interface-number: Specifies an existing aggregate interface number.

brief: Displays brief interface information. If you do not specify this keyword, the command displays detailed interface information.

description: Displays complete interface descriptions. If you do not specify this keyword, the command displays only the first 27 characters of each interface description.

down: Displays information about interfaces in down state and the causes for the down state. If you do not specify this keyword, the command displays information about interfaces in all states.

Usage guidelines

If you do not specify an aggregate interface type, the command displays information about all interfaces.

If you specify an aggregate interface type but do not specify an interface number, the command displays information about all aggregate interfaces of the specified type.

Examples

Display detailed information about Layer 2 aggregate interface Bridge-Aggregation 1.

```
<Switch> display interface bridge-aggregation 1
Bridge-Aggregation1
Current state: UP
IP packet frame type: Ethernet II, hardware address: 000f-e207-f2e0
Description: Bridge-Aggregation1 Interface
Bandwidth: 1000 kbps
2Gbps-speed mode, full-duplex mode
Link speed type is autonegotiation, link duplex type is autonegotiation
PVID: 1
Port link-type: Access
 Tagged VLANs:   None
 UnTagged VLANs: 1
Last clearing of counters: Never
Last 300 seconds input:  6900 packets/sec 885160 bytes/sec    0%
Last 300 seconds output:  3150 packets/sec 404430 bytes/sec    0%
Input (total):  5364747 packets, 686688416 bytes
         2682273 unicasts, 1341137 broadcasts, 1341337 multicasts, 0 pauses
Input (normal):  5364747 packets, 686688416 bytes
         2682273 unicasts, 1341137 broadcasts, 1341337 multicasts, 0 pauses
Input:  0 input errors, 0 runts, 0 giants, 0 throttles
         0 CRC, 0 frame, 0 overruns, - aborts
         - ignored, - parity errors
Output (total): 1042508 packets, 133441832 bytes
         1042306 unicasts, 0 broadcasts, 202 multicasts, - pauses
Output (normal): 1042508 packets, 133441832 bytes
         1042306 unicasts, 0 broadcasts, 202 multicasts, 0 pauses
Output: 0 output errors, - underruns, - buffer failures
         0 aborts, 0 deferred, 0 collisions, 0 late collisions
         - lost carrier, - no carrier
```

Display brief information about Layer 2 aggregate interface Bridge-Aggregation 1.

```
<Switch> display interface bridge-aggregation 1 brief
Brief information on interfaces in bridge mode:
Link: ADM - administratively down; Stby - standby
Speed: (a) - auto
Duplex: (a)/A - auto; H - half; F - full
Type: A - access; T - trunk; H - hybrid
Interface            Link Speed   Duplex Type PVID Description
BAGG1                UP   auto    A      A    1
```

Table 6-1 Command output

Field	Description
Bridge-Aggregation1	Layer 2 aggregate interface name.
Current state	Physical link state of the interface: • **Administratively DOWN**—The interface has been shut down by using the **shutdown** command. • **DOWN**—The interface is administratively up, but its physical state is down (possibly because no physical link exists or the link has failed). • **UP**—The interface is both administratively and physically up.
IP packet frame type	IPv4 packet framing format.
Description	Description of the interface.
Bandwidth	Expected bandwidth of the interface. This field is not displayed when the bandwidth is 0 kbps.
Port priority	Port priority of the interface.
Output queue - Urgent queuing: Size/Length/Discards	Information about the urgent output queue: • **Size**—Number of packets in the queue. • **Length**—Maximum number of packets that the queue can contain. • **Discards**—Number of dropped packets.
Output queue - Protocol queuing: Size/Length/Discards	Information about the protocol output queue: • **Size**—Number of packets in the queue. • **Length**—Maximum number of packets that the queue can contain. • **Discards**—Number of dropped packets.
Output queue - FIFO queuing: Size/Length/Discards	Information about the FIFO output queue: • **Size**—Number of packets in the queue. • **Length**—Maximum number of packets that the queue can contain. • **Discards**—Number of dropped packets.
Unknown-speed mode, unknown-duplex mode	The interface speed and duplex mode are unknown.
Port link-type	Port link type: • Access. • Trunk. • Hybrid.
Tagged VLANs	VLAN whose packets are sent out of this interface with a

Field	Description
	tag.
Untagged VLANs	VLAN whose packets are sent out of this interface without a tag.
Last clearing of counters	Time when the **reset counters interface** command was last used to clear the interface statistics. This field displays **Never** if the **reset counters interface** command has never been used on the interface since device startup.
Last 300 seconds input/output rate	Average input or output rate over the last 300 seconds.
Input/Output (total)	Statistics of all packets received or sent on the interface.
Input/Output (normal)	Statistics of all normal packets received or sent on the interface.
Line protocol state	Data link layer state of the interface: • **UP**. • **DOWN**.
Maximum transmission unit	MTU of the interface.
Internet protocol processing: Disabled	The interface is not assigned an IP address and cannot process IP packets.
Internet address	IP address of the interface. The **primary** attribute indicates that the address is the primary IP address.
Brief information on interfaces in route mode	Brief information about Layer 3 interfaces.
Brief information on interfaces in bridge mode	Brief information about Layer 2 interfaces.
Interface	Abbreviated interface name.
Link	Physical link state of the interface: • **UP**—The interface is physically up. • **DOWN**—The interface is physically down. • **ADM**—The interface has been shut down by using the **shutdown** command. To restore the physical state of the interface, use the **undo shutdown** command. • **Stby**—The interface is a backup interface in standby state.
Speed	Speed of the interface, in bps. This field displays the **(a)** flag next to the speed if the speed is automatically negotiated. This field displays **auto** if the interface is configured to autonegotiate its speed but the autonegotiation has not started.
Duplex	Duplex mode of the interface: • **A**—Autonegotiation. The interface is configured to autonegotiate its duplex mode but the autonegotiation has not started. • **F**—Full duplex. • **F(a)**—Autonegotiated full duplex. • **H**—Half duplex.

Field	Description
	• **H(a)**—Autonegotiated half duplex.
Type	Link type of the interface: • **A**—Access. • **H**—Hybrid. • **T**—Trunk.
Protocol	Data link layer protocol state of the interface: • **UP**—The data link layer protocol of the interface is up. • **DOWN**—The data link layer protocol of the interface is down. • **UP(s)**—The data link layer protocol of the interface is up, but the link is an on-demand link or does not exist. The **(s)** attribute represents the spoofing flag. This value is typical of null interfaces and loopback interfaces.
Primary IP	Primary IP address of the interface. This field displays two hyphens (**--**) if the interface does not have an IP address.
Cause	Cause for the physical link state of an interface to be **DOWN**.

6.1.3. display lacp system-id

Use **display lacp system-id** to display the local system ID.

Syntax

display lacp system-id

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

You can use the **lacp system-priority** command to change the LACP priority of the local system. The LACP priority value is specified in decimal format in the **lacp system-priority** command. However, it is displayed in hexadecimal format in the output from the **display lacp system-id** command.

Examples

Display the local system ID.

```
<Switch> display lacp system-id
Actor System ID: 0x8000, 0000-fc00-6504
```

Table 6-2 Command output

Field	Description
Actor System ID: 0x8000,	Local system ID, which contains the system LACP

Field	Description
0000-fc00-6504	priority (0x8000 in this sample output) and the system MAC address (0000-FC00-6504 in this sample output).

Related commands

lacp system-priority

6.1.4. display link-aggregation load-sharing mode

Use **display link-aggregation load-sharing mode** to display global or group-specific link-aggregation load sharing modes.

Syntax

display link-aggregation load-sharing mode

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display the default global link-aggregation load sharing modes.

```
<Switch> display link-aggregation load-sharing mode
Link-aggregation load-sharing mode:
Layer 2 traffic: packet type-based sharing
Layer 3 traffic: packet type-based sharing
```

Display the configured global link-aggregation load sharing mode.

```
<Switch> display link-aggregation load-sharing mode
Link-aggregation load-sharing mode:
destination-mac address, source-mac address
```

Table 6-3 Command output

Field	Description
Link-aggregation load-sharing mode	Global link-aggregation load sharing mode. By default, this field displays the link-aggregation load sharing modes for Layer 2 and Layer 3 traffic. If you have set the global link-aggregation load sharing mode, this field displays the set mode.
Route-Aggregation10 load-sharing mode	Link-aggregation load sharing mode of aggregation group 10. By default, this field displays the global link-aggregation load sharing modes. If you have set a link-aggregation load sharing mode for this aggregation group, this field displays the set mode.
Layer 2 traffic: packet type-based sharing	Default link-aggregation load sharing mode for Layer 2 traffic. In this sample output, Layer 2 traffic is load shared based on the packet type.

Field	Description
Layer 3 traffic: packet type-based sharing	Default link-aggregation load sharing mode for Layer 3 traffic. In this sample output, Layer 3 traffic is load shared based on the packet type.
destination-mac address, source-mac address	User-configured link-aggregation load sharing mode. In this sample output, traffic is load shared based on source and destination MAC addresses.

6.1.5. display link-aggregation member-port

Use **display link-aggregation member-port** to display detailed link aggregation information for the specified member ports.

Syntax

display link-aggregation member-port [*interface-list* | **auto**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-list: Specifies a list of link aggregation member ports, in the format *interface-type interface-number1* [**to** *interface-type interface-number2*]. The value for the *interface-number2* argument must be equal to or greater than the value for the *interface-number1* argument.

auto: Specifies all link aggregation member ports that are enabled with automatic assignment.

Usage guidelines

A member port in a static aggregation group cannot obtain information about the peer group. For such member ports, the command displays the port number, port priority, and operational key of only the local end.

Examples

Display detailed information about GigabitEthernet 1/0/1, which is a member port of a static aggregation group.

```
<Switch> display link-aggregation member-port gigabitethernet 1/0/1
Flags: A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
       D -- Synchronization, E -- Collecting, F -- Distributing,
       G -- Defaulted, H -- Expired

GigabitEthernet1/0/1:
Aggregate Interface: Bridge-Aggregation1
Port Number: 1
Port Priority: 32768
Oper-Key: 1
```

Display detailed information about GigabitEthernet 1/0/2, which is a member port of a dynamic aggregation group.

```
<Switch> display link-aggregation member-port gigabitethernet 1/0/2
Flags: A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
       D -- Synchronization, E -- Collecting, F -- Distributing,
       G -- Defaulted, H -- Expired

GigabitEthernet1/0/2:
Aggregate Interface: Bridge-Aggregation10
Local:
    Port Number: 2
    Port Priority: 32768
    Oper-Key: 2
    Flag: {ACDEF}
Remote:
    System ID: 0x8000, 000f-e267-6c6a
    Port Number: 26
    Port Priority: 32768
    Oper-Key: 2
    Flag: {ACDEF}
Received LACP Packets: 5 packet(s)
Illegal: 0 packet(s)
Sent LACP Packets: 7 packet(s)
```

Display detailed information about all link aggregation member ports that are enabled with automatic assignment.

```
<Switch> display link-aggregation member-port auto
Flags: A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
       D -- Synchronization, E -- Collecting, F -- Distributing,
       G -- Defaulted, H -- Expired

GigabitEthernet1/0/3:
Preference Aggregation Interface: Bridge-Aggregation11
Aggregate Interface: Bridge-Aggregation11
Local:
    Port Number: 3
    Port Priority: 32768
    Oper-Key: 1
    Flag: {ACDEF}
Remote:
    System ID: 0x8000, a057-75a2-0100
    Port Number: 3
    Port Priority: 32768
    Oper-Key: 1
    Flag: {ACDEF}
Received LACP Packets: 3 packet(s)
Illegal: 0 packet(s)
Sent LACP Packets: 6 packet(s)
```

Table 6-4 Command output

Field	Description
Flags	LACP state flags. This field is one byte long, represented by ABCDEFGH from the least significant bit to the most significant bit. A letter appears when its bit is 1 and does not appear when its bit is 0. • **A**—Indicates whether LACP is active on the port. 1 indicates active. 0 indicates passive. • **B**—Indicates the LACP timeout interval. 1 indicates the short timeout interval. 0 indicates the long timeout interval. • **C**—Indicates whether the sending system considers that the link is aggregatable. 1 indicates yes. 0 indicates no. • **D**—Indicates whether the sending system considers that the link has been aggregated. 1 indicates yes. 0 indicates no. • **E**—Indicates whether the sending system considers that the link can collect frames. 1 indicates yes. 0 indicates no. • **F**—Indicates whether the sending system considers that the link can distribute frames. 1 indicates yes. 0 indicates no. • **G**—Indicates whether the RX state machine of the sending system is in default state. 1 indicates yes. 0 indicates no. • **H**—Indicates whether the RX state machine of the sending system is in expired state. 1 indicates yes. 0 indicates no.
Aggregate Interface	Aggregate interface to which the member port belongs.
Preferred Aggregate Interface	Aggregate interface to which you prefer to assign the member port during automatic assignment.
Local	Information about the local end.
Oper-key	Operational key.
Flag	LACP protocol state flag.
Remote	Information about the peer end.
System ID	Peer system ID, containing the system LACP priority and the system MAC address.
Received LACP Packets	Total number of LACP packets received.
Illegal	Total number of illegal packets.
Sent LACP Packets	Total number of LACP packets sent.

6.1.6. display link-aggregation summary

Use **`display link-aggregation summary`** to display brief information about all aggregation groups.

Syntax

`display link-aggregation summary`

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

Static link aggregation groups cannot obtain information about the peer groups. As a result, the **Partner ID** field displays **None** for a static link aggregation group.

Examples

Display brief information about all aggregation groups.

```
<Switch> display link-aggregation summary
Aggregate Interface Type:
BAGG -- Bridge-Aggregation, BLAGG -- Blade-Aggregation, RAGG -- Route-Aggregation, SCH-B
- Schannel-Bundle
Aggregation Mode: S -- Static, D -- Dynamic
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Actor System ID: 0x8000, 000f-e267-6c6a

AGG          AGG   Partner ID              Selected  Unselected  Individual  Share
Interface    Mode                          Ports     Ports       Ports       Type
--------------------------------------------------------------------------------
RAGG10       S     None                    1         0           0           NonS
BAGG20       D     0x8000,f474-88ff-ff01   2         0           0           Shar
```

Table 6-5 Command output

Field	Description
Aggregate Interface Type	Aggregate interface type: • **BAGG**—Layer 2.
Aggregation Mode	Aggregation group type: • **S**—Static. • **D**—Dynamic.
Loadsharing Type	Load sharing type: • **Shar**—Load-sharing. • **NonS**—Non-load-sharing.
Actor System ID	Local system ID, which contains the local system LACP priority and the local system MAC address.
AGG Interface	Type and number of the aggregate interface.
AGG Mode	Aggregation group type.
Partner ID	System ID of the peer system, which contains the peer system LACP priority and the peer system MAC address.
Selected Ports	Total number of Selected ports.
Unselected Ports	Total number of Unselected ports.
Individual Ports	Total number of Individual ports.
Share Type	Load sharing type.

6.1.7. display link-aggregation verbose

Use **display link-aggregation verbose** to display detailed information about the aggregation groups that correspond to the specified aggregate interfaces.

Syntax

display link-aggregation verbose [**bridge-aggregation** [*interface-number*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

bridge-aggregation: Specifies Layer 2 aggregate interfaces.

interface-number: Specifies an existing aggregate interface by its number.

Usage guidelines

If you do not specify an aggregate interface type, the command displays detailed information about all aggregation groups.

If you specify an aggregate interface type but do not specify an interface number, the command displays detailed information about all aggregation groups of the specified type.

The **bridge-aggregation** keyword is available only when the corresponding aggregate interfaces exist on the device.

This command does not display the interfaces that are enabled with automatic assignment if they have not joined an aggregation group.

Examples

Display detailed information about Layer 2 aggregation group 10, which is a dynamic aggregation group.

```
<Switch> display link-aggregation verbose bridge-aggregation 10
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Port: A -- Auto port, M -- Management port, R -- Reference port
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregate Interface: Bridge-Aggregation10
Aggregation Mode: Dynamic
Loadsharing Type: Shar
Management VLANs: None
System ID: 0x8000, 000f-e267-6c6a
Local:
  Port                Status   Priority Index    Oper-Key               Flag
  GE1/0/1             S        32768    61       2                      {ACDEF}
  GE1/0/2             S        32768    62       2                      {ACDEF}
```

```
  GE1/0/3             S        32768    63       2                     {AG}
Remote:
  Actor               Priority Index    Oper-Key SystemID              Flag
  GE1/0/1(R)          32768    111      2        0x8000, 000f-e267-57ad {ACDEF}
  GE1/0/2             32768    112      2        0x8000, 000f-e267-57ad {ACDEF}
  GE1/0/3             32768    113      0        0x8000, 0000-0000-0000 {DEF}
```

Display detailed information about Layer 2 aggregation group 20, which is a static aggregation group.

```
<Switch> display link-aggregation verbose bridge-aggregation 20
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Port: A -- Auto port, M -- Management port, R -- Reference port
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregate Interface: Bridge-Aggregation20
Aggregation Mode: Static
Loadsharing Type: Shar
Management VLANs: None
  Port              Status  Priority Oper-Key
  GE1/0/1(R)        S       32768    1
  GE1/0/2           S       32768    1
  GE1/0/3           S       32768    1
```

Table 6-6 Command output

Field	Description
Loadsharing Type	Load sharing type: • **Shar**—Load-sharing. • **NonS**—Non-load-sharing.
Port Status	Port state: • **Selected**. • **Unselected**. • **Individual**.
Port	Port type: • **Auto port**—The port is enabled with automatic assignment. • **Management port**—The port is a management port. This field is not supported in the current software version. • **Reference port**—The port is a reference port.
Flags	LACP state flags. This field is one byte long, represented by ABCDEFGH from the least significant bit to the most significant bit. A letter appears when its bit is 1 and does not appear when its bit is 0. • **A**—Indicates whether LACP is active on the port. 1 indicates active. 0 indicates passive. • **B**—Indicates the LACP timeout interval. 1 indicates the short timeout interval. 0 indicates the long timeout interval. • **C**—Indicates whether the sending system considers that the link is aggregatable. 1 indicates yes. 0 indicates no. • **D**—Indicates whether the sending system considers that the link

Field	Description
	has been aggregated. 1 indicates yes. 0 indicates no. • **E**—Indicates whether the sending system considers that the link can collect frames. 1 indicates yes. 0 indicates no. • **F**—Indicates whether the sending system considers that the link can distribute frames. 1 indicates yes. 0 indicates no. • **G**—Indicates whether the RX state machine of the sending system is in default state. 1 indicates yes. 0 indicates no. • **H**—Indicates whether the RX state machine of the sending system is in expired state. 1 indicates yes. 0 indicates no.
Aggregate Interface	Name of the aggregate interface.
Aggregation Mode	Aggregation group type: • **S**—Static. • **D**—Dynamic.
Management VLANs	(This field is not supported in the current software version.) Management VLANs. If no management VLANs are specified, this field displays **None**.
System ID	Local system ID, containing the local system LACP priority and the local system MAC address.
Local	Information about the local end: • **Port**—Port type and number. • **Status**—Port state, which can be Selected, Unselected, or Individual. • **Priority**—Port priority. • **Index**—Port index. • **Oper-Key**—Operational key. • **Flag**—LACP state flag. **NOTE:** For static aggregation groups, the **Flag** field is not displayed.
Remote	Information about the peer end: • **Actor**—Type and number of the local port. This field displays the **(R)** flag next to the port if its peer port is the reference port. • **Priority**—Priority of the peer port. • **Index**—Index of the peer port. • **Oper-Key**—Operational key of the peer port. • **System ID**—System ID of the peer end. • **Flag**—LACP state flag of the peer end.

6.1.8. interface bridge-aggregation

Use **interface bridge-aggregation** to create a Layer 2 aggregate interface and enter its view, or enter the view of an existing Layer 2 aggregate interface.

Use **undo interface bridge-aggregation** to delete a Layer 2 aggregate interface.

Syntax

interface bridge-aggregation *interface-number*

undo interface bridge-aggregation *interface-number*

Default

No Layer 2 aggregate interfaces exist.

Views

System view

Predefined user roles

network-admin

Parameters

interface-number: Specifies a Layer 2 aggregate interface number. The value range for the *interface-number* argument is 1 to 1024.

Usage guidelines

When you create a Layer 2 aggregate interface, the system automatically creates a Layer 2 aggregation group with the same number. The aggregation group operates in static aggregation mode by default.

Deleting a Layer 2 aggregate interface also deletes the Layer 2 aggregation group. At the same time, the member ports of the aggregation group, if any, leave the aggregation group.

Examples

Create Layer 2 aggregate interface Bridge-Aggregation 1, and enter its view.

```
<Switch> system-view
[Switch] interface bridge-aggregation 1
[Switch-Bridge-Aggregation1]
```

6.1.9. lacp period short

Use **lacp period short** to enable the short LACP timeout interval (3 seconds) on an interface.

Use **undo lacp period** to restore the default.

Syntax

lacp period short

undo lacp period

Default

The LACP timeout interval is the long timeout interval (90 seconds) on an interface.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

To avoid traffic interruption during an ISSU, do not enable the short LACP timeout interval before performing the ISSU. For more information about ISSU, see *Fundamentals Configuration Guide*.

Examples

Enable the short LACP timeout interval (3 seconds) on GigabitEthernet 1/0/1.

```
<Switch> system-view
```

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] lacp period short
```

6.1.10. lacp system-priority

Use **lacp system-priority** to set the system LACP priority.

Use **undo lacp system-priority** to restore the default.

Syntax

lacp system-priority *priority*

undo lacp system-priority

Default

The system LACP priority is 32768.

Views

System view

Predefined user roles

network-admin

Parameters

priority: Specifies the system LACP priority in the range of 0 to 65535. The smaller the value, the higher the system LACP priority.

Examples

Set the system LACP priority to 64.

```
<Switch> system-view
[Switch] lacp system-priority 64
```

Related commands

link-aggregation port-priority

6.1.11. link-aggregation global load-sharing mode

Use **link-aggregation global load-sharing mode** to set the global link-aggregation load sharing mode.

Use **undo link-aggregation global load-sharing mode** to restore the default.

Syntax

link-aggregation global load-sharing mode { **destination-ip** | **destination-mac** | **destination-port** | **ingress-port** | **source-ip** | **source-mac** | **source-port** } *

undo link-aggregation global load-sharing mode

Default

The system automatically chooses link-aggregation load sharing mode based on packet types.

Views

System view

Predefined user roles

network-admin

Parameters

destination-ip: Distributes traffic based on destination IP addresses.

destination-mac: Distributes traffic based on destination MAC addresses.

destination-port: Distributes traffic based on destination ports.

ingress-port: Distributes traffic based on ingress ports.

source-ip: Distributes traffic based on source IP addresses.

source-mac: Distributes traffic based on source MAC addresses.

source-port: Distributes traffic based on source ports.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

If an unsupported load sharing mode is set, the device displays an error message.

The following are global load sharing modes supported on the device:

- Load sharing mode automatically determined based on the packet type.
- Source IP.
- Destination IP.
- Source MAC.
- Destination MAC.
- Source IP and destination IP.
- Source IP and source port.
- Destination IP and destination port.
- Source IP, source port, destination IP, and destination port.
- Ingress port.

Examples

Set the global load sharing mode to load share packets based on destination MAC addresses.

```
<Switch> system-view
[Switch] link-aggregation global load-sharing mode destination-mac
```

6.1.12. link-aggregation load-sharing mode local-first

Use **link-aggregation load-sharing mode local-first** to enable local-first load sharing for link aggregation.

Use **undo link-aggregation load-sharing mode local-first** to disable local-first load sharing for link aggregation.

Syntax

link-aggregation load-sharing mode local-first

undo link-aggregation load-sharing mode local-first

Default

Local-first load sharing is enabled for link aggregation.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Use local-first load sharing in a multidevice link aggregation scenario to distribute traffic preferentially across member ports on the ingress card or device. Local-first load sharing takes effect only on known unicast traffic.

If you disable local-first load sharing, packets of an aggregate interface are load shared among all Selected ports on IRF member devices.

Examples

Disable local-first load sharing for link aggregation.

```
<Switch> system-view
[Switch] undo link-aggregation load-sharing mode local-first
```

6.1.13. link-aggregation mode

Use **link-aggregation mode dynamic** to configure an aggregation group to operate in dynamic aggregation mode and enable LACP.

Use **undo link-aggregation mode** to restore the default.

Syntax

link-aggregation mode dynamic

undo link-aggregation mode

Default

An aggregation group operates in static aggregation mode.

Views

Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

If a dynamic aggregation group contains member ports enabled with automatic assignment, changing the aggregation mode to static might cause Selected member ports to become Unselected. At the same time, automatic assignment is disabled automatically on the member ports. As a best practice, make sure a dynamic aggregation group does not contain such member ports before you change its aggregation mode.

Examples

Configure Layer 2 aggregation group 1 to operate in dynamic aggregation mode.

```
<Switch> system-view
[Switch] interface bridge-aggregation 1
[Switch-Bridge-Aggregation1] link-aggregation mode dynamic
```

6.1.14. link-aggregation port-priority

Use **link-aggregation port-priority** to set the port priority of an interface.

Use **undo link-aggregation port-priority** to restore the default.

Syntax

link-aggregation port-priority *priority*

undo link-aggregation port-priority

Default

The port priority of an interface is 32768.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Predefined user roles

network-admin

Parameters

priority: Specifies the port priority in the range of 0 to 65535. The smaller the value, the higher the port priority.

Examples

Set the port priority to 64 for Layer 2 Ethernet interface GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] link-aggregation port-priority 64
```

Set the port priority to 64 for Layer 3 Ethernet interface GigabitEthernet 1/0/2.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] link-aggregation port-priority 64
```

Related commands

lacp system-priority

6.1.15. link-aggregation selected-port maximum

Use **link-aggregation selected-port maximum** to set the maximum number of Selected ports allowed in an aggregation group.

Use **undo link-aggregation selected-port maximum** to restore the default.

Syntax

link-aggregation selected-port maximum *max-number*

undo link-aggregation selected-port maximum

Default

The maximum number of Selected ports allowed in an aggregation group is 8.

Views

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

max-number: Specifies the maximum number of Selected ports allowed in an aggregation group. The value range for this argument is 1 to 8.

Usage guidelines

Executing this command might cause some of the Selected ports in an aggregation group to become Unselected ports.

The maximum number of Selected ports allowed in the aggregation groups must be the same for the local and peer ends.

The maximum number of Selected ports allowed in an aggregation group is limited by one of the following values, whichever value is smaller:

- Maximum number set by using the **link-aggregation selected-port maximum** command.
- Maximum number of Selected ports allowed by the link aggregation capability.

You can implement backup between two ports by performing the following tasks:

- Assigning two ports to an aggregation group.
- Setting the maximum number of Selected ports to 1 for the aggregation group.

Then, only one Selected port is allowed in the aggregation group at any point in time, while the Unselected port acts as a backup port.

Examples

Set the maximum number of Selected ports to 5 for Layer 2 aggregation group 1.

```
<Switch> system-view
[Switch] interface bridge-aggregation 1
[Switch-Bridge-Aggregation1] link-aggregation selected-port maximum 5
```

Related commands

link-aggregation selected-port minimum

6.1.16. link-aggregation selected-port minimum

Use **link-aggregation selected-port minimum** to set the minimum number of Selected ports in an aggregation group.

Use **undo link-aggregation selected-port minimum** to restore the default.

Syntax

link-aggregation selected-port minimum *min-number*

undo link-aggregation selected-port minimum

Default

The minimum number of Selected ports in an aggregation group is not specified.

Views

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

min-number: Specifies the minimum number of Selected ports in an aggregation group required to bring up the aggregate interface. The value range for this argument is 1 to 8.

Usage guidelines

Executing this command might cause all member ports in the aggregation group to become Unselected ports.

The minimum number of Selected ports allowed in the aggregation groups must be the same for the local and peer ends.

Examples

Set the minimum number of Selected ports to 3 for Layer 2 aggregation group 1.

```
<Switch> system-view
[Switch] interface bridge-aggregation 1
[Switch-Bridge-Aggregation1] link-aggregation selected-port minimum 3
```

Related commands

link-aggregation selected-port maximum

6.1.17. port link-aggregation group

Use **port link-aggregation group** to assign an interface to an aggregation group.

Use **undo port link-aggregation group** to remove an interface from the aggregation group to which it belongs.

Syntax

port link-aggregation group *group-id* [force]

undo port link-aggregation group

Memo:

The **force** option is practicable after V7.2.16.

Default

An interface does not belong to any aggregation group.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Predefined user roles

network-admin

Parameters

group-id: Specifies an aggregation group by its aggregate interface number. The value range for the *number* argument is 1 to 1024.

force: Enables the current interface to synchronize attribute configurations from the aggregate interface. If you do not specify this keyword, the current interface does not synchronize attribute

configurations from the aggregate interface when it joins the aggregation group. This keyword is supported only on Layer 2 Ethernet interfaces.

Usage guidelines

A Layer 2 Ethernet interface can be assigned to a Layer 2 aggregation group only.

An interface can belong to only one aggregation group.

The device assigns the interface to the preferred aggregation group as long as the LACPDUs received on the interface match the peer information of the reference port in the group.

If you do not specify a preferred group or if the preferred group match fails, the device attempts to select a matching group from the existing dynamic aggregation groups. If no match is found, the device creates a dynamic aggregation group based on the LACPDUs and assigns the interface to that aggregation group.

Examples

Assign Layer 2 Ethernet interface GigabitEthernet 1/0/1 to Layer 2 aggregation group 1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-aggregation group 1
```

6.1.18. reset counters interface

Use **reset counters interface** to clear statistics for the specified aggregate interfaces.

Syntax

reset counters interface [**bridge-aggregation** | *interface-number*]

Views

User view

Predefined user roles

network-admin

Parameters

bridge-aggregation: Specifies Layer 2 aggregate interfaces.

interface-number: Specifies an existing aggregate interface number.

Usage guidelines

Use this command to clear history statistics before you collect traffic statistics for a time period.

If you do not specify an aggregate interface type, the command clears statistics for all interfaces in the system.

If you specify only an aggregate interface type, the command clears statistics for all aggregate interfaces of the specified type.

The **bridge-aggregation** keyword is available only when the corresponding aggregate interfaces exist on the device.

Examples

Clear statistics for Layer 2 aggregate interface Bridge-Aggregation 1.

```
<Switch> reset counters interface bridge-aggregation 1
```

6.1.19. reset lacp statistics

Use **reset lacp statistics** to clear LACP statistics for the specified link aggregation member ports.

Syntax

reset lacp statistics [**interface** *interface-list*]

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-list*: Specifies a list of link aggregation member ports, in the format *interface-type interface-number1* [**to** *interface-type interface-number2*]. The value for the *interface-number1* argument must be equal to or greater than the value for the *interface-number2* argument. If you do not specify any member ports, the command clears LACP statistics for all member ports.

Examples

Clear LACP statistics for all link aggregation member ports.

```
<Switch> reset lacp statistics
```

Related commands

display link-aggregation member-port

6.1.20. shutdown

Use **shutdown** to shut down an interface.

Use **undo shutdown** to bring up an interface.

Syntax

shutdown

undo shutdown

Views

Layer 2 aggregate interface view

Predefined user roles

network-admin

Examples

Bring up Layer 2 aggregate interface Bridge-Aggregation 1.

```
<Switch> system-view
[Switch] interface bridge-aggregation 1
[Switch-Bridge-Aggregation1] undo shutdown
```

Contents

A page of this section is **3-x-x**

7. Port isolation commands 7-1
7.1. Port isolation commands 7-1
7.1.1. display port-isolate group 7-1
7.1.2. port-isolate enable 7-2
7.1.3. port-isolate group 7-2

7. Port isolation commands

7.1. Port isolation commands

7.1.1. display port-isolate group

Use **display port-isolate group** to display port isolation group information.

Syntax

display port-isolate group [*group-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

group-id: Specifies an isolation group by its ID. The value range is 1 to 8.

Examples

Display all isolation groups.

```
<Switch> display port-isolate group
 Port isolation group information:
 Group ID: 1
 Group members:
    GigabitEthernet1/0/1

 Group ID: 5
 Group members:
    GigabitEthernet1/0/2            GigabitEthernet1/0/4
```

Display information about isolation group 1.

```
<Switch> display port-isolate group 1
 Port isolation group information:
 Group ID: 1
 Group members:
    GigabitEthernet1/0/1
```

Table 7-1 Command output

Field	Description
Group ID	ID of the isolation group.
Group members	Isolated ports in the isolation group. **No ports** indicates that the isolation group does not contain isolated ports.

Related commands

port-isolate enable

7.1.2. port-isolate enable

Use **port-isolate enable** to assign a port to an isolation group.

Use **undo port-isolate enable** to remove a port from an isolation group.

Syntax

port-isolate enable group *group-id*

undo port-isolate enable

Default

The port is not assigned to an isolation group.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

group *group-id*: Specifies an isolation group by its ID. The value range is 1 to 8.

Usage guidelines

The configuration in Layer 2 Ethernet interface view applies only to the interface.

The configuration in Layer 2 aggregate interface view applies to the Layer 2 aggregate interface and its aggregation member ports. If the device fails to apply the configuration to the aggregate interface, it does not assign any aggregation member port to the isolation group. If the failure occurs on an aggregation member port, the device skips the port and continues to assign other aggregation member ports to the isolation group.

To assign ports to an isolation group, make sure the isolation group already exists.

One port can be assigned to only one isolation group.

Examples

Assign GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 to isolation group 1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port-isolate enable group 1
[Switch-GigabitEthernet1/0/1] quit
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port-isolate enable group 1
```

Related commands

display port-isolate group

7.1.3. port-isolate group

Use **port-isolate group** to create an isolation group.

Use **undo port-isolate group** to delete isolation groups.

Syntax

port-isolate group *group-id*

undo port-isolate group { *group-id* | **all** }

Default

No isolation groups exist.

Views

System view

Predefined user roles

network-admin

Parameters

group-id: Specifies an isolation group by its ID. The value range is 1 to 8.

all: Deletes all isolation groups.

Examples

Create isolation group 1.

```
<Switch> system-view
[Switch] port-isolate group 1
```

Contents

A page of this section is **3-x-x**

8. Spanning tree commands ····· 8-1
8.1. Spanning tree commands ····· 8-1
8.1.1. active region-configuration ····· 8-1
8.1.2. bpdu-drop any ····· 8-1
8.1.3. check region-configuration ····· 8-2
8.1.4. display stp ····· 8-3
8.1.5. display stp abnormal-port ····· 8-10
8.1.6. display stp bpdu-statistics ····· 8-11
8.1.7. display stp down-port ····· 8-14
8.1.8. display stp history ····· 8-14
8.1.9. display stp region-configuration ····· 8-16
8.1.10. display stp root ····· 8-17
8.1.11. display stp tc ····· 8-17
8.1.12. instance ····· 8-19
8.1.13. region-name ····· 8-20
8.1.14. reset stp ····· 8-21
8.1.15. revision-level ····· 8-21
8.1.16. snmp-agent trap enable stp ····· 8-22
8.1.17. stp bpdu-protection ····· 8-23
8.1.18. stp bridge-diameter ····· 8-23
8.1.19. stp compliance ····· 8-24
8.1.20. stp config-digest-snooping ····· 8-25
8.1.21. stp cost ····· 8-26
8.1.22. stp dispute-protection ····· 8-27
8.1.23. stp edged-port ····· 8-28
8.1.24. stp enable ····· 8-29
8.1.25. stp global config-digest-snooping ····· 8-30
8.1.26. stp global enable ····· 8-30
8.1.27. stp global mcheck ····· 8-31
8.1.28. stp log enable tc ····· 8-32
8.1.29. stp loop-protection ····· 8-32
8.1.30. stp max-hops ····· 8-33
8.1.31. stp mcheck ····· 8-34
8.1.32. stp mode ····· 8-35
8.1.33. stp no-agreement-check ····· 8-36
8.1.34. stp pathcost-standard ····· 8-36
8.1.35. stp point-to-point ····· 8-37
8.1.36. stp port bpdu-protection ····· 8-38
8.1.37. stp port priority ····· 8-39
8.1.38. stp port shutdown permanent ····· 8-40
8.1.39. stp port-log ····· 8-41
8.1.40. stp priority ····· 8-42
8.1.41. stp pvst-bpdu-protection ····· 8-42
8.1.42. stp region-configuration ····· 8-43
8.1.43. stp role-restriction ····· 8-44
8.1.44. stp root primary ····· 8-44
8.1.45. stp root secondary ····· 8-45
8.1.46. stp root-protection ····· 8-46
8.1.47. stp tc-protection ····· 8-47
8.1.48. stp tc-protection threshold ····· 8-47
8.1.49. stp tc-snooping ····· 8-48
8.1.50. stp timer forward-delay ····· 8-49
8.1.51. stp timer hello ····· 8-50

8.1.52. stp timer max-age ····· 8-51
8.1.53. stp timer-factor ····· 8-52
8.1.54. stp transmit-limit····· 8-52
8.1.55. stp vlan enable ····· 8-53
8.1.56. vlan-mapping modulo····· 8-54

8. Spanning tree commands

8.1. Spanning tree commands

8.1.1. active region-configuration

Use **active region-configuration** to activate your MST region configuration.

Syntax

active region-configuration

Views

MST region view

Predefined user roles

network-admin

Usage guidelines

When you configure MST region parameters, MSTP launches a new spanning tree calculation process that might cause network topology instability. This is most likely to occur when you configure the VLAN-to-instance mapping table. The launch occurs after you execute the **active region-configuration** command or the **stp global enable** command.

As a best practice, use the **check region-configuration** command to determine whether the MST region configurations to be activated are correct. Run this command only when they are correct.

Examples

Map VLAN 2 to MSTI 1 and activate the MST region configuration.

```
<Switch> system-view
[Switch] stp region-configuration
[Switch-mst-region] instance 1 vlan 2
[Switch-mst-region] active region-configuration
```

Related commands

check region-configuration

instance

region-name

revision-level

stp global enable

vlan-mapping modulo

8.1.2. bpdu-drop any

Use **bpdu-drop any** to enable BPDU drop on a port.

Use **undo bpdu-drop any** to disable BPDU drop on a port.

Syntax

bpdu-drop any

undo bpdu-drop any

Default

BPDU drop is disabled on a port.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

This feature allows the device to drop BPDUs of STP, RSTP, MSTP, PVST, LACP, Ethernet OAM, GVRP, and LLDP. Make sure you are fully aware of the impact of this feature when you use it on a live network.

Examples

Enable BPDU drop on port GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] bpdu-drop any
```

8.1.3. check region-configuration

Use **check region-configuration** to display MST region pre-configuration information.

Syntax

check region-configuration

Views

MST region view

Predefined user roles

network-admin

Usage guidelines

Spanning tree devices belong to the same MST region only when they are connected through a physical link and configured with the same details as follows:

- Format selector (0 by default and not configurable).
- MST region name.
- MST region revision level.
- VLAN-to-instance mapping entries in the MST region.

As a best practice, use this command to determine whether the MST region configurations to be activated are correct. Activate them only when they are correct.

Examples

Display MST region pre-configurations.

```
<Switch> system-view
[Switch] stp region-configuration
```

```
[Switch-mst-region] check region-configuration
 Admin Configuration
   Format selector      : 0
   Region name          : 001122334400
   Revision level       : 0
   Configuration digest : 0x3ab68794d602fdf43b21c0b37ac3bca8

   Instance  VLANs Mapped
   0         1, 3 to 4094
   15        2
```

Table 8-1 Command output

Field	Description
Format selector	Format selector of the MST region, which is 0 (not configurable).
Region name	MST region name.
Revision level	Revision level of the MST region.
Instance VLANs Mapped	VLAN-to-instance mappings in the MST region.

Related commands

active region-configuration

instance

region-name

revision-level

vlan-mapping modulo

8.1.4. display stp

Use **display stp** to display spanning tree status and statistics.

Syntax

display stp [**instance** *instance-list* | **vlan** *vlan-id-list*] [**interface** *interface-list* | **slot** *slot-number*] [**brief**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

instance *instance-list*: Specifies a space-separated list of up to 10 MSTI items. Each item specifies an MSTI or a range of MSTIs in the form of *instance-id1* [**to** *instance-id2*]. The value for *instance-id2* must be equal to or greater than the value for *instance-id1*. The value range for the *instance-id* argument is 0 to 4094, and the value 0 represents the CIST.

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094.

interface *interface-list*: Specifies a space-separated list of up to 10 interface items. Each item specifies an interface or a range of interfaces in the form of *interface-type interface-number 1* [**to** *interface-type interface-number 2*]. The interface number for *interface-number 2* must be equal to or greater than the interface number for *interface-number 1*.

brief: Displays brief spanning tree status and statistics. If this keyword is not specified, the command displays detailed spanning tree status and statistics.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information for all member devices.

Usage guidelines

In STP or RSTP mode, the command output is sorted by port name.

- If you do not specify a port, this command applies to all ports.
- If you specify a port list, this command applies to the specified ports.

In PVST mode, the command output is sorted by VLAN ID and by port name in each VLAN.

- If you do not specify a VLAN or port, this command applies to all ports in all VLANs.
- If you only specify a VLAN list but not a port, this command applies to all ports in the specified VLANs.
- If you only specify a port list but not a VLAN, this command applies to the specified ports in all VLANs.
- If you specify both a VLAN list and a port list, this command applies to the ports in the specified VLANs.

In MSTP mode, the command output is sorted by MSTI ID and by port name in each MSTI.

- If you do not specify an MSTI or port, this command applies to all MSTIs on all ports.
- If you specify an MSTI list but not a port, this command applies to all ports in the specified MSTIs.
- If you specify a port list but not an MSTI, this command applies to all MSTIs on the specified ports.
- If you specify both an MSTI list and a port list, this command applies to the specified ports in the specified MSTIs.

Examples

In MSTP mode, display the brief spanning tree status and statistics for MSTI 0 on port GigabitEthernet 1/0/1.

```
<Switch> display stp instance 0 interface GigabitEthernet 1/0/1 brief
 MST ID      Port                        Role  STP State     Protection
 0           0           GigabitEthernet1/0/1         ALTE  DISCARDING    LOOP
```

In PVST mode, display the brief spanning tree status and statistics for VLAN 2 on port GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] stp mode pvst
[Switch] display stp vlan 2 interface gigabitethernet 1/0/1 brief
 VLAN ID     Port                        Role  STP State     Protection
 2           GigabitEthernet1/0/1        ALTE  DISCARDING    LOOP
```

Table 8-2 Command output

Field	Description
MST ID	MSTI ID in the MST region.
Port	Port name, corresponding to each MSTI or VLAN.
Role	Port role: • **ALTE**—The port is an alternate port. • **BACK**—The port is a backup port. • **ROOT**—The port is a root port. • **DESI**—The port is a designated port. • **MAST**—The port is a master port. • **DISA**—The port is disabled.
STP State	Spanning tree status on the port: • **FORWARDING**—The port can receive and send BPDUs and also forward user traffic. • **DISCARDING**—The port can receive and send BPDUs but cannot forward user traffic. • **LEARNING**—The port is in a transitional state. It can receive and send BPDUs but cannot forward user traffic.
Protection	Effective spanning tree protection feature on the port: • **ROOT**—Root guard. • **LOOP**—Loop guard. • **BPDU**—BPDU guard. If no spanning tree protection feature is configured or spanning tree protection is not triggered, this field displays **NONE**.

In MSTP mode, display the detailed spanning tree status and statistics for all MSTIs on all ports.

```
<Switch> display stp
-------[CIST Global Info][Mode MSTP]-------
 Bridge ID           : 32768.0001-0000-0000
 Bridge times        : Hello 2s MaxAge 20s FwdDelay 15s MaxHops 20
 Root ID/ERPC        : 32768.0001-0000-0000, 0
 RegRoot ID/IRPC     : 32768.0001-0000-0000, 0
 RootPort ID         : 0.0
 BPDU-Protection     : Disabled
 Bridge Config-
 Digest-Snooping     : Disabled
 TC or TCN received  : 2
 Time since last TC  : 0 days 0h:0m:58s

----[Port1(GigabitEthernet1/0/1)][FORWARDING]----
 Port protocol       : Enabled
 Port role           : Designated Port (Boundary)
 Port ID             : 128.3
 Port cost(Legacy)   : Config=auto, Active=200
 Desg.bridge/port    : 32768.0001-0000-0000, 128.3
 Port edged          : Config=disabled, Active=disabled
 Point-to-Point      : Config=auto, Active=true
 Transmit limit      : 10 packets/hello-time
```

```
 TC-Restriction      : Disabled
 Role-Restriction    : Disabled
 Protection type     : Config=none, Active=none
 MST BPDU format     : Config=auto, Active=802.1s
 Port Config-
 Digest-Snooping     : Disabled
 Rapid transition    : True
 Num of VLANs mapped : 0
 Port times          : Hello 2s MaxAge 20s FwdDelay 15s MsgAge 0s RemHops 20
 BPDU sent           : 32
          TCN: 0, Config: 0, RST: 0, MST: 32
 BPDU received       : 2
          TCN: 0, Config: 0, RST: 0, MST: 2

-------[MSTI 1 Global Info]-------
 Bridge ID           : 32768.0001-0000-0000
 RegRoot ID/IRPC     : 32768.0001-0000-0000, 0
 RootPort ID         : 0.0
 Master bridge       : 32768.0001-0000-0000
 Cost to master      : 0
 TC received         : 0

----[Port1(GigabitEthernet1/0/1)][FORWARDING]----
 Port protocol       : Enabled
 Port role           : Designated Port (Boundary)
 Port ID             : 128.3
 Port cost(Legacy)   : Config=auto, Active=200
 Desg.bridge/port    : 32768.0001-0000-0000, 128.3
 Protection type     : Config=none, Active=none
 Rapid transition    : True
 Num of VLANs mapped : 64
 Port times          : RemHops 20
```

In PVST mode, display the spanning tree status and statistics for all ports in all VLANs.

```
<Switch> system-view
[Switch] stp mode pvst
[Switch] display stp
-------[VLAN 1 Global Info]-------
Protocol status     : Enabled
Bridge ID           : 32768.000f-e200-2200
Bridge times        : Hello 2s MaxAge 20s FwdDelay 15s
VlanRoot ID/RPC     : 0.f474-880e-6554, 200200
RootPort ID         : 128.48
BPDU-Protection     : Disabled
TC or TCN received  : 2
Time since last TC  : 0 days 0h:5m:42s

 ----[Port1(GigabitEthernet1/0/1)][FORWARDING]----
```

```
 Port protocol       : Enabled
 Port role           : Designated Port
 Port ID             : 128.153
 Port cost(Legacy)   : Config=auto, Active=200
 Desg. bridge/port   : 32768.000f-e200-2200, 128.2
 Port edged          : Config=disabled, Active=disabled
 Point-to-Point      : Config=auto, Active=true
 Transmit limit      : 10 packets/hello-time
 Protection type     : Config=none, Active=none
 Rapid transition    : False
 Port times          : Hello 2s MaxAge 20s FwdDelay 15s MsgAge 2s

-------[VLAN 2 Global Info]-------
Protocol status      : Enabled
Bridge ID            : 32768.000f-e200-2200
Bridge times         : Hello 2s MaxAge 20s FwDly 15s
VlanRoot ID/RPC      : 0.f474-880e-6554, 200200
RootPort ID          : 128.48
BPDU-Protection      : Disabled
TC or TCN received   : 2
Time since last TC   : 0 days 0h:5m:42s
```

In MSTP mode, display the spanning tree status and statistics when the spanning tree feature is disabled.

```
<Switch> display stp
 Protocol status    : Disabled
 Protocol Std.      : IEEE 802.1s
 Version            : 3
 Bridge-Prio.       : 32768
 MAC address        : 000f-e200-8048
 Max age(s)         : 20
 Forward delay(s)   : 15
 Hello time(s)      : 2
 Max hops           : 20
 TC Snooping        : Disabled
```

In PVST mode, display the spanning tree status and statistics when the spanning tree feature is disabled.

```
<Switch> display stp
 Protocol status    : Disabled
 Protocol Std.      : IEEE 802.1w (pvst)
 Version            : 2
 Bridge-Prio.       : 32768
 MAC address        : 3822-d69f-0800
 Max age(s)         : 20
 Forward delay(s)   : 15
 Hello time(s)      : 2
 TC Snooping        : Disabled
```

Table 8-3 Command output

Field	Description
Bridge ID	Bridge ID, which contains the device's priority and its MAC address. For example, in output 32768.000f-e200-2200, the value preceding the dot is the device's priority. The value following the dot is the device's MAC address.
Bridge times	Major parameters for the bridge: • **Hello**—Hello timer. • **MaxAge**—Maximum age timer. • **FwdDelay**—Forward delay timer. • **MaxHops**—Maximum hops within the MST region.
Root ID/ERPC	CIST root ID and external path cost (the path cost from the device to the CIST root).
RegRoot ID/IRPC	CIST regional root ID and internal path cost (the path cost from the device to the CIST regional root).
VlanRoot ID/RPC	VLAN root ID and root path cost (the path cost from the device to the VLAN root bridge).
RootPort ID	Root port ID. The value **0.0** indicates that the device is the root and there is no root port.
BPDU-Protection	Global status of the BPDU guard feature.
Bridge Config-Digest-Snooping	Global status of Digest Snooping.
TC or TCN received	Number of TC/TCN BPDUs received in the MSTI or VLAN.
Time since last TC	Time since the latest topology change in the MSTI or VLAN.
[FORWARDING]	The port is in forwarding state.
[DISCARDING]	The port is in discarding state.
[LEARNING]	The port is in learning state.
Port protocol	Status of the spanning tree feature on the port.
Port role	Port role: • Alternate. • Backup. • Root. • Designated. • Master. • Disabled.
(Boundary)	The port is a regional boundary port.
Port cost(Legacy)	Path cost of the port. The field in parentheses indicates the standard (legacy, dot1d-1998, or dot1t) used for port path cost calculation. • **Config**—Configured value. • **Active**—Actual value.
Desg.bridge/port	Designated bridge ID and port ID of the port. The port ID displayed is insignificant for a port which does not support port priority.
Port edged	The port is an edge port or non-edge port.

Field	Description
	• **Config**—Configured value. • **Active**—Actual value.
Point-to-Point	The port is connected to a point-to-point link or not. • **Config**—Configured value. • **Active**—Actual value.
Transmit limit	Maximum number of BPDUs sent by a port within each hello time.
Protection type	Whether spanning tree protection is configured on the port: • **Config**—Configured spanning tree protection feature. • **Active**—Effective spanning tree protection feature. Spanning tree protection features are as follows: • **ROOT**—Root guard. • **LOOP**—Loop guard. • **BPDU**—BPDU guard. • **PVST BPDU**—PVST BPDU guard. If no spanning tree protection feature is configured or spanning tree protection is not triggered, this field displays **NONE**.
TC-Restriction	Status of TC transmission restriction on the port.
Role-Restriction	Status of port role restriction on the port.
MST BPDU format	Format of the MST BPDUs that the port can send: • **Config**—Configured value (legacy or 802.1s). • **Active**—Actual value (legacy or 802.1s). During MSTP operation, if fast convergence becomes disabled, it changes from "802.1 s compliant" to "legacy."
Port Config-Digest-Snooping	Status of Digest Snooping on the port.
Rapid transition	Indicates whether the port rapidly transits to the forwarding state in the MSTI or VLAN.
Num of VLANs mapped	Number of VLANs that are mapped to the MSTI.
Port times	Major parameters for the port: • **Hello**—Hello timer. • **MaxAge**—Maximum age timer. • **FwdDelay**—Forward delay timer. • **MsgAge**—Message age timer. • **RemHops**—Remaining hops.
BPDU sent	Statistics on sent BPDUs.
BPDU received	Statistics on received BPDUs.
RegRoot ID/IRPC	MSTI regional root/internal path cost.
Root Type	MSTI root type: • **Primary root**. • **Secondary root**.
Master bridge	MSTI root bridge ID.
Cost to master	Path cost from the MSTI to the master bridge.
TC received	Number of received TC BPDUs.

Field	Description
Protocol status	Spanning tree protocol status.
Protocol Std.	Spanning tree protocol standard.
Version	Spanning tree protocol version.
Bridge-Prio.	In MSTP mode: Device's priority in the CIST. In PVST mode: Device's priority in VLAN 1.
Max age(s)	Aging timer for BPDUs (in seconds, which is the same as the aging timer for VLAN 1 in PVST mode).
Forward delay(s)	Port state transition delay (in seconds, which is the same as the port state transition delay for VLAN 1 in PVST mode).
Hello time(s)	Interval for the root bridge to send BPDUs (in seconds, which is the same as the interval for VLAN 1 in PVST mode).
Max hops	Maximum hops in the MSTI.
TC Snooping	Status of TC Snooping: **Enabled** or **Disabled**.

Related commands

reset stp

8.1.5. display stp abnormal-port

Use **display stp abnormal-port** to display history about ports that are blocked by spanning tree protection features.

Syntax

display stp abnormal-port

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

In an MSTI or VLAN, this command can display a maximum of three history records for a port that is blocked by spanning tree protection features.

Examples

In MSTP mode, display history about ports that are blocked by spanning tree protection features.

```
---[GigabitEthernet1/0/1]---
    MST ID   BlockReason                    Time
    0        Root-Protected                 14:39:04 04/15/2016
    0        Root-Protected                 14:39:02 04/15/2016
    0        Root-Protected                 14:39:00 04/15/2016
```

In PVST mode, display history about ports that are blocked by spanning tree protection features.

```
---[GigabitEthernet1/0/1]---
    VLAN ID  BlockReason                    Time
```

```
1         Root-Protected                  14:49:17 04/15/2016
1         Root-Protected                  14:49:15 04/15/2016
1         Root-Protected                  14:49:12 04/15/2016
```

Table 8-4 Command output

Field	Description
MST ID	MSTI of a blocked port.
VLAN ID	VLAN of a blocked port.
BlockReason	Reason that the port was blocked: • **Root-Protected**—Root guard feature. • **Loop-Protected**—Loop guard feature. • **Loopback-Protected**—Self-loop protection. A port in the MSTI receives a BPDU sent by itself. • **Disputed**—Dispute guard. A port receives a low-priority BPDU from a non-blocked designated port in forwarding or learning state. • **InconsistentPortType-Protected**—Inconsistent port type protection. • **InconsistentPvid-Protected**—Inconsistent PVID protection.
Time	Protection feature trigger time.

8.1.6. display stp bpdu-statistics

Use **display stp bpdu-statistics** to display the BPDU statistics for ports.

Syntax

display stp bpdu-statistics [**interface** *interface-type interface-number* [**instance** *instance-list*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number.

instance *instance-list*: Specifies a space-separated list of up to 10 MSTI items. Each item specifies an MSTI or a range of MSTIs in the form of *instance-id1* [**to** *instance-id2*]. The value for *instance-id2* must be equal to or greater than the value for *instance-id1*. The value range for the *instance-id* argument is 0 to 4094, and the value 0 represents the CIST.

Usage guidelines

In MSTP mode, the command output is sorted by port name and by MSTI ID on each port.

- If you do not specify an MSTI or port, this command applies to all MSTIs on all ports.
- If you specify a port but not an MSTI, this command applies to all MSTIs on the port.
- If you specify both an MSTI ID and a port, this command applies to the specified MSTI on the port.

In STP, RSTP, or PVST mode, the command output is sorted by port name.

- If you do not specify a port, this command applies to all ports.
- If you specify a port, this command applies to the port.

Examples

In MSTP mode, display the BPDU statistics for all MSTIs on GigabitEthernet 1/0/1.

```
<Switch> display stp bpdu-statistics interface gigabitethernet 1/0/1
 Port: GigabitEthernet1/0/1

 Instance-Independent:

 Type                        Count      Last Updated
 --------------------------- ---------- -----------------
 Invalid BPDUs               0
 Looped-back BPDUs           0
 Max-aged BPDUs              0
 TCN sent                    0
 TCN received                0
 TCA sent                    0
 TCA received                2          10:33:12 01/13/2011
 Config sent                 0
 Config received             0
 RST sent                    0
 RST received                0
 MST sent                    4          10:33:11 01/13/2011
 MST received                151        10:37:43 01/13/2011

 Instance 0:
 Type                        Count      Last Updated
 --------------------------- ---------- -----------------
 Timeout BPDUs               0
 Max-hoped BPDUs             0
 TC detected                 1          10:32:40 01/13/2011
 TC sent                     3          10:33:11 01/13/2011
 TC received                 0
```

In PVST mode, display the BPDU statistics for GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] stp mode pvst
[Switch] display stp bpdu-statistics interface gigabitethernet 1/0/1
 Port: GigabitEthernet1/0/1

 Type                        Count      Last Updated
 --------------------------- ---------- -----------------
 Invalid BPDUs               0
 Looped-back BPDUs           0
 Max-aged BPDUs              0
 TCN sent                    0
```

```
TCN received                0
TCA sent                    0
TCA received                2           10:33:12 01/13/2010
Config sent                 0
Config received             0
RST sent                    0
RST received                0
MST sent                    4           10:33:11 01/13/2010
MST received                151         10:37:43 01/13/2010
Timeout BPDUs               0
Max-hoped BPDUs             0
TC detected                 511         10:32:40 01/13/2010
TC sent                     8844        10:33:11 01/13/2010
TC received                 1426        10:33:32 01/13/2010
PVID inconsistency BPDUs    0
```

Table 8-5 Command output

Field	Description
Port	Port name.
Instance-Independent	Statistics not related to a specific MSTI.
Type	Statistical item.
Looped-back BPDUs	Number of BPDUs sent and then received by the same port.
Max-aged BPDUs	Number of BPDUs whose max age was exceeded.
TCN sent	Number of sent TCN BPDUs.
TCN received	Number of received TCN BPDUs.
TCA sent	Number of sent TCA BPDUs.
TCA received	Number of received TCA BPDUs.
Config sent	Number of sent configuration BPDUs.
Config received	Number of received configuration BPDUs.
RST sent	Number of sent RSTP BPDUs.
RST received	Number of received RSTP BPDUs.
MST sent	Number of sent MSTP BPDUs.
MST received	Number of received MSTP BPDUs.
Instance	Statistics for a specific MSTI.
Timeout BPDUs	Number of expired BPDUs.
Max-hoped BPDUs	Number of BPDUs whose maximum hops were exceeded.
TC detected	Number of detected topology changes.
TC sent	Number of sent TC BPDUs.
TC received	Number of received TC BPDUs.
PVID inconsistency BPDUs	Number of received PVST BPDUs with a PVID inconsistent with the incoming port.

8.1.7. display stp down-port

Use **display stp down-port** to display information about ports that were shut down by spanning tree protection features.

Syntax

display stp down-port

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display information about ports that were shut down by spanning tree protection features.

```
<Switch> display stp down-port
 Down Port                      Reason
 GigabitEthernet1/0/1           BPDU protection
```

Table 8-6 Command output

Field	Description
Down Port	Name of a port that was shut down by the spanning tree protection features.
Reason	Reason that the port was shut down: • **BPDU protection**—Indicates the BPDU guard feature. • **PVST BPDU protection**—Indicates the PVST BPDU guard feature.

8.1.8. display stp history

Use **display stp history** to display port role calculation history.

Syntax

display stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **history** [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

instance *instance-list*: Specifies a space-separated list of up to 10 MSTI items. Each item specifies an MSTI or a range of MSTIs in the form of *instance-id1* [**to** *instance-id2*]. The value for *instance-id2* must be equal to or greater than the value for *instance-id1*. The value range for the *instance-id* argument is 0 to 4094, and the value 0 represents the CIST.

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information for all member devices.

Usage guidelines

In STP or RSTP mode, the command output is sorted by port role calculation time.

In PVST mode, the command output is sorted by VLAN ID and by port role calculation time in each VLAN.

- If you do not specify a VLAN, this command applies to all VLANs.
- If you specify a VLAN list, this command applies to the specified VLANs.

In MSTP mode, the command output is sorted by MSTI ID and by port role calculation time in each MSTI.

- If you do not specify an MSTI, this command applies to all MSTIs.
- If you specify an MSTI list, this command applies to the specified MSTIs.

Examples

In MSTP mode, display the port role calculation history on the specified slot in MSTI 2.

```
<Switch> display stp instance 2 history slot 1
 -------------- STP slot 1 history trace ---------------
 ------------------  Instance 2   ---------------------
Port GigabitEthernet1/0/1
   Role change         : ROOT->DESI (Aged)
   Time                : 2009/02/08 00:22:56
   Port priority       : 0.f474-8801-6510 0 0.f474-8801-6510 128.1
   Designated priority : 0.f474-8801-6510 0 0.f474-8801-6510 128.1
 Port GigabitEthernet1/0/2
   Role change         : ALTER->ROOT
   Time                : 2009/02/08 00:22:56
   Port priority       : 0.f474-8801-6510 0 0.f474-8801-6510 128.2
                         128.153
   Designated priority : 0.f474-8801-6510 0 0.f474-8801-6510 128.2
                         128.153
```

In PVST mode, display the port role calculation history on the specified slot in VLAN 2.

```
<Switch> display stp vlan 2 history slot 1
 -------------- STP slot 1 history trace ---------------
 ------------------  VLAN 2   ---------------------

 Port GigabitEthernet1/0/1
   Role change         : ROOT->DESI (Aged)
   Time                : 2009/02/08 00:22:56
   Port priority       : 0.f474-8801-6510 0 0.f474-8801-6510 128.1
   Designated priority : 0.f474-8801-6510 0 0.f474-8801-6510 128.1
 Port GigabitEthernet1/0/2
   Role change         : ALTER->ROOT
   Time                : 2009/02/08 00:22:56
```

```
Port priority       : 0.f474-8801-6510 0 0.f474-8801-6510 128.2
Designated priority : 0.f474-8801-6510 0 0.f474-8801-6510 128.2
```

Table 8-7 Command output

Field	Description
Port	Port name.
Role change	Role change of the port (**Aged** means that the change was caused by expiration of the received configuration BPDU).
Time	Time of port role calculation.

8.1.9. display stp region-configuration

Use **display stp region-configuration** to display effective MST region configuration.

Syntax

display stp region-configuration

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

In MSTP mode, display effective MST region configuration.

```
<Switch> display stp region-configuration
 Oper Configuration
   Format selector      : 0
   Region name          : hello
   Revision level       : 0
   Configuration digest : 0x5f762d9a46311effb7a488a3267fca9f

   Instance   VLANs Mapped
   0          21 to 4094
   1          1 to 10
   2          11 to 20
```

Table 8-8 Command output

Field	Description
Format selector	Format selector that is defined by the spanning tree protocol. The default value is 0, and the selector cannot be configured.
Region name	MST region name.
Revision level	Revision level of the MST region. The default value is 0, and the level can be configured by using the **revision-level** command.
VLANs Mapped	VLANs mapped to the MSTI.

Related commands

instance

region-name

revision-level

vlan-mapping modulo

8.1.10. display stp root

Use **display stp root** to display the root bridge information of spanning trees.

Syntax

display stp root

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

In MSTP mode, display the root bridge information of all spanning trees.

```
<Switch> display stp root
 MST ID  Root Bridge ID        ExtPathCost IntPathCost Root Port
 0       0.f474-880e-6554      200200      0           GigabitEthernet1/0/1
```

In PVST mode, display the root bridge information of all spanning trees.

```
<Switch> display stp root
 VLAN ID  Root Bridge ID        ExtPathCost IntPathCost Root Port
 1        0.f474-880e-6554      200200      0           GigabitEthernet1/0/1
```

Table 8-9 Command output

Field	Description
ExtPathCost	External path cost. The path cost of a port is either automatically calculated by the device or manually configured by using the **stp cost** command.
IntPathCost	Internal path cost. The path cost of a port is either automatically calculated by the device or manually configured by using the **stp cost** command.
Root Port	Root port name (displayed only if a port of the device is the root port of the MSTI).

8.1.11. display stp tc

Use **display stp tc** to display the incoming and outgoing TC/TCN BPDU statistics for ports.

Syntax

display stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **tc** [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

instance *instance-list*: Specifies a space-separated list of up to 10 MSTI items. Each item specifies an MSTI or a range of MSTIs in the form of *instance-id1* [**to** *instance-id2*]. The value for *instance-id2* must be equal to or greater than the value for *instance-id1*. The value range for the *instance-id* argument is 0 to 4094, and the value 0 represents the CIST.

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information for all member devices.

Usage guidelines

In STP or RSTP mode, the command output is sorted by port name.

In PVST mode, the command output is sorted by VLAN ID and by port name in each VLAN.

- If you do not specify a VLAN, this command applies to all VLANs.
- If you specify a VLAN list, this command applies to the specified VLANs.

In MSTP mode, the command output is sorted by MSTI ID and by port name in each MSTI.

- If you do not specify an MSTI, this command applies to all MSTIs.
- If you specify an MSTI list, this command applies to the specified MSTIs.

Examples

In MSTP mode, display the incoming and outgoing TC/TCN BPDU statistics for all ports on slot 1 in MSTI 0.

```
<Switch> display stp instance 0 tc slot 1
 -------------- STP slot 1 TC or TCN count -------------
 MST ID      Port                      Receive      Send
 0           GigabitEthernet1/0/1      6            4
 0           GigabitEthernet1/0/2      0            2
```

In PVST mode, display the incoming and outgoing TC/TCN BPDU statistics for all ports on slot 1 in VLAN 2.

```
<Switch> display stp vlan 2 tc slot 1
 -------------- STP slot 1 TC or TCN count -------------
 VLAN ID     Port                      Receive      Send
 2           GigabitEthernet1/0/1      6            4
 2           GigabitEthernet1/0/2      0            2
```

Table 8-10 Command output

Field	Description
Port	Port name.

Field	Description
Receive	Number of TC/TCN BPDUs received on a port.
Send	Number of TC/TCN BPDUs sent by a port.

8.1.12. instance

Use **instance** to map a list of VLANs to an MSTI.

Use **undo instance** to remap the specified VLAN or all VLANs to the CIST (MSTI 0).

Syntax

instance *instance-id* **vlan** *vlan-id-list*

undo instance *instance-id* [**vlan** *vlan-id-list*]

Default

All VLANs are mapped to the CIST.

Views

MST region view

Predefined user roles

network-admin

Parameters

instance-id: Specifies an MSTI ID in the range of 0 to 4094. A value of 0 represents the CIST. The value range for the *instance-id* argument is 1 to 4094 for the **undo instance** command.

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094.

Usage guidelines

CAUTION:
Use caution with global Digest Snooping in the following situations:

- When you modify the VLAN-to-instance mappings.
- When you restore the default MST region configuration.

If the local device has different VLAN-to-instance mappings than its neighboring devices, loops or traffic interruption will occur.

If you do not specify any VLANs in the **undo instance** command, all VLANs mapped to the specified MSTI are remapped to the CIST.

You cannot map a VLAN to different MSTIs. If you map a VLAN that has been mapped to an MSTI to a new MSTI, the old mapping is automatically deleted.

You can configure VLAN-to-instance mapping for up to 65 MSTIs.

After configuring this command, run the **active region-configuration** command to activate the VLAN-to-instance mapping.

Examples

Map VLAN 2 to MSTI 1.

```
<Switch> system-view
[Switch] stp region-configuration
[Switch-mst-region] instance 1 vlan 2
```

Related commands

active region-configuration

check region-configuration

display stp region-configuration

8.1.13. region-name

Use **region-name** to configure the MST region name.

Use **undo region-name** to restore the default MST region name.

Syntax

region-name *name*

undo region-name

Default

The MST region name of the device is its MAC address.

Views

MST region view

Predefined user roles

network-admin

Parameters

name: Specifies the MST region name, a string of 1 to 32 characters.

Usage guidelines

The MST region name, the VLAN-to-instance mapping table, and the MSTP revision level of a device determine the device's MST region.

After configuring this command, execute the **active region-configuration** command to activate the configured MST region name.

Examples

Set the MST region name of the device to **hello**.

```
<Switch> system-view
[Switch] stp region-configuration
[Switch-mst-region] region-name hello
```

Related commands

active region-configuration

check region-configuration

display stp region-configuration

instance

revision-level

vlan-mapping modulo

8.1.14. reset stp

Use **reset stp** to clear the spanning tree statistics.

Syntax

reset stp [**interface** *interface-list*]

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-list*: Specifies a space-separated list of up to 10 interface items. Each item specifies an interface or a range of interfaces in the form of *interface-type interface-number 1* [**to** *interface-type interface-number 2*]. The interface number for *interface-number 2* must be equal to or greater than the interface number for *interface-number 1*. If you do not specify this option, this command clears the spanning tree statistics on all ports.

Examples

Clear the spanning tree statistics on ports GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3.

```
<Switch> reset stp interface gigabitethernet 1/0/1 to gigabitethernet 1/0/3
```

Related commands

display stp

8.1.15. revision-level

Use **revision-level** to configure the MSTP revision level.

Use **undo revision-level** to restore the default MSTP revision level.

Syntax

revision-level *level*

undo revision-level

Default

The MSTP revision level is 0.

Views

MST region view

Predefined user roles

network-admin

Parameters

level: Specifies an MSTP revision level in the range of 0 to 65535.

Usage guidelines

The MSTP revision level, the MST region name, and the VLAN-to-instance mapping table of a device determine the device's MST region.

After configuring this command, execute the **active region-configuration** command to activate the configured MST region level.

Examples

Set the MSTP revision level of the MST region to 5.

```
<Switch> system-view
[Switch] stp region-configuration
[Switch-mst-region] revision-level 5
```

Related commands

active region-configuration

check region-configuration

display stp region-configuration

instance

region-name

vlan-mapping modulo

8.1.16. snmp-agent trap enable stp

Use **snmp-agent trap enable stp** to enable SNMP notifications for new-root election events or spanning tree topology changes.

Use **undo snmp-agent trap enable stp** to disable SNMP notifications for new-root election events or spanning tree topology changes.

Syntax

snmp-agent trap enable stp [**new-root** | **tc**]

undo snmp-agent trap enable stp [**new-root** | **tc**]

Default

SNMP notifications are disabled for new-root election events.

In MSTP mode, SNMP notifications are enabled in MSTI 0 and disabled in other MSTIs for spanning tree topology changes.

In PVST mode, SNMP notifications are disabled for spanning tree topology changes in all VLANs.

Views

System view

Predefined user roles

network-admin

Parameters

new-root: Enables the device to send notifications if the device is elected as a new root bridge. This keyword applies only to STP, MSTP, and RSTP modes.

tc: Enables the device to send notifications if the device receives TCN BPDUs. This keyword applies only to PVST mode.

Usage guidelines

If no keyword is specified, the **snmp-agent trap enable stp** command applies to SNMP notifications for different events as follows:

- In STP, MSTP, and RSTP modes, the command applies to SNMP notifications for new-root election events.
- In PVST mode, the command applies to SNMP notifications for spanning tree topology changes.

Examples

Enable SNMP notifications for new-root election events.

```
<Switch> system-view
[Switch] snmp-agent trap enable stp new-root
```

8.1.17. stp bpdu-protection

Use **stp bpdu-protection** to enable BPDU guard globally.

Use **undo stp bpdu-protection** to disable BPDU guard globally.

Syntax

stp bpdu-protection

undo stp bpdu-protection

Default

BPDU guard is globally disabled.

Views

System view

Predefined user roles

network-admin

Examples

Enable BPDU guard globally.

```
<Switch> system-view
[Switch] stp bpdu-protection
```

Related commands

stp edged-port

stp port bpdu-protection

8.1.18. stp bridge-diameter

Use **stp bridge-diameter** to set the network diameter. The switched network diameter refers to the maximum number of devices on the path for an edge device to reach another through the root bridge.

Use **undo stp bridge-diameter** to restore the default.

Syntax

stp [**vlan** *vlan-id-list*] **bridge-diameter** *diameter*

undo stp [**vlan** *vlan-id-list*] **bridge-diameter**

Default

The network diameter of the switched network is 7.

Views

System view

Predefined user roles

network-admin

Parameters

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094. If you set the STP, RSTP, or MSTP switched network diameter, do not specify this option.

diameter: Specifies the switched network diameter in the range of 2 to 7.

Usage guidelines

An appropriate setting of hello time, forward delay, and max age can speed up network convergence. The values of these timers are related to the network size, and you can set the timers by setting the network diameter. With the network diameter set to 7 (the default), the three timers are also set to their defaults.

In STP, RSTP, or MSTP mode, each MST region is considered as a device. The configured network diameter of the switched network takes effect only on the CIST (or the common root bridge).

In PVST mode, the configured network diameter takes effect only on the root bridges of the specified VLANs.

Examples

In MSTP mode, set the network diameter of the switched network to 5.

```
<Switch> system-view
[Switch] stp bridge-diameter 5
```

In PVST mode, set the network diameter of VLAN 2 in the switched network to 5.

```
<Switch> system-view
[Switch] stp vlan 2 bridge-diameter 5
```

Related commands

stp timer forward-delay

stp timer hello

stp timer max-age

8.1.19. stp compliance

Use **stp compliance** to configure the mode a port uses to recognize and send MSTP BPDUs.

Use **undo stp compliance** to restore the default.

Syntax

stp compliance { **auto** | **dot1s** | **legacy** }

undo stp compliance

Default

A port automatically recognizes the formats of received MSTP packets and determines the formats of MSTP packets to be sent based on the recognized formats.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

auto: Configures the port to recognize the MSTP BPDU format automatically and determine the format of MSTP BPDUs to send.

dot1s: Configures the port to receive and send only standard-format (802.1s-compliant) MSTP BPDUs.

legacy: Configures the port to receive and send only compatible-format MSTP BPDUs.

Usage guidelines

If this command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If this command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If this command is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

Examples

Configure GigabitEthernet 1/0/1 to send only standard-format (802.1s) MSTP packets.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] stp compliance dot1s
```

8.1.20. stp config-digest-snooping

Use **stp config-digest-snooping** to enable Digest Snooping.

Use **undo stp config-digest-snooping** to disable Digest Snooping.

Syntax

stp config-digest-snooping

undo stp config-digest-snooping

Default

Digest Snooping is disabled.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

For Digest Snooping to take effect, you must enable Digest Snooping both globally and on associated ports. As a best practice, first enable Digest Snooping on ports connected to third-party

vendor devices and then enable the feature globally. Digest Snooping takes effect on the ports simultaneously, which reduces impact on the network.

If this command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If this command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If this command is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

Examples

Enable Digest Snooping on GigabitEthernet 1/0/1 and then globally.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] stp config-digest-snooping
[Switch-GigabitEthernet1/0/1] quit
[Switch] stp global config-digest-snooping
```

Related commands

display stp

stp global config-digest-snooping

8.1.21. stp cost

Use **stp cost** to set the path cost of a port.

Use **undo stp cost** to restore the default.

Syntax

stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **cost** *cost-value*

undo stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **cost**

Default

The device automatically calculates the path costs of ports in each spanning tree based on the corresponding standard.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

instance *instance-list*: Specifies a space-separated list of up to 10 MSTI items. Each item specifies an MSTI or a range of MSTIs in the form of *instance-id1* [**to** *instance-id2*]. The value for *instance-id2* must be equal to or greater than the value for *instance-id1*. The value range for the *instance-id* argument is 0 to 4094, and the value 0 represents the CIST.

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094.

cost-value: Specifies the path cost of the port, with an effective range that varies by path cost calculation standard that is used.

- When the IEEE 802.1d-1998 standard is selected for path cost calculation, the value range for the *cost* argument is 1 to 65535.
- When the IEEE 802.1t standard is selected for path cost calculation, the value range for the *cost* argument is 1 to 200000000.
- When the private standard is selected for path cost calculation, the value range for the *cost* argument is 1 to 200000.

Usage guidelines

Path cost is an important factor in spanning tree calculation. Setting different path costs for a port in MSTIs allows VLAN traffic flows to be forwarded along different physical links. This results in VLAN-based load balancing.

The path cost setting of a port can affect the role selection of the port. When the path cost of a port is changed, the system calculates the role of the port and initiates a state transition.

If this command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If this command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If this command is configured on a member port in an aggregation group, is takes effect only after the port leaves the aggregation group.

If you do not specify an MSTI or VLAN, this command sets the path cost of a port in the MSTP CIST or in the STP or RSTP spanning tree.

Examples

In MSTP mode, set the path cost to 200 for GigabitEthernet 1/0/1 in MSTI 2.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] stp instance 2 cost 200
```

In PVST mode, set the path cost to 200 for GigabitEthernet 1/0/1 in VLAN 2.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] stp vlan 2 cost 200
```

Related commands

display stp

stp pathcost-standard

8.1.22. stp dispute-protection

Use **stp dispute-protection** to enable dispute guard.

Use **undo stp dispute-protection** to disable dispute guard.

Syntax

stp dispute-protection

undo stp dispute-protection

Default

Dispute guard is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Dispute guard blocks a port to prevent loops when a unidirectional link is detected on the port by the spanning tree feature.

In some VLAN networks, an uplink port on a downstream device is configured to deny packets from the PVID. As a result, the downstream device cannot receive BPDUs of the PVID from the upstream device. However, the upstream device can receive BPDUs from the downstream device. In this case, dispute guard blocks the receiving port on the upstream device, which causes traffic interruption.

To ensure service continuity and prevent the link from being blocked, you can disable dispute guard by using the **undo stp dispute-protection** command.

Examples

Disable dispute guard.

```
<Switch> system-view
[Switch] undo stp dispute-protection
```

8.1.23. stp edged-port

Use **stp edged-port** to configure a port as an edge port.

Use **undo stp edged-port** to restore the default.

Syntax

stp edged-port

undo stp edged-port

Default

All ports are non-edge ports.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

A port directly connecting to a user terminal rather than another device or a shared LAN segment can be configured as an edge port. In case the network topology changes, an edge port does not cause a temporary loop. You can enable the port to transit to the forwarding state rapidly by configuring it as an edge port. As a best practice, configure ports that directly connect to user terminals as edge ports.

Typically, configuration BPDUs from other devices cannot reach an edge port, because the edge port does not connect to any other device. When BPDU guard is disabled on a port configured as an edge port, the port acts as a non-edge port if it receives configuration BPDUs.

On a port, the loop guard feature and the edge port setting are mutually exclusive.

If this command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If this command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If this command is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

Examples

Configure GigabitEthernet 1/0/1 as an edge port.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] stp edged-port
```

Related commands

stp bpdu-protection

stp loop-protection

stp port bpdu-protection

stp root-protection

8.1.24. stp enable

Use **stp enable** to enable the spanning tree feature.

Use **undo stp enable** to disable the spanning tree feature.

Syntax

stp enable

undo stp enable

Default

The spanning tree feature is enabled on all ports.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

When you enable the spanning tree feature, the device operates in STP, RSTP, PVST, or MSTP mode, depending on the spanning tree mode setting.

When you enable the spanning tree feature, the device dynamically maintains the spanning tree status of VLANs, based on received configuration BPDUs. When you disable the spanning tree feature, the device stops maintaining the spanning tree status.

If this command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If this command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If this command is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

Examples

In MSTP mode, disable the spanning tree feature on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] undo stp enable
```

Related commands

stp global enable

stp mode

stp vlan enable

8.1.25. stp global config-digest-snooping

Use **stp global config-digest-snooping** to enable Digest Snooping globally.

Use **undo stp global config-digest-snooping** to disable Digest Snooping globally.

Syntax

stp global config-digest-snooping

undo stp global config-digest-snooping

Default

Digest Snooping is disabled globally.

Views

System view

Predefined user roles

network-admin

Usage guidelines

For Digest Snooping to take effect, you must enable Digest Snooping both globally and on associated ports. As a best practice, first enable Digest Snooping on ports connected to third-party vendor devices and then enable the feature globally. Digest Snooping takes effect on the ports simultaneously, which reduces impact on the network.

Examples

Enable Digest Snooping on GigabitEthernet 1/0/1 and then globally.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] stp config-digest-snooping
[Switch-GigabitEthernet1/0/1] quit
[Switch] stp global config-digest-snooping
```

Related commands

display stp

stp config-digest-snooping

8.1.26. stp global enable

Use **stp global enable** to enable the spanning tree feature globally.

Use **undo stp global enable** to disable the spanning tree feature globally.

Syntax

stp global enable

undo stp global enable

Default

The spanning tree feature is globally disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

When you enable the spanning tree feature, the device operates in STP, RSTP, PVST, or MSTP mode, depending on the spanning tree mode setting.

When the spanning tree feature is enabled, the device dynamically maintains the spanning tree status of VLANs based on received configuration BPDUs. When the spanning tree feature is disabled, the device stops maintaining the spanning tree status.

Examples

Enable the spanning tree feature globally.

```
<Switch> system-view
[Switch] stp global enable
```

Related commands

stp enable

stp mode

8.1.27. stp global mcheck

Use **stp global mcheck** to perform mCheck globally.

Syntax

stp global mcheck

Views

System view

Predefined user roles

network-admin

Usage guidelines

When a port on an MSTP, RSTP, or PVST device connects to an STP device and receives STP BPDUs, the port automatically transits to the STP mode. However, the port cannot automatically transit back to the original mode when the following conditions exist:

- The peer STP device is shut down or removed.
- The port cannot detect the change.

In this case, you can perform a mCheck operation to forcibly transit the port to operate in the original mode.

The device operates in STP, RSTP, PVST, or MSTP mode, depending on the spanning tree mode setting.

The **stp global mcheck** command takes effect only when the device operates in MSTP, RSTP, or PVST mode.

Examples

Perform mCheck globally.

```
<Switch> system-view
[Switch] stp global mcheck
```

Related commands

stp mcheck

stp mode

8.1.28. stp log enable tc

Use **stp log enable tc** to enable the device to log events of detecting or receiving TC BPDUs.

Use **undo stp log enable tc** to restore the default.

Syntax

stp log enable tc

undo stp log enable tc

Default

In PVST mode, the device does not generate logs when it detects or receives TC BPDUs.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command applies only to PVST mode.

Examples

In PVST mode, enable the device to log events of detecting or receiving TC BPDUs.

```
<Switch> system-view
[Switch] stp log enable tc
```

8.1.29. stp loop-protection

Use **stp loop-protection** to enable loop guard on a port.

Use **undo stp loop-protection** to disable loop guard on a port.

Syntax

stp loop-protection

undo stp loop-protection

Default

Loop guard is disabled.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

On a port, the loop guard feature is mutually exclusive with the root guard feature or the edge port setting.

If this command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If this command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If this command is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

Examples

Enable loop guard on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] stp loop-protection
```

Related commands

stp edged-port

stp root-protection

8.1.30. stp max-hops

Use **stp max-hops** to set the maximum number of hops for an MST region.

Use **undo stp max-hops** to restore the default.

Syntax

stp max-hops *hops*

undo stp max-hops

Default

The maximum number of hops for an MST region is 20.

Views

System view

Predefined user roles

network-admin

Parameters

hops: Specifies the maximum hops in the range of 1 to 40.

Examples

Set the maximum hops of the MST region to 35.

```
<Switch> system-view
[Switch] stp max-hops 35
```

Related commands

display stp

8.1.31. stp mcheck

Use **stp mcheck** to perform mCheck on a port.

Syntax

stp mcheck

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

When a port on an MSTP, RSTP, or PVST device connects to an STP device and receives STP BPDUs, the port automatically transits to the STP mode. However, the port cannot automatically transit back to the original mode when the following conditions exist:

- The peer STP device is shut down or removed.
- The port cannot detect the change.

In this case, you can perform a mCheck operation to forcibly transit the port to operation in the original mode.

For example, Device A, Device B, and Device C are connected in sequence. Device A runs STP, Device B does not run any spanning tree protocol, and Device C runs RSTP, MSTP, or PVST. When Device C receives an STP BPDU transparently transmitted by Device B, the receiving port transits to the STP mode. If you configure Device B to run RSTP, MSTP, or PVST with Device C, perform mCheck operations on the ports that connect Device B and Device C.

The device operates in STP, RSTP, PVST, or MSTP mode, depending on the spanning tree mode setting.

The **stp mcheck** command takes effect only when the device operates in MSTP, RSTP, or PVST mode.

If this command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If this command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If this command is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

Examples

Perform mCheck on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
```

```
[Switch-GigabitEthernet1/0/1] stp mcheck
```

Related commands

stp global mcheck

stp mode

8.1.32. stp mode

Use **stp mode** to configure the spanning tree operating mode.

Use **undo stp mode** to restore the default.

Syntax

stp mode { **mstp** | **pvst** | **rstp** | **stp** }

undo stp mode

Default

A spanning tree device operates in MSTP mode.

Views

System view

Predefined user roles

network-admin

Parameters

mstp: Configures the spanning tree device to operate in MSTP mode.

pvst: Configures the spanning tree device to operate in PVST mode.

rstp: Configures the spanning tree device to operate in RSTP mode.

stp: Configures the spanning tree device to operate in STP mode.

Usage guidelines

The MSTP mode is compatible with the RSTP mode, and the RSTP mode is compatible with the STP mode.

The PVST mode's compatibility with other modes is as follows:

- **Access port**—The PVST mode is compatible with other modes in any VLAN.
- **Trunk or hybrid port**—The PVST mode is compatible with other modes only in the default VLAN.

Examples

Configure the spanning tree device to operate in STP mode.

```
<Switch> system-view
[Switch] stp mode stp
```

Related commands

stp enable

stp global enable

stp global mcheck

stp mcheck

stp vlan enable

8.1.33. stp no-agreement-check

Use **stp no-agreement-check** to enable No Agreement Check on a port.

Use **undo stp no-agreement-check** to disable No Agreement Check on a port.

Syntax

stp no-agreement-check

undo stp no-agreement-check

Default

No Agreement Check is disabled.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

This command takes effect only after you enable it on the root port.

If this command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If this command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If this command is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

Examples

Enable No Agreement Check on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] stp no-agreement-check
```

8.1.34. stp pathcost-standard

Use **stp pathcost-standard** to specify a standard for the device to use when calculating the default path costs for ports.

Use **undo stp pathcost-standard** to restore the default.

Syntax

stp pathcost-standard { **dot1d-1998** | **dot1t** | **legacy** }

undo stp pathcost-standard

Default

The default standard used by the device is **legacy**.

Views

System view

Predefined user roles

network-admin

Parameters

dot1d-1998: Configures the device to calculate the default path cost for ports based on IEEE 802.1d-1998.

dot1t: Configures the device to calculate the default path cost for ports based on IEEE 802.1t.

legacy: Configures the device to calculate the default path cost for ports based on a private standard.

Usage guidelines

If you change the standard that the device uses in calculating the default path costs, you restore the path costs to the default.

Examples

Configure the device to calculate the default path cost for ports based on IEEE 802.1d-1998.

```
<Switch> system-view
[Switch] stp pathcost-standard dot1d-1998
```

Related commands

display stp

stp cost

8.1.35. stp point-to-point

Use **stp point-to-point** to configure the link type of a port.

Use **undo stp point-to-point** to restore the default.

Syntax

stp point-to-point { **auto** | **force-false** | **force-true** }

undo stp point-to-point

Default

The default setting is **auto,** and the spanning tree device automatically detects whether a port connects to a point-to-point link.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

auto: Specifies automatic detection of the link type.

force-false: Specifies the non-point-to-point link type.

force-true: Specifies the point-to-point link type.

Usage guidelines

When connecting to a non-point-to-point link, a port is incapable of rapid state transition.

You can configure the link type as point-to-point for a Layer 2 aggregate interface or a port that operates in full duplex mode. As a best practice, use the default setting to let the device automatically detect the port link type.

In MSTP or PVST mode, the **stp point-to-point force-false** or **stp point-to-point force-true** command configured on a port takes effect on all MSTIs or VLANs.

Before you set the link type of a port to point-to-point, make sure the port is connected to a point-to-point link. Otherwise, a temporary loop might occur.

If this command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If this command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If this command is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

Examples

Configure the link type of GigabitEthernet 1/0/1 as point-to-point.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] stp point-to-point force-true
```

Related commands

display stp

8.1.36. stp port bpdu-protection

Use **stp port bpdu-protection** to configure BPDU guard on an interface.

Use **undo stp port bpdu-protection** to restore the default.

Syntax

stp port bpdu-protection { **enable** | **disable** }

undo stp port bpdu-protection

Default

BPDU guard is not configured on a per-edge port basis. The status of BPDU guard on an interface is the same as the global BPDU guard status.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

enable: Enables BPDU guard.

disable: Disables BPDU guard.

Usage guidelines

If this command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If this command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If this command is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

Examples

Enable BPDU guard on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] stp port bpdu-protection enable
```

Related commands

stp bpdu-protection

stp edged-port

8.1.37. stp port priority

Use **stp port priority** to set the priority of a port. The port priority affects the role of a port in a spanning tree.

Use **undo stp port priority** to restore the default.

Syntax

stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **port priority** *priority*

undo stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **port priority**

Default

The port priority is 128.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

instance *instance-list*: Specifies a space-separated list of up to 10 MSTI items. Each item specifies an MSTI or a range of MSTIs in the form of *instance-id1* [**to** *instance-id2*]. The value for *instance-id2* must be equal to or greater than the value for *instance-id1*. The value range for the *instance-id* argument is 0 to 4094, and the value 0 represents the CIST.

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094.

priority: Specifies the port priority in the range of 0 to 240 in increments of 16 (as in 0, 16, 32).

Usage guidelines

The smaller the value, the higher the port priority. If all ports on your device use the same priority value, the port priority depends on the port index. The smaller the index, the higher the priority.

If this command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If this command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If this command is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

If you do not specify an MSTI or VLAN, this command configures the priority of the ports in the MSTP CIST or in the STP or RSTP spanning tree.

Examples

In MSTP mode, set the port priority of GigabitEthernet 1/0/1 to 16 in MSTI 2.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] stp instance 2 port priority 16
```

In PVST mode, set the port priority of GigabitEthernet 1/0/1 to 16 in VLAN 2.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] stp vlan 2 port priority 16
```

Related commands

display stp

8.1.38. stp port shutdown permanent

Use **stp port shutdown permanent** to disable the device from reactivating edge ports shut down by BPDU guard.

Use **undo stp port shutdown permanent** to restore the default.

Syntax

stp port shutdown permanent

undo stp port shutdown permanent

Default

The device reactivates an edge port shut down by BPDU guard after the port status detection timer expires.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command takes effect only on edge ports shut down by BPDU guard after this command is configured. The device does not bring up the shutdown ports if you execute the **undo stp port shutdown permanent** command. To bring up these ports, you must use the **undo shutdown** command.

For more information about the port status detection timer, see device management configuration in *Fundamentals Configuration Guide*.

Examples

Disable the device from reactivating edge ports shut down by BPDU guard.

```
<Switch> system-view
[Switch] stp port shutdown permanent
```

8.1.39. stp port-log

Use **stp port-log** to enable outputting port state transition information.

Use **undo stp port-log** to disable outputting port state transition information.

Syntax

stp port-log { **all** | **instance** *instance-list* | **vlan** *vlan-id-list* }

undo stp port-log { **all** | **instance** *instance-list* | **vlan** *vlan-id-list* }

Default

Outputting port state transition information is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

all: Specifies all MSTIs or VLANs.

instance *instance-list*: Specifies a space-separated list of up to 10 MSTI items. Each item specifies an MSTI or a range of MSTIs in the form of *instance-id1* [**to** *instance-id2*]. The value for *instance-id2* must be equal to or greater than the value for *instance-id1*. The value range for the *instance-id* argument is 0 to 4094, and the value 0 represents the CIST.

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094.

Examples

In MSTP mode, enable outputting port state transition information for MSTI 2.

```
<Switch> system-view
[Switch] stp port-log instance 2
%Aug 16 00:49:41:856 2011 Switch STP/3/STP_DISCARDING: Instance 2's port
GigabitEthernet1/0/1 has been set to discarding state.
%Aug 16 00:49:41:856 2011 Switch STP/3/STP_FORWARDING: Instance 2's port
GigabitEthernet1/0/2 has been set to forwarding state.
```

The output shows that GigabitEthernet 1/0/1 in MSTI 2 transited to the discarding state and GigabitEthernet 1/0/2 in MSTI 2 transited to the forwarding state.

In PVST mode, enable outputting port state transition information for VLAN 1 through VLAN 4094.

```
<Switch> system-view
[Switch] stp port-log vlan 1 to 4094
%Aug 16 00:49:41:856 2006 Switch STP/3/STP_DISCARDING: VLAN 2's GigabitEthernet1/0/1 has
been set to discarding state.
%Aug 16 00:49:41:856 2006 Switch STP/3/STP_FORWARDING: VLAN 2's GigabitEthernet1/0/2 has
been set to forwarding state.
```

The output shows that GigabitEthernet 1/0/1 in VLAN 2 transited to the discarding state and GigabitEthernet 1/0/2 in VLAN 2 transited to the forwarding state.

8.1.40. stp priority

Use **stp priority** to set the priority of the device.

Use **undo stp priority** to restore the default.

Syntax

stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **priority** *priority*

undo stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **priority**

Default

The device priority is 32768.

Views

System view

Predefined user roles

network-admin

Parameters

instance *instance-list*: Specifies a space-separated list of up to 10 MSTI items. Each item specifies an MSTI or a range of MSTIs in the form of *instance-id1* [**to** *instance-id2*]. The value for *instance-id2* must be equal to or greater than the value for *instance-id1*. The value range for the *instance-id* argument is 0 to 4094, and the value 0 represents the CIST.

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094.

priority: Specifies the device priority in the range of 0 to 61440 in increments of 4096 (as in 0, 4096, 8192). You can set up to 16 priority values on the device. The smaller the value, the higher the device priority.

Usage guidelines

If you do not specify an MSTI or VLAN, this command configures the priority of the device in the MSTP CIST or in the STP or RSTP spanning tree.

Examples

In MSTP mode, set the device priority to 4096 in MSTI 1.

```
<Switch> system-view
[Switch] stp instance 1 priority 4096
```

In PVST mode, set the device priority to 4096 in VLAN 1.

```
<Switch> system-view
[Switch] stp vlan 1 priority 4096
```

8.1.41. stp pvst-bpdu-protection

Use **stp pvst-bpdu-protection** to enable PVST BPDU guard.

Use **undo stp pvst-bpdu-protection** to disable PVST BPDU guard.

Syntax

stp pvst-bpdu-protection

undo stp pvst-bpdu-protection

Default

PVST BPDU guard is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

PVST BPDU guard enables an MSTP-enabled device to shut down a port if the port receives PVST BPDUs. The shutdown port is brought up after a detection timer expires. To set the detection timer, use the **shutdown-interval** command.

Examples

In MSTP mode, enable PVST BPDU guard.

```
<Switch> system-view
[Switch] stp pvst-bpdu-protection
```

Related commands

shutdown-interval (For more information, see *Fundamentals Command Reference*.)

8.1.42. stp region-configuration

Use **stp region-configuration** to enter MST region view.

Use **undo stp region-configuration** to restore the default MST region configurations.

Syntax

stp region-configuration

undo stp region-configuration

Default

The default settings for an MST region are as follows:

- The MST region name of the device is its MAC address.
- All VLANs are mapped to the CIST.
- The MSTP revision level is 0.

Views

System view

Predefined user roles

network-admin

Usage guidelines

After you enter MST region view, you can configure MST region parameters, including the region name, VLAN-to-instance mappings, and revision level.

Examples

Enter MST region view.

```
<Switch> system-view
```

```
[Switch] stp region-configuration
[Switch-mst-region]
```

8.1.43. stp role-restriction

Use **stp role-restriction** to enable port role restriction.

Use **undo stp role-restriction** to disable port role restriction.

Syntax

stp role-restriction

undo stp role-restriction

Default

Port role restriction is disabled.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

When port role restriction is enabled on a port, the port cannot become a root port.

If this command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If this command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If this command is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

Examples

Enable port role restriction on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] stp role-restriction
```

8.1.44. stp root primary

Use **stp root primary** to configure the device as the root bridge.

Use **undo stp root** to restore the default.

Syntax

stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **root primary**

undo stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **root**

Default

The device is not a root bridge.

Views

System view

Predefined user roles

network-admin

Parameters

instance *instance-list*: Specifies a space-separated list of up to 10 MSTI items. Each item specifies an MSTI or a range of MSTIs in the form of *instance-id1* [**to** *instance-id2*]. The value for *instance-id2* must be equal to or greater than the value for *instance-id1*. The value range for the *instance-id* argument is 0 to 4094, and the value 0 represents the CIST.

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094.

Usage guidelines

Once you specify the device as the root bridge, you cannot change the priority of the device.

If you do not specify an MSTI or VLAN, this command configures the device as the root bridge of the MSTP CIST or of the STP or RSTP spanning tree.

Examples

In MSTP mode, specify the device as the root bridge of MSTI 1.

```
<Switch> system-view
[Switch] stp instance 1 root primary
```

In PVST mode, specify the device as the root bridge of VLAN 1.

```
<Switch> system-view
[Switch] stp vlan 1 root primary
```

Related commands

stp priority

stp root secondary

8.1.45. stp root secondary

Use **stp root secondary** to configure the device as a secondary root bridge.

Use **undo stp root** to restore the default.

Syntax

stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **root secondary**

undo stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **root**

Default

The device is not a secondary root bridge.

Views

System view

Predefined user roles

network-admin

Parameters

instance *instance-list*: Specifies a space-separated list of up to 10 MSTI items. Each item specifies an MSTI or a range of MSTIs in the form of *instance-id1* [**to** *instance-id2*]. The value for *instance-id2* must be equal to or greater than the value for *instance-id1*. The value range for the *instance-id* argument is 0 to 4094, and the value 0 represents the CIST.

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094.

Usage guidelines

Once you specify the device as a secondary root bridge, you cannot change the priority of the device.

If you do not specify an MSTI or VLAN, this command configures a secondary root bridge for the MSTP CIST or the STP or RSTP spanning tree.

Examples

In MSTP mode, specify the device as a secondary root bridge in MSTI 1.

```
<Switch> system-view
[Switch] stp instance 1 root secondary
```

In PVST mode, specify the device as a secondary root bridge in VLAN 1.

```
<Switch> system-view
[Switch] stp vlan 1 root secondary
```

Related commands

stp priority

stp root primary

8.1.46. stp root-protection

Use **stp root-protection** to enable root guard on a port.

Use **undo stp root-protection** to disable root guard on a port.

Syntax

stp root-protection

undo stp root-protection

Default

Root guard is disabled.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

On a port, the loop guard feature and the root guard feature are mutually exclusive.

If this command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If this command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If this command is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

Examples

Enable root guard on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] stp root-protection
```

Related commands

stp edged-port

stp loop-protection

8.1.47. stp tc-protection

Use **stp tc-protection** to enable TC-BPDU attack guard for the device.

Use **undo stp tc-protection** to disable TC-BPDU attack guard for the device.

Syntax

stp tc-protection

undo stp tc-protection

Default

TC-BPDU attack guard is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

With TC-BPDU guard, you can set the maximum number of immediate forwarding address entry flushes that the device can perform every 10 seconds. For TC-BPDUs received that exceed the limit, the device performs a forwarding address entry flush when the interval elapses. This prevents frequent flushing of forwarding address entries.

Examples

Disable TC-BPDU attack guard for the device.

```
<Switch> system-view
[Switch] undo stp tc-protection
```

Related commands

stp tc-protection threshold

8.1.48. stp tc-protection threshold

Use **stp tc-protection threshold** to set the maximum number of forwarding address entry flushes that the device can perform every 10 seconds.

Use **undo stp tc-protection threshold** to restore the default.

Syntax

stp tc-protection threshold *number*

undo stp tc-protection threshold

Default

By default, the device can perform a maximum of 6 forwarding address entry flushes every 10 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

number: Specifies the maximum number of immediate forwarding address entry flushes that the device can perform every 10 seconds. The value is in the range of 1 to 255.

Examples

Configure the device to perform up to 10 forwarding address entry flushes every 10 seconds.

```
<Switch> system-view
[Switch] stp tc-protection threshold 10
```

Related commands

stp tc-protection

8.1.49. stp tc-snooping

Use **stp tc-snooping** to enable TC Snooping.

Use **undo stp tc-snooping** to disable TC Snooping.

Syntax

stp tc-snooping

undo stp tc-snooping

Default

TC Snooping is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

TC Snooping and the spanning tree feature are mutually exclusive. You must globally disable the spanning tree feature before enabling TC Snooping.

Examples

Globally disable the spanning tree feature and enable TC Snooping.

```
<Switch> system-view
```

```
[Switch] undo stp global enable
[Switch] stp tc-snooping
```

Related commands

stp global enable

8.1.50. stp timer forward-delay

Use **stp timer forward-delay** to set the forward delay timer.

Use **undo stp timer forward-delay** to restore the default.

Syntax

stp [**vlan** *vlan-id-list*] **timer forward-delay** *time*

undo stp [**vlan** *vlan-id-list*] **timer forward-delay**

Default

The forward delay timer is 1500 centiseconds.

Views

System view

Predefined user roles

network-admin

Parameters

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094. If you set the STP, RSTP, or MSTP forward delay, do not specify this option.

time: Specifies the forward delay in centiseconds, in the range of 400 to 3000 in increments of 100 (as in 400, 500, 600).

Usage guidelines

The forward delay timer determines the time interval of state transition. To prevent temporary loops, a spanning tree port goes through the learning (intermediate) state before it transits from the discarding state to the forwarding state. To stay synchronized with the remote device, the port has a wait period that is determined by the forward delay timer between transition states.

As a best practice, do not set the forward delay with this command. Instead, you can specify the network diameter of the switched network by using the **stp bridge-diameter** command. This command makes the spanning tree protocols automatically calculate the optimal settings for the forward delay timer. If the network diameter uses the default value, the forward delay timer also uses the default value.

Examples

In MSTP mode, set the forward delay timer to 2000 centiseconds.

```
<Switch> system-view
[Switch] stp timer forward-delay 2000
```

In PVST mode, set the forward delay timer for VLAN 2 to 2000 centiseconds.

```
<Switch> system-view
[Switch] stp vlan 2 timer forward-delay 2000
```

Related commands

stp bridge-diameter

stp timer hello

stp timer max-age

8.1.51. stp timer hello

Use **stp timer hello** to set the hello time.

Use **undo stp timer hello** to restore the default.

Syntax

stp [**vlan** *vlan-id-list*] **timer hello** *time*

undo stp [**vlan** *vlan-id-list*] **timer hello**

Default

The hello time is 200 centiseconds.

Views

System view

Predefined user roles

network-admin

Parameters

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094. If you set the STP, RSTP, or MSTP hello time, do not specify this option.

time: Specifies the hello time in centiseconds, in the range of 100 to 1000 in increments of 100 (as in 100, 200, 300).

Usage guidelines

Hello time is the interval at which spanning tree devices send configuration BPDUs to maintain the spanning tree. If a device fails to receive configuration BPDUs within the set period of time, a new spanning tree calculation process is triggered.

As a best practice, do not set the hello time with this command. Instead, you can specify the network diameter of the switched network by using the **stp bridge-diameter** command. This command makes the spanning tree protocols automatically calculate the optimal settings for the hello timer. If the network diameter uses the default value, the hello timer also uses the default value.

Examples

In MSTP mode, set the hello time to 400 centiseconds.

```
<Switch> system-view
[Switch] stp timer hello 400
```

In PVST mode, set the hello time for VLAN 2 to 400 centiseconds.

```
<Switch> system-view
[Switch] stp vlan 2 timer hello 400
```

Related commands

stp bridge-diameter

stp timer forward-delay

stp timer max-age

8.1.52. stp timer max-age

Use **stp timer max-age** to set the max age timer.

Use **undo stp timer max-age** to restore the default.

Syntax

stp [**vlan** *vlan-id-list*] **timer max-age** *time*

undo stp [**vlan** *vlan-id-list*] **timer max-age**

Default

The max age is 2000 centiseconds.

Views

System view

Predefined user roles

network-admin

Parameters

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094. If you set the STP, RSTP, or MSTP max age, do not specify this option.

time: Specifies the max age in centiseconds, in the range of 600 to 4000 in increments of 100 (as in 600, 700, 800).

Usage guidelines

In the CIST of an MSTP network, the device determines whether a configuration BPDU received on a port has expired based on the max age timer. If the configuration BPDU has expired, a new spanning tree calculation process starts. The max age timer takes effect only on the CIST (or MSTI 0).

As a best practice, do not set the max age timer with this command. Instead, you can specify the network diameter of the switched network by using the **stp bridge-diameter** command. This command makes the spanning tree protocols automatically calculate the optimal settings for the max age timer. If the network diameter uses the default value, the max age timer also uses the default value.

Examples

In MSTP mode, set the max age timer to 1000 centiseconds.

```
<Switch> system-view
[Switch] stp timer max-age 1000
```

In PVST mode, set the max age timer for VLAN 2 to 1000 centiseconds.

```
<Switch> system-view
[Switch] stp vlan 2 timer max-age 1000
```

Related commands

stp bridge-diameter

stp timer forward-delay

stp timer hello

8.1.53. stp timer-factor

Use **stp timer-factor** to configure the timeout period by setting the timeout factor.

Timeout period = timeout factor × 3 × hello time.

Use **undo stp timer-factor** to restore the default.

Syntax

stp timer-factor *factor*

undo stp timer-factor

Default

The timeout factor of the device is set to 3.

Views

System view

Predefined user roles

network-admin

Parameters

factor: Specifies the timeout factor in the range of 1 to 20.

Usage guidelines

In a stable network, each non-root-bridge forwards configuration BPDUs to surrounding devices at the interval of hello time to determine whether any link fails. If a device does not receive a BPDU from the upstream device within nine times of the hello time, it assumes that the upstream device has failed. Then it will start a new spanning tree calculation process.

As a best practice, set the timeout factor to 5, 6, or 7 in the following situations:

- To prevent undesired spanning tree calculations. An upstream device might be too busy to forward configuration BPDUs in time, for example, many Layer 2 interfaces are configured on the upstream device. In this case, the downstream device fails to receive a BPDU within the timeout period and then starts an undesired spanning tree calculation.
- To save network resources on a stable network.

Examples

Set the timeout factor of the device to 7.

```
<Switch> system-view
[Switch] stp timer-factor 7
```

Related commands

stp timer hello

8.1.54. stp transmit-limit

Use **stp transmit-limit** to set the BPDU transmission rate of a port.

Use **undo stp transmit-limit** to restore the default.

Syntax

stp transmit-limit *limit*

undo stp transmit-limit

Default

The BPDU transmission rate of all ports is 10.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

limit: Specifies the BPDU transmission rate in the range of 1 to 255.

Usage guidelines

The maximum number of BPDUs a port can send within each hello time equals the BPDU transmission rate plus the hello timer value.

A larger BPDU transmission rate value requires more system resources. An appropriate BPDU transmission rate setting can prevent spanning tree protocols from using excessive bandwidth resources during network topology changes. As a best practice, use the default value.

If this command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If this command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If this command is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

Examples

Set the BPDU transmission rate of GigabitEthernet 1/0/1 to 5.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] stp transmit-limit 5
```

8.1.55. stp vlan enable

Use **stp vlan enable** to enable the spanning tree feature for VLANs.

Use **undo stp enable** to disable the spanning tree feature for VLANs.

Syntax

stp vlan *vlan-id-list* **enable**

undo stp vlan *vlan-id-list* **enable**

Default

The spanning tree feature is enabled in VLANs.

Views

System view

Predefined user roles

network-admin

Parameters

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094.

Usage guidelines

When you enable the spanning tree feature, the device operates in STP, RSTP, PVST, or MSTP mode, depending on the spanning tree mode setting.

When you enable the spanning tree feature, the device dynamically maintains the spanning tree status of VLANs, based on received configuration BPDUs. When you disable the spanning tree feature, the device stops maintaining the spanning tree status.

Examples

In PVST mode, globally enable the spanning tree feature and then enable the spanning tree feature for VLAN 2.

```
<Switch> system-view
[Switch] stp mode pvst
[Switch] stp global enable
[Switch] stp vlan 2 enable
```

Related commands

stp enable

stp global enable

stp mode

8.1.56. vlan-mapping modulo

Use **vlan-mapping modulo** to map VLANs in an MST region to MSTIs according to the specified modulo value and quickly create a VLAN-to-instance mapping table.

Syntax

vlan-mapping modulo *modulo*

Default

All VLANs are mapped to the CIST (MSTI 0).

Views

MST region view

Predefined user roles

network-admin

Parameters

modulo: Specifies the modulo value. The value range for this argument is 1 to 64.

Usage guidelines

You cannot map a VLAN to different MSTIs. If you map a VLAN that has been mapped to an MSTI to a new MSTI, the old mapping is automatically deleted.

This command maps each VLAN to the MSTI with ID (VLAN ID – 1) % *modulo* + 1. (VLAN ID – 1) % *modulo* is the modulo operation for (VLAN ID – 1). If the modulo value is 15, then VLAN 1 is mapped to MSTI 1, VLAN 2 to MSTI 2, …, VLAN 15 to MSTI 15, VLAN 16 to MSTI 16, and so on.

Examples

Map VLANs to MSTIs as per modulo 8.

```
<Switch> system-view
[Switch] stp region-configuration
[Switch-mst-region] vlan-mapping modulo 8
```

Related commands

active region-configuration

check region-configuration

display stp region-configuration

region-name

revision-level

Contents

A page of this section is **3-x-x**

9. Loop detection commands 9-1
9.1. Loop detection commands 9-1
9.1.1. display loopback-detection 9-1
9.1.2. loopback-detection action 9-2
9.1.3. loopback-detection enable 9-3
9.1.4. loopback-detection global action 9-3
9.1.5. loopback-detection global enable 9-4
9.1.6. loopback-detection interval-time 9-5

9. Loop detection commands

9.1. Loop detection commands

9.1.1. display loopback-detection

Use **display loopback-detection** to display the loop detection configuration and status.

Syntax

display loopback-detection

Views

Any view

Predefined user roles

network-admin

network-operator

Example

Display the loop detection configuration and status.

```
<Switch> display loopback-detection
Loopback detection is enabled.
Loopback detection interval is 30 second(s).
Loopback is detected on following interfaces:
 Interface                Action mode     VLANs
 GigabitEthernet1/0/1     Shutdown        10
```

Table 9-1 Command output

Field	Description

Action mode	Loop protection action:
	• **Block**—When a loop is detected on a port, the device performs the following operations:
	  ○ Generates a log.
	  ○ Disables the port from learning MAC addresses.
	  ○ Blocks the port.
	• **None**—When a loop is detected on a port, the device generates a log but performs no action on the port.
	• **No-learning**—When a loop is detected on a port, the device generates a log and disables the port from learning MAC addresses.
	• **Shutdown**—When a loop is detected on a port, the device performs the following operations:
	  ○ Generates a log.
	  ○ Shuts down the port to disable the port from receiving or sending frames. The device automatically sets the port to the forwarding state after a time interval. Set the time interval by using the **shutdown-interval** command (see *Fundamentals Command Reference*).

VLANs	VLANs to which the interface belongs and where loops are detected.

9.1.2. loopback-detection action

Use **loopback-detection action** to set the loop protection action on a per-port basis.

Use **undo loopback-detection action** to restore the default.

Syntax

In Layer 2 Ethernet interface view:

loopback-detection action { **block** | **no-learning** | **shutdown** }

undo loopback-detection action

In Layer 2 aggregate interface view:

loopback-detection action shutdown

undo loopback-detection action

Default

When the device detects a loop on a port, it generates a log but performs no action on the port.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

block: Enables the block mode. If a loop is detected, the device performs the following operations:

- Generates a log.
- Disables MAC address learning.
- Blocks the port.

Layer 2 aggregate interfaces do not support this keyword.

no-learning: Enables the no-learning mode. If a loop is detected, the device generates a log and disables MAC address learning on the port. Layer 2 aggregate interfaces do not support this keyword.

shutdown: Enables the shutdown mode. If a loop is detected, the device generates a log and shuts down the port. The device automatically sets the port to the forwarding state after the time interval set by using the **shutdown-interval** command (see *Fundamentals Command Reference*).

Usage guidelines

To set the loop protection action globally, use the **loopback-detection global action** command.

The global configuration applies to all ports. The per-port configuration applies to the individual ports. The per-port configuration takes precedence over the global configuration.

Example

Set the loop protection action to **shutdown** on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] loopback-detection action shutdown
```

Related commands

display loopback-detection

loopback-detection global action

9.1.3. loopback-detection enable

Use **loopback-detection enable** to enable loop detection on a per-port basis.

Use **undo loopback-detection enable** to disable loop detection on a port.

Syntax

loopback-detection enable vlan { *vlan-id-list* | **all** }

undo loopback-detection enable vlan { *vlan-id-list* | **all** }

Default

Loop detection is disabled on ports.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

vlan-id-list: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN ID or a range of VLAN IDs in the form of *vlan-id1* to *vlan-id2*. The value range for VLAN IDs is 1 to 4094. The ID for *vlan-id2* must be no less than the ID for *vlan-id1*.

all: Specifies all existing VLANs.

Usage guidelines

You can enable loop detection globally or on a per-port basis. When a port receives a detection frame in any VLAN, the loop protection action is triggered on that port, regardless of whether loop detection is enabled on it.

Example

Enable loop detection on GigabitEthernet 1/0/1 for VLAN 10 through VLAN 20.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] loopback-detection enable vlan 10 to 20
```

Related commands

display loopback-detection

loopback-detection global enable

9.1.4. loopback-detection global action

Use **loopback-detection global action** to set the global loop protection action.

Use **undo loopback-detection global action** to restore the default.

Syntax

loopback-detection global action shutdown

undo loopback-detection global action

Default

When the device detects a loop on a port, it generates a log but performs no action on the port.

Views

System view

Predefined user roles

network-admin

Parameters

shutdown: Enables the shutdown mode. If a loop is detected, the device generates a log and shuts down the port. The device automatically sets the port to the forwarding state after you set the time interval by using the **shutdown-interval** command (see *Fundamentals Command Reference*).

Usage guidelines

To set the loop protection action on a per-port basis, use the **loopback-detection action** command in interface view.

The global configuration applies to all ports. The per-port configuration applies to the individual ports. The per-port configuration takes precedence over the global configuration.

Example

Set the global loop protection action to **shutdown**.

```
<Switch> system-view
[Switch] loopback-detection global action shutdown
```

Related commands

display loopback-detection

loopback-detection action

9.1.5. loopback-detection global enable

Use **loopback-detection global enable** to enable loop detection globally.

Use **undo loopback-detection global enable** to disable loop detection globally.

Syntax

loopback-detection global enable vlan { *vlan-id-list* | **all** }

undo loopback-detection global enable vlan { *vlan-id-list* | **all** }

Default

Loop detection is globally enabled.

Views

System view

Predefined user roles

network-admin

Parameters

vlan-id-list: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN ID or a range of VLAN IDs in the form of *vlan-id1* to *vlan-id2*. The value range for VLAN IDs is 1 to 4094. The ID for *vlan-id2* must be equal to or greater than the ID for *vlan-id1*.

all: Specifies all existing VLANs.

Usage guidelines

You can enable loop detection globally or on a per-port basis. When a port receives a detection frame in any VLAN, the loop protection action is triggered on that port, regardless of whether loop detection is enabled on it.

Example

Globally enable loop detection for VLAN 10 through VLAN 20.

```
<Switch> system-view
[Switch] loopback-detection global enable vlan 10 to 20
```

Related commands

display loopback-detection

loopback-detection enable

9.1.6. loopback-detection interval-time

Use **loopback-detection interval-time** to set the loop detection interval.

Use **undo loopback-detection interval-time** to restore the default.

Syntax

loopback-detection interval-time *interval*

undo loopback-detection interval-time

Default

The loop detection interval is 5 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Sets the loop detection interval in the range of 1 to 300 seconds.

Usage guidelines

With loop detection enabled, the device sends loop detection frames at the specified interval. A shorter interval offers more sensitive detection but consumes more resources. Consider the system performance and loop detection speed when you set the loop detection interval.

Using **undo loopback-detection interval-time** cannot restore the default. You must use the **loopback-detection interval-time 5** command to reconfigure the interval-time.

Example

Set the loop detection interval to 10 seconds.

```
<Switch> system-view
```

```
[Switch] loopback-detection interval-time 10
```

Related commands

display loopback-detection

Contents

A page of this section is **3-x-x**

10. VLAN commands 10-1
10.1. Basic VLAN commands 10-1
10.1.1. description 10-1
10.1.2. display interface vlan-interface 10-2
10.1.3. display vlan 10-4
10.1.4. display vlan brief 10-5
10.1.5. interface vlan-interface 10-6
10.1.6. mac-address 10-7
10.1.7. name 10-8
10.1.8. reset counters interface vlan-interface 10-8
10.1.9. shutdown 10-9
10.1.10. vlan 10-10
10.2. Port-based VLAN commands 10-11
10.2.1. display port 10-11
10.2.2. port 10-12
10.2.3. port access vlan 10-12
10.2.4. port hybrid pvid 10-13
10.2.5. port hybrid vlan 10-14
10.2.6. port link-type 10-15
10.2.7. port trunk permit vlan 10-15
10.2.8. port trunk pvid 10-16
10.3. MAC-based VLAN commands 10-17
10.3.1. display mac-vlan 10-17
10.3.2. display mac-vlan interface 10-19
10.3.3. mac-vlan enable 10-19
10.3.4. mac-vlan mac-address 10-20
10.3.5. mac-vlan trigger enable 10-21
10.3.6. port pvid forbidden 10-21
10.3.7. vlan precedence 10-22
10.4. IP subnet-based VLAN commands 10-23
10.4.1. display ip-subnet-vlan interface 10-23
10.4.2. display ip-subnet-vlan vlan 10-24
10.4.3. ip-subnet-vlan 10-25
10.4.4. port hybrid ip-subnet-vlan 10-26
10.5. Protocol-based VLAN commands 10-27
10.5.1. display protocol-vlan interface 10-27
10.5.2. display protocol-vlan vlan 10-28
10.5.3. port hybrid protocol-vlan 10-29
10.5.4. protocol-vlan 10-30

10. VLAN commands

10.1. Basic VLAN commands

10.1.1. description

Use **description** to configure the description of a VLAN or VLAN interface.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

For a VLAN, the description is **VLAN** *vlan-id*. The *vlan-id* argument specifies the VLAN ID in a four-digit format. If the VLAN ID has fewer than four digits, leading zeros are added. For example, the default description of VLAN 100 is **VLAN 0100**.

For a VLAN interface, the description is the name of the interface. For example, **Vlan-interface1 Interface**.

Views

VLAN view

VLAN interface view

Predefined user roles

network-admin

Parameters

text: Specifies a description, a case-sensitive string of 1 to 255 characters.

Usage guidelines

To manage VLANs and VLAN interfaces efficiently, configure descriptions for them based on their functions or connections.

Examples

Configure the description of VLAN 2 as **sales-private**.

```
<Switch> system-view
[Switch] vlan 2
[Switch-vlan2] description sales-private
```

Configure the description of VLAN-interface 2 as **linktoPC56**.

```
<Switch> system-view
[Switch] vlan 2
[Switch-vlan2] quit
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] description linktoPC56
```

Related commands

display interface vlan-interface

display vlan

10.1.2. display interface vlan-interface

Use **display interface vlan-interface** to display VLAN interface information.

Syntax

display interface vlan-interface [*interface-number*] [**brief** [**description** | **down**]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vlan-interface *interface-number*: Specifies a VLAN interface number. If you do not specify this argument, the command displays information about all VLAN interfaces.

brief: Displays brief interface information. If you do not specify this keyword, the command displays detailed interface information.

description: Displays complete interface descriptions. If you do not specify this keyword, the command displays only the first 27 characters of each interface description.

down: Displays VLAN interfaces in down state and their down causes. If you do not specify this keyword, the command displays information about VLAN interfaces in all states.

Examples

Display information about VLAN-interface 10.

```
<Switch> display interface vlan-interface 10
Vlan-interface10
Current state: UP
Line protocol state: UP
Description: Vlan-interface10 Interface
Bandwidth: 100000 kbps
Maximum transmission unit: 1500
Internet Address is 192.168.1.54/24 Primary
IP packet frame type: Ethernet II, hardware address: 0023-89b6-d613
IPv6 packet frame type: Ethernet II, hardware address: 0023-89b6-d613
Last clearing of counters: Never
```

Display brief information about VLAN-interface 2.

```
<Switch> display interface vlan-interface 2 brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Primary IP         Description
Vlan2                DOWN DOWN     --
```

Table 10-1 Command output

Field	Description
Vlan-interface2	VLAN interface name.
Current state	Physical link state of the VLAN interface: • **Administratively DOWN**—The interface has been shut down by using the **shutdown** command. • **DOWN**—The interface is administratively up, but its physical state is down. The VLAN of this VLAN interface does not contain any physical ports in up state. The ports might not be connected correctly or the links might have failed. • **UP**—The interface is both administratively and physically up.
Line protocol state	Data link layer state of the VLAN interface: • **DOWN**—The link layer protocol state of the interface is down. • **UP**—The link layer protocol state of the interface is up.
Description	Description of the VLAN interface.
Bandwidth	Expected bandwidth of the VLAN interface.
Maximum transmission unit	MTU of the VLAN interface.
Internet protocol processing : Disabled	The VLAN interface is not assigned an IP address and cannot process IP packets.
Internet Address	IP address of the VLAN interface. The **primary** attribute indicates that the address is the primary IP address.
IP packet frame type	IPv4 packet framing format.
hardware address	MAC address of the VLAN interface.
IPv6 packet frame type	IPv6 packet framing format.
Last clearing of counters	The most recent time that the **reset counters interface vlan-interface** command was executed. This field displays **Never** if you have never executed this command.
Brief information on interfaces in route mode	Brief information about Layer 3 interfaces.
Interface	Abbreviated interface name.
Link	Physical link state of the interface: • **UP**—The interface is physically up. • **DOWN**—The interface is physically down. • **ADM**—The interface has been shut down by using the **shutdown** command. To restore the physical state of the interface, use the **undo shutdown** command. • **Stby**—The interface is a backup interface in standby state. To see the primary interface, use the **display interface-backup state** command.
Protocol	Data link layer protocol state of the interface: • **UP**—The data link layer protocol state of the

Field	Description
	interface is up. • **DOWN**—The data link layer protocol state of the interface is down. • **UP(s)**—The data link layer protocol of the interface is up, but the link is an on-demand link or does not exist. The **(s)** attribute represents the spoofing flag.
Primary IP	Primary IP address of the interface.

Related commands

reset counters interface vlan-interface

10.1.3. display vlan

Use **display vlan** to display VLAN information.

Syntax

display vlan [*vlan-id1* [**to** *vlan-id2*] | **all** | **dynamic** | **reserved** | **static**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vlan-id1: Specifies a VLAN by its ID in the range of 1 to 4094.

vlan-id1 **to** *vlan-id2*: Specifies a VLAN ID range. Both the *vlan-id1* and the *vlan-id2* arguments are in the range of 1 to 4094. The value for the *vlan-id2* argument must be equal to or greater than the value for the *vlan-id1* argument.

all: Specifies all VLANs except the reserved VLANs.

dynamic: Specifies dynamic VLANs. If you specify this keyword, the command displays the total number of dynamic VLANs and each dynamic VLAN ID. Dynamic VLANs are generated through MVRP or assigned by a RADIUS server.

reserved: Specifies reserved VLANs. Protocol modules determine which VLANs are reserved according to function implementation. The reserved VLANs provide services for protocol modules. You cannot configure reserved VLANs.

static: Specifies static VLANs. If you specify this keyword, the command displays the total number of static VLANs and each static VLAN ID. Static VLANs are manually created.

Examples

Display information about VLAN 2.

```
<Switch> display vlan 2
 VLAN ID: 2
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0002
 Name: VLAN 0002
```

```
 Tagged ports:   None
 Untagged ports:
    GigabitEthernet1/0/1  GigabitEthernet1/0/2  GigabitEthernet1/0/3
```

Display information about VLAN 3.

```
<Switch> display vlan 3
 VLAN ID: 3
 VLAN type: static
 Route interface: Configured
 IPv4 address: 1.1.1.1
 IPv4 subnet mask: 255.255.255.0
 Description: VLAN 0003
 Name: VLAN 0003
 Tagged ports:   None
 Untagged ports: None
```

Table 10-2 Command output

Field	Description
VLAN type	VLAN type, static or dynamic.
Route interface	Whether the VLAN interface is configured for the VLAN. • Not configured. • Configured.
Description	Description of the VLAN.
Name	VLAN name.
IP address	Primary IPv4 address of the VLAN interface. This field is displayed only when an IPv4 address is configured for the VLAN interface. When the VLAN interface is also configured with secondary IPv4 addresses, you can view them by using one of the following commands: • **display interface vlan-interface**. • **display this** (VLAN interface view).
Subnet mask	Subnet mask of the primary IP address. This field is available only when an IP address is configured for the VLAN interface.
Tagged ports	Tagged members of the VLAN.
Untagged ports	Untagged members of the VLAN.

Related commands

vlan

10.1.4. display vlan brief

Use **display vlan brief** to display brief VLAN information.

Syntax

display vlan brief

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display brief VLAN information.

```
<Switch> display vlan brief
Brief information about all VLANs:
Supported Minimum VLAN ID: 1
Supported Maximum VLAN ID: 4094
Default VLAN ID: 1
VLAN ID   Name                                Port
1         VLAN 0001                           GE1/0/1  GE1/0/2  GE1/0/3  GE1/0/4
                                              GE1/0/5  GE1/0/6  GE1/0/7  GE1/0/8
                                              GE1/0/9  GE1/0/10  GE1/0/11
                                              GE1/0/12  GE1/0/13  GE1/0/14
                                              GE1/0/15  GE1/0/16  GE1/0/17
                                              GE1/0/18  GE1/0/19  GE1/0/20
                                              GE1/0/21  GE1/0/22  GE1/0/23
                                              GE1/0/24  GE1/0/25  GE1/0/26
                                              GE1/0/27  GE1/0/28  GE1/0/29
                                              GE1/0/30  GE1/0/31  GE1/0/32
                                              GE1/0/33  GE1/0/34  GE1/0/35
                                              GE1/0/36  GE1/0/37  GE1/0/38
                                              GE1/0/39  GE1/0/40  GE1/0/41
                                              GE1/0/42  GE1/0/43  GE1/0/44
                                              GE1/0/45  GE1/0/46  GE1/0/47
                                              GE1/0/48
2         VLAN 0002
3         VLAN 0003
```

Table 10-3 Command output

Field	Description
Default VLAN ID	System default VLAN ID.
Name	VLAN name.
Port	Ports that allow packets from the VLAN to pass through.

10.1.5. interface vlan-interface

Use **interface vlan-interface** to create a VLAN interface and enter its view, or enter the view of an existing VLAN interface.

Use **undo interface vlan-interface** to delete a VLAN interface.

Syntax

interface vlan-interface *interface-number*

undo interface vlan-interface *interface-number*

Default

No VLAN interfaces exist.

Views

System view

Predefined user roles

network-admin

Parameters

interface-number: Specifies a VLAN interface number in the range of 1 to 4094.

Usage guidelines

Create the VLAN before you create the VLAN interface for a VLAN.

You cannot create VLAN interfaces for sub-VLANs.

You cannot create VLAN interfaces for secondary VLANs that meet the following requirements:

- Associated with the same primary VLAN.
- Enabled with Layer 3 communication in VLAN interface view of the primary VLAN interface.

Examples

Create VLAN-interface 2, and enter its view.

```
<Switch> system-view
[Switch] vlan 2
[Switch-vlan2] quit
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2]
```

Related commands

display interface vlan-interface

10.1.6. mac-address

Use **mac-address** to assign a MAC address to a VLAN interface.

Use **undo mac-address** to restore the default.

Syntax

mac-address *mac-address*

undo mac-address

Default

No MAC address is configured for a VLAN interface.

Views

VLAN interface view

Predefined user roles

network-admin

Parameters

mac-address: Specifies a MAC address in the format of H-H-H.

Examples

Assign MAC address 0001-0001-0001 to VLAN-interface 2.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] mac-address 1-1-1
```

10.1.7. name

Use **name** to assign a name to a VLAN.

Use **undo name** to restore the default.

Syntax

name *text*

undo name

Default

The name of a VLAN is **VLAN** *vlan-id*. The *vlan-id* argument specifies the VLAN ID in a four-digit format. If the VLAN ID has fewer than four digits, leading zeros are added. For example, the name of VLAN 100 is **VLAN 0100**.

Views

VLAN view

Predefined user roles

network-admin

Parameters

text: Specifies a VLAN name, a case-sensitive string of 1 to 32 characters.

Usage guidelines

For 802.1X or MAC authentication, you can specify authorization VLANs by their names or IDs. If a large number of VLANs are configured, use VLAN names to identify them.

Examples

Assign the name **test vlan** to VLAN 2.

```
<Switch> system-view
[Switch] vlan 2
[Switch-vlan2] name test vlan
```

Related commands

display vlan

10.1.8. reset counters interface vlan-interface

Use **reset counters interface vlan-interface** to clear statistics on a VLAN interface.

Syntax

reset counters interface vlan-interface [*interface-number*]

Views

User view

Predefined user roles

network-admin

Parameters

vlan-interface *interface-number*: Specifies a VLAN interface by its number. If you do not specify the *interface-number* argument, this command clears statistics on all VLAN interfaces.

Usage guidelines

Use this command to clear the history statistics before you collect statistics within a time period.

Examples

Clear statistics on VLAN-interface 2.

```
<Switch> reset counters interface vlan-interface 2
```

Related commands

display interface vlan-interface

10.1.9. shutdown

Use **shutdown** to shut down a VLAN interface.

Use **undo shutdown** to bring up a VLAN interface.

Syntax

shutdown

undo shutdown

Default

A VLAN interface is not manually shut down, and the following guidelines apply to the interface state:

- The VLAN interface is down if all ports in the VLAN are down.
- The VLAN interface is up if one or more ports in the VLAN are up.

Views

VLAN interface view

Predefined user roles

network-admin

Usage guidelines

When you use this command to shut down a VLAN interface, the VLAN interface remains in DOWN (Administratively) state. In this case, the VLAN interface state is not affected by the state of the ports in the VLAN.

Before you configure parameters for a VLAN interface, use this command to shut it down to prevent the configuration from affecting the network. After you complete the VLAN interface configuration, use the **undo shutdown** command to make the settings take effect.

To troubleshoot a failed VLAN interface, you can use the **shutdown** command and then the **undo shutdown** command on the interface to see whether it recovers.

In a VLAN, the state of each Ethernet port is independent of the state of the VLAN interface.

Examples

Shut down VLAN-interface 2, and then bring it up.

```
<Switch> system-view
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] shutdown
[Switch-Vlan-interface2] undo shutdown
```

10.1.10. vlan

Use **vlan** *vlan-id-list* to create VLANs in batches, except reserved VLANs.

Use **vlan all** to create VLANs 1 through 4094.

Use **undo vlan** to delete the specified VLANs.

Syntax

vlan { *vlan-id-list* | **all** }

undo vlan { *vlan-id-list* | **all** }

Default

VLAN 1 (system default VLAN) exists.

Views

System view

Predefined user roles

network-admin

Parameters

vlan-id-list: Specifies a space-separated list of up to 32 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094.

all: Specifies all VLANs except reserved VLANs. The keyword is not supported when the maximum number of VLANs that can be created on a device is less than 4094.

Usage guidelines

You cannot create or delete the system default VLAN (VLAN 1) or reserved VLANs.

Before you delete a dynamic VLAN or a VLAN locked by an application, you must first remove the configuration from the VLAN.

Examples

Create VLAN 2 and enter its view.

```
<Switch> system-view
[Switch] vlan 2
[Switch-vlan2]
```

Create VLAN 2 and VLANs 4 through 100.

```
<Switch> system-view
```

```
[Switch] vlan 2 4 to 100
```

Related commands

display vlan

10.2. Port-based VLAN commands

10.2.1. display port

Use **display port** to display information about hybrid or trunk ports.

Syntax

display port { **hybrid** | **trunk** }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

hybrid: Specifies hybrid ports.

trunk: Specifies trunk ports.

Examples

Display information about hybrid ports.

```
<Switch> display port hybrid
Interface            PVID  VLAN Passing
GE1/0/1              100   Tagged:  1000, 1002, 1500, 1600-1611, 2000,
                                    2555-2558, 3000, 4000
                           Untagged:1, 10, 15, 18, 20-30, 44, 55, 67, 100,
                                    150-160, 200, 255, 286, 300-302
```

Display information about trunk ports.

```
<Switch> display port trunk
Interface            PVID  VLAN Passing
GE1/0/2              2     1-4, 6-100, 145, 177, 189-200, 244, 289, 400,
                           555, 600-611, 1000, 2006-2008
```

Table 10-4 Command output

Field	Description
Interface	Interface name.
PVID	Port VLAN ID.
VLAN Passing	Existing VLANs allowed on the port.
Tagged	VLANs from which the port sends packets without removing VLAN tags.
Untagged	VLANs from which the port sends packets after removing VLAN tags.

10.2.2. port

Use **port** to assign the specified access ports to a VLAN.

Use **undo port** to remove the specified access ports from a VLAN.

Syntax

port *interface-list*

undo port *interface-list*

Default

All ports are in VLAN 1.

Views

VLAN view

Predefined user roles

network-admin

Parameters

interface-list: Specifies a space-separated list of up to 10 Ethernet interface items. Each item specifies an Ethernet interface or a range of Ethernet interfaces in the form of *interface-type interface-number1* **to** *interface-type interface-number2*. The value for the *interface-number2* argument must be equal to or greater than the value for the *interface-number1* argument.

Usage guidelines

This command is applicable only to access ports.

By default, all ports are access ports. You can manually configure the port link type. For more information, see "port link-type."

Examples

Assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 to VLAN 2.

```
<Switch> system-view
[Switch] vlan 2
[Switch-vlan2] port gigabitethernet 1/0/1 to gigabitethernet 1/0/3
```

Related commands

display vlan

10.2.3. port access vlan

Use **port access vlan** to assign an access port to the specified VLAN.

Use **undo port access vlan** to restore the default.

Syntax

port access vlan *vlan-id*

undo port access vlan

Default

All access ports belong to VLAN 1.

Views

Layer 2 aggregate interface view

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

vlan-id: Specifies a VLAN by its ID in the range of 1 to 4094.

Usage guidelines

Before assigning an access port to a VLAN, make sure the VLAN has been created.

Examples

Assign GigabitEthernet 1/0/1 to VLAN 3.

```
<Switch> system-view
[Switch] vlan 3
[Switch-vlan3] quit
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port access vlan 3
```

10.2.4. port hybrid pvid

Use **port hybrid pvid** to set the PVID of a hybrid port.

Use **undo port hybrid pvid** to set the PVID of a hybrid port to 1.

Syntax

port hybrid pvid vlan *vlan-id*

undo port hybrid pvid

Default

The PVID of a hybrid port is the ID of the VLAN to which the port belongs when its link type is **access**.

Views

Layer 2 aggregate interface view

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

vlan-id: Specifies a VLAN by its ID in the range of 1 to 4094.

Usage guidelines

You can use a nonexistent VLAN as the PVID of a hybrid port. When you delete the PVID of a hybrid port by using the **undo vlan** command, the PVID setting of the port does not change.

For correct packet transmission, set the same PVID for a local hybrid port and its peer.

To enable a hybrid port to transmit packets from its PVID, you must assign the hybrid port to the PVID by using the **port hybrid vlan** command.

Examples

Configure GigabitEthernet 1/0/1 as a hybrid port, set its PVID to VLAN 100, and assign it to VLAN 100 as an untagged member.

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type hybrid
[Switch-GigabitEthernet1/0/1] port hybrid pvid vlan 100
[Switch-GigabitEthernet1/0/1] port hybrid vlan 100 untagged
```

Related commands

port hybrid vlan

port link-type

10.2.5. port hybrid vlan

Use **port hybrid vlan** to assign a hybrid port to the specified VLANs.

Use **undo port hybrid vlan** to remove a hybrid port from the specified VLANs.

Syntax

port hybrid vlan *vlan-id-list* { **tagged** | **untagged** }

undo port hybrid vlan *vlan-id-list*

Default

A hybrid port is an untagged member of the VLAN to which the port belongs when its link type is **access**.

Views

Layer 2 aggregate interface view

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

vlan-id-list: Specifies a space-separated list of up to 32 VLAN items. Each item specifies a VLAN ID or a range of VLAN IDs in the form of *vlan-id1* **to** *vlan-id2*. The value range for VLAN IDs is 1 to 4094. The value for the *vlan-id2* argument must be equal to or greater than the value for the *vlan-id1* argument. The specified VLANs must already exist on the device.

tagged: Configures the port as a tagged member of the specified VLANs. A tagged member of a VLAN sends packets from the VLAN without removing VLAN tags.

untagged: Configures the port as an untagged member of the specified VLANs. An untagged member of a VLAN sends packets from the VLAN after removing VLAN tags.

Usage guidelines

A hybrid port can allow multiple VLANs. If you execute this command multiple times on a hybrid port, the hybrid port allows all the specified VLANs.

Examples

Configure GigabitEthernet 1/0/1 as a hybrid port, and assign it to VLAN 2, VLAN 4, and VLAN 50 through VLAN 100 as a tagged member.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type hybrid
[Switch-GigabitEthernet1/0/1] port hybrid vlan 2 4 50 to 100 tagged
```

Related commands

port link-type

10.2.6. port link-type

Use **port link-type** to set the link type of a port.

Use **undo port link-type** to restore the default link type of a port.

Syntax

port link-type { **access** | **hybrid** | **trunk** }

undo port link-type

Default

Each port is an access port.

Views

Layer 2 aggregate interface view

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

access: Sets the port link type to access.

hybrid: Sets the port link type to hybrid.

trunk: Sets the port link type to trunk.

Usage guidelines

To change the link type of a port from trunk to hybrid or vice versa, first set the link type to access.

Examples

Configure GigabitEthernet 1/0/1 as a trunk port.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
```

10.2.7. port trunk permit vlan

Use **port trunk permit vlan** to assign a trunk port to the specified VLANs.

Use **undo port trunk permit vlan** to remove a trunk port from the specified VLANs.

Syntax

port trunk permit vlan { *vlan-id-list* | **all** }

undo port trunk permit vlan { *vlan-id-list* | **all** }

Default

A trunk port allows packets only from VLAN 1 to pass through.

Views

Layer 2 aggregate interface view

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

vlan-id-list: Specifies a space-separated list of up to 32 VLAN items. Each item specifies a VLAN ID or a range of VLAN IDs in the form of *vlan-id1* **to** *vlan-id2*. The value range for VLAN IDs is 1 to 4094. The value for the *vlan-id2* argument must be equal to or greater than the value for the *vlan-id1* argument.

all: Specifies all VLANs. To prevent unauthorized VLAN users from accessing restricted resources through the port, use the **port trunk permit vlan all** command with caution.

Usage guidelines

A trunk port can allow multiple VLANs. If you execute this command multiple times on a trunk port, the trunk port allows all the specified VLANs.

On a trunk port, packets only from the PVID can pass through untagged.

Examples

Configure GigabitEthernet 1/0/1 as a trunk port, and assign it to VLAN 2, VLAN 4, and VLAN 50 through VLAN 100.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 2 4 50 to 100
```

Related commands

port link-type

10.2.8. port trunk pvid

Use **port trunk pvid** to set the PVID for a trunk port.

Use **undo port trunk pvid** to restore the default.

Syntax

port trunk pvid vlan *vlan-id*

undo port trunk pvid

Default

The PVID of a trunk port is VLAN 1.

Views

Layer 2 aggregate interface view

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

vlan-id: Specifies a VLAN by its ID in the range of 1 to 4094.

Usage guidelines

You can use a nonexistent VLAN as the PVID for a trunk port. When you delete the PVID of a trunk port by using the **undo vlan** command, the PVID setting of the port does not change.

For correct packet transmission, set the same PVID for a local trunk port and its peer.

To enable a trunk port to transmit packets from its PVID, you must assign the trunk port to the PVID by using the **port trunk permit vlan** command.

Examples

Configure GigabitEthernet 1/0/1 as a trunk, set its PVID to VLAN 100, and assign it to VLAN 100.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100
```

Related commands

port link-type

port trunk permit vlan

10.3. MAC-based VLAN commands

IMPORTANT:
Do not configure MAC-based VLANs together with mapping an Ethernet service instance to a VSI on a Layer 2 Ethernet interface or Layer 2 aggregate interface. Do not configure MAC-based VLANs on a Layer 2 Ethernet interface or Layer 2 aggregate interface that acts as the source interface of a VXLAN tunnel. For information about VXLAN and VSIs, see *VXLAN Configuration Guide*.

10.3.1. display mac-vlan

Use **display mac-vlan** to display MAC-to-VLAN entries.

Syntax

display mac-vlan { **all** | **dynamic** | **mac-address** *mac-address* [**mask** *mac-mask*] | **static** | **vlan** *vlan-id* }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

all: Specifies all MAC-to-VLAN entries.

dynamic: Specifies dynamically configured MAC-to-VLAN entries.

mac-address *mac-address*: Specifies the MAC address in the MAC-to-VLAN entry. The format of the *mac-address* argument is H-H-H.

mask *mac-mask*: Specifies the mask for matching MAC addresses in MAC-to-VLAN entries. For the *mac-mask* argument, the high-order bits must be consecutive 1s in binary notation or consecutive Fs in hexadecimal notation. The default value is ffff-ffff-ffff.

static: Specifies statically configured MAC-to-VLAN entries.

vlan *vlan-id*: Specifies the VLAN in MAC-to-VLAN entries. The value range for the *vlan-id* argument is 1 to 4094.

Examples

Display all MAC-to-VLAN entries.

```
<Switch> display mac-vlan all
The following MAC VLAN entries exist:
State: S - Static, D - Dynamic

MAC address         Mask                VLAN ID   Dot1q      State
0008-0001-0000      ffff-ff00-0000      5         3          S
0002-0001-0000      ffff-ffff-ffff      5         3          S&D

Total MAC VLAN entries count: 2
```

Table 10-5 Command output

Field	Description
S - Static	Statically configured MAC-to-VLAN entries.
D - Dynamic	Dynamically configured MAC-to-VLAN entries.
MAC address	MAC address of the MAC-to-VLAN entry.
Mask	MAC address mask of the MAC-to-VLAN entry.
VLAN ID	VLAN ID of the MAC-to-VLAN entry.
Dot1q	802.1p priority of the VLAN in the MAC-to-VLAN entry.
State	State of a MAC-to-VLAN entry: • **S**—The MAC-to-VLAN entry is configured statically. • **D**—The MAC-to-VLAN entry is dynamically issued by the authentication server. • **S&D**—The MAC-to-VLAN entry is configured both statically and dynamically.

Related commands

mac-vlan mac-address

10.3.2. display mac-vlan interface

Use **display mac-vlan interface** to display all ports that are enabled with the MAC-based VLAN feature.

Syntax

display mac-vlan interface

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display all ports that are enabled with the MAC-based VLAN feature.

```
<Switch> display mac-vlan interface
MAC VLAN is enabled on following ports:
GigabitEthernet1/0/1  GigabitEthernet1/0/2  GigabitEthernet1/0/3
```

Related commands

mac-vlan enable

10.3.3. mac-vlan enable

Use **mac-vlan enable** to enable the MAC-based VLAN feature on a port.

Use **undo mac-vlan enable** to disable the MAC-based VLAN feature on a port.

Syntax

mac-vlan enable

undo mac-vlan enable

Default

The MAC-based VLAN feature is disabled on a port.

Views

Layer 2 aggregate interface view

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Examples

Enable the MAC-based VLAN feature on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] mac-vlan enable
```

Related commands

display mac-vlan interface

10.3.4. mac-vlan mac-address

Use **mac-vlan mac-address** to configure a MAC-to-VLAN entry.

Use **undo mac-vlan** to delete the specified MAC-to-VLAN entries.

Syntax

mac-vlan mac-address *mac-address* [**mask** *mac-mask*] **vlan** *vlan-id* [**dot1q** *priority*]

undo mac-vlan { **all** | **mac-address** *mac-address* [**mask** *mac-mask*] | **vlan** *vlan-id* }

Default

No MAC-to-VLAN entries exist.

Views

System view

Predefined user roles

network-admin

Parameters

mac-address *mac-address*: Specifies a MAC address in the format of H-H-H. The MAC address cannot be a multicast MAC address or all 0s. When you configure a MAC address, leading zeros in each H section can be omitted. For example, to configure a MAC address 000f-00e2-0001, you can enter only **f-e2-1**.

mask *mac-mask*: Specifies the MAC address mask. For the *mac-mask* argument, the high-order bits must be consecutive 1s in binary notation or consecutive Fs in hexadecimal notation. The default value is ffff-ffff-ffff.

vlan *vlan-id*: Specifies a VLAN ID in the range of 1 to 4094.

dot1q *priority*: Specifies the 802.1p priority of the VLAN specific to the MAC-to-VLAN entry. The value range for the *priority* argument is 0 to 7, and the default value is 0. The higher the value, the higher the 802.1p priority.

all: Specifies all static MAC-to-VLAN entries.

Usage guidelines

For successful dynamic MAC-based VLAN assignment, use static VLANs when you create MAC-to-VLAN entries.

Different types of MAC-to-VLAN entries are created depending on whether you specify the **mask** keyword.

- When you specify this keyword, the created MAC-to-VLAN entry describes the relationship among a group of MAC addresses, a VLAN, and the 802.1p priority for the VLAN.
- When you do not specify this keyword, the created MAC-to-VLAN entry describes the relationship among a MAC address, a VLAN, and the 802.1p priority for the VLAN.

These different types of MAC-to-VLAN entries are stored separately in two tables. The system updates the two tables according to the configuration.

Examples

Associate the MAC address 0000-0001-0001 with VLAN 100, and set the 802.1p priority to 7 for VLAN 100 in this entry.

```
<Switch> system-view
```

```
[Switch] mac-vlan mac-address 0-1-1 vlan 100 dot1q 7
```

Associate VLAN 100 with MAC addresses whose six high-order bits are 121122, and set the 802.1p priority to 4 for VLAN 100 in this entry.

```
<Switch> system-view
[Switch] mac-vlan mac-address 1211-2222-3333 mask ffff-ff00-0000 vlan 100 dot1q 4
```

Related commands

display mac-vlan

10.3.5. mac-vlan trigger enable

Use **mac-vlan trigger enable** to enable dynamic MAC-based VLAN assignment on a port.

Use **undo mac-vlan trigger enable** to disable dynamic MAC-based VLAN assignment on a port.

Syntax

mac-vlan trigger enable

undo mac-vlan trigger enable

Default

Dynamic MAC-based VLAN assignment is disabled on a port.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

VLAN assignment for a port is triggered only when the source MAC address of its received packet exactly matches the MAC address in a MAC-to-VLAN entry.

Examples

Enable dynamic MAC-based VLAN assignment on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] mac-vlan trigger enable
```

Related commands

mac-vlan mac-address

port pvid forbidden

10.3.6. port pvid forbidden

Use **port pvid forbidden** to disable a port from forwarding packets that fail the exact MAC address match in its PVID.

Use **undo port pvid forbidden** to restore the default.

Syntax

port pvid forbidden

undo port pvid forbidden

Default

When a port receives packets whose source MAC addresses fail the exact MAC address match, the port forwards them in its PVID.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

Use this feature only with dynamic MAC-based VLAN assignment.

Examples

Disable GigabitEthernet 1/0/1 from forwarding packets that fail the exact MAC address match in its PVID.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port pvid forbidden
```

Related commands

mac-vlan trigger enable

10.3.7. vlan precedence

Use **vlan precedence** to set the VLAN matching order.

Use **undo vlan precedence** to restore the default.

Syntax

vlan precedence { **mac-vlan** | **ip-subnet-vlan** }

undo vlan precedence

Default

A port matches VLANs based on MAC addresses preferentially.

Views

Layer 2 aggregate interface view

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

mac-vlan: Matches VLANs based on MAC addresses preferentially.

ip-subnet-vlan: Matches VLANs based on IP subnets preferentially.

Usage guidelines

This command takes effect only on MAC-based VLANs and IP subnet-based VLANs.

When you enable dynamic MAC-based VLAN assignment, configure the **vlan precedence mac-vlan** command as a best practice to ensure the priority of MAC-based VLAN matching. If you execute the **vlan precedence ip-subnet-vlan** command, the command does not take effect.

Examples

Configure GigabitEthernet 1/0/1 to match VLANs based on MAC addresses preferentially.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] vlan precedence mac-vlan
```

Related commands

mac-vlan trigger enable

10.4. IP subnet-based VLAN commands

10.4.1. display ip-subnet-vlan interface

Use **display ip-subnet-vlan interface** to display IP subnet-based VLANs that are associated with the specified ports.

Syntax

display ip-subnet-vlan interface { *interface-type interface-number1* [**to** *interface-type interface-number2*] | **all** }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number1 **to** *interface-type interface-number2*: Specifies an interface range. Both the *interface-type interface-number1* argument and the *interface-type interface-number2* argument represent the interface type and interface number. The value for the *interface-number2* argument must be greater than or equal to the value for the *interface-number1* argument.

all: Specifies all ports.

Examples

Display IP subnet-based VLANs on GigabitEthernet 1/0/1.

```
<Switch> display ip-subnet-vlan interface gigabitethernet 1/0/1
 Interface: GigabitEthernet1/0/1
  VLAN ID   Subnet index    IP address       Subnet mask       Status
  3         0               192.168.1.0      255.255.255.0     Active
  4         N/A             N/A              N/A               Inactive
  4094      65535           172.16.1.1       255.255.0.0       Inactive
```

Table 10-6 Command output

Field	Description
VLAN ID	ID of the IP subnet-based VLAN.
Subnet index	Index of the IP subnet. This field displays **N/A** if no IP subnet-based VLAN is configured.
IP address	IP address of the subnet. It can be an IP address or a subnet address. This field displays **N/A** if no IP subnet address is configured for the VLAN.
Subnet mask	Mask of the IP subnet. This field displays **N/A** if no subnet mask is configured for the VLAN.
Status	Whether the IP subnet-based VLAN has taken effect on the port: • **Active**—The IP subnet-based VLAN has taken effect. • **Inactive**—The IP subnet-based VLAN has not taken effect. For example, this field displays **Inactive** in one of the following conditions: o The configuration of the IP subnet-based VLAN is not complete. o The port does not allow the IP subnet-based VLAN.

Related commands

display ip-subnet-vlan vlan

ip-subnet-vlan

port hybrid ip-subnet-vlan

10.4.2. display ip-subnet-vlan vlan

Use **display ip-subnet-vlan vlan** to display information about IP subnet-based VLANs.

Syntax

display ip-subnet-vlan vlan { *vlan-id1* [**to** *vlan-id2*] | **all** }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vlan-id1: Specifies an IP subnet-based VLAN by its VLAN ID in the range of 1 to 4094.

vlan-id1 **to** *vlan-id2*: Specifies an IP subnet-based VLAN ID range. Both the *vlan-id1* and the *vlan-id2* arguments are in the range of 1 to 4094. The value for the *vlan-id2* argument must be equal to or greater than the value for the *vlan-id1* argument.

all: Specifies all IP subnet-based VLANs.

Examples

Display information about all IP subnet-based VLANs.

```
<Switch> display ip-subnet-vlan vlan all
```

```
VLAN ID: 3
 Subnet index       IP address       Subnet mask
 0                  192.168.1.0      255.255.255.0
```

Table 10-7 Command output

Field	Description
VLAN ID	ID of the IP subnet-based VLAN.
Subnet index	Index of the IP subnet.
IP address	IP address of the subnet. It can be an IP address or a subnet address.
Subnet mask	Mask of the IP subnet.

Related commands

display ip-subnet-vlan interface

ip-subnet-vlan

port hybrid ip-subnet-vlan

10.4.3. ip-subnet-vlan

Use **ip-subnet-vlan** to associate a VLAN with the specified IP subnet or IP address.

Use **undo ip-subnet-vlan** to disassociate a VLAN from the specified IP subnet or IP address.

Syntax

ip-subnet-vlan [*ip-subnet-index*] **ip** *ip-address* [*mask*]

undo ip-subnet-vlan { *ip-subnet-index* [**to** *ip-subnet-end*] | **all** }

Default

A VLAN is not associated with an IP subnet or IP address.

Views

VLAN view

Predefined user roles

network-admin

Parameters

ip-subnet-index: Specifies a beginning IP subnet index in the range of 0 to 65535. The value can be configured by users. It can also be automatically numbered by the system based on the order in which the IP subnets or IP addresses are associated with the VLAN.

ip *ip-address* [*mask*]: Specifies the source IP address or network address that is associated with the VLAN. The *ip-address* argument specifies the source IP address or network address in dotted decimal notation. The *mask* argument is the subnet mask of the source IP address or network address, in dotted decimal notation with a default value of 255.255.255.0.

to *ip-subnet-end*: Specifies an end IP subnet index of an IP subnet index range, in the range of 0 to 65535. The value for the *ip-subnet-end* argument must be greater than or equal to the beginning IP subnet index.

all: Specifies all IP subnets or IP addresses that are associated with the VLAN.

Usage guidelines

The IP subnet or IP address cannot be a multicast network segment or a multicast address.

Examples

Configure VLAN 3 as an IP subnet-based VLAN and associate it with the subnet 192.168.1.0/24.

```
<Switch> system-view
[Switch] vlan 3
[Switch-vlan3] ip-subnet-vlan ip 192.168.1.0 255.255.255.0
```

Related commands

display ip-subnet-vlan interface

display ip-subnet-vlan vlan

port hybrid ip-subnet-vlan

10.4.4. port hybrid ip-subnet-vlan

Use **port hybrid ip-subnet-vlan** to associate a port with the specified IP subnet-based VLAN.

Use **undo port hybrid ip-subnet-vlan** to disassociate a port from the specified IP subnet-based VLAN.

Syntax

port hybrid ip-subnet-vlan vlan *vlan-id*

undo port hybrid ip-subnet-vlan { **vlan** *vlan-id* | **all** }

Default

A port is not associated with an IP subnet-based VLAN.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

vlan *vlan-id*: Specifies a VLAN by its ID in the range of 1 to 4094.

all: Specifies all VLANs.

Usage guidelines

For this command to take effect, perform the following tasks:

1. Create a VLAN and associate it with the specified IP subnet or IP address.
2. Set the port link type to hybrid.
3. Configure the port to allow the IP subnet-based VLAN to pass through.

Examples

Associate GigabitEthernet 1/0/1 with IP subnet-based VLAN 3.

```
<Switch> system-view
[Switch] vlan 3
[Switch-vlan3] ip-subnet-vlan ip 192.168.1.0 255.255.255.0
```

```
[Switch-vlan3] quit
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type hybrid
[Switch-GigabitEthernet1/0/1] port hybrid vlan 3 untagged
[Switch-GigabitEthernet1/0/1] port hybrid ip-subnet-vlan vlan 3
```

Associate Layer 2 aggregate interface Bridge-Aggregation 1 with IP subnet-based VLAN 3.

```
<Switch> system-view
[Switch] vlan 3
[Switch-vlan3] ip-subnet-vlan ip 192.168.1.0 255.255.255.0
[Switch-vlan3] quit
[Switch] interface bridge-aggregation 1
[Switch-Bridge-Aggregation1] port link-type hybrid
[Switch-Bridge-Aggregation1] port hybrid vlan 3 untagged
[Switch-Bridge-Aggregation1] port hybrid ip-subnet-vlan vlan 3
```

Related commands

display ip-subnet-vlan interface

display ip-subnet-vlan vlan

ip-subnet-vlan

10.5. Protocol-based VLAN commands

10.5.1. display protocol-vlan interface

Use **display protocol-vlan interface** to display protocol-based VLANs that are associated with the specified ports.

Syntax

display protocol-vlan interface { *interface-type interface-number1* [**to** *interface-type interface-number2*] | **all** }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number1 **to** *interface-type interface-number2*: Specifies an interface range. Both the *interface-type interface-number1* argument and the *interface-type interface-number2* argument represent the interface type and interface number. The value for the *interface-number2* argument must be greater than or equal to the value for the *interface-number1* argument.

all: Specifies all ports.

Examples

Display protocol-based VLAN information on GigabitEthernet 1/0/1.

```
<Switch> display protocol-vlan interface gigabitethernet 1/0/1
```

```
Interface: GigabitEthernet1/0/1
 VLAN ID  Protocol index  Protocol type            Status
 2        0              IPv6                    Active
 2        1              N/A                     Inactive
 4094     65535          IPv4                    Inactive
```

Table 10-8 Command output

Field	Description
VLAN ID	ID of the protocol-based VLAN.
Protocol index	Protocol template index.
Protocol type	Protocol type specified by the protocol template. This field displays **N/A** if the protocol type is not specified.
Status	Whether the protocol-based VLAN has taken effect: • **Active**—The protocol-based VLAN has taken effect. • **Inactive**—The protocol-based VLAN has not taken effect.

Related commands

display protocol-vlan vlan

port hybrid protocol-vlan

protocol-vlan

10.5.2. display protocol-vlan vlan

Use **display protocol-vlan vlan** to display information about protocol-based VLANs.

Syntax

display protocol-vlan vlan { *vlan-id1* [**to** *vlan-id2*] | **all** }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vlan-id1: Specifies a protocol-based VLAN ID in the range of 1 to 4094.

vlan-id1 **to** *vlan-id2*: Specifies a protocol-based VLAN ID range. Both the *vlan-id1* and the *vlan-id2* arguments are in the range of 1 to 4094. The value for the *vlan-id2* argument must be equal to or greater than the value for the *vlan-id1* argument.

all: Specifies all protocol-based VLANs.

Examples

Displays information about all protocol-based VLANs.

```
<Switch> display protocol-vlan vlan all
 VLAN ID: 2
  Protocol index  Protocol type
```

```
 0               IPv4
 65535           IPv6

VLAN ID: 3
 Protocol index  Protocol type
 0               IPv4
 65535           LLC DSAP 0x11 SSAP 0x22
```

Table 10-9 Command output

Field	Description
VLAN ID	ID of the protocol-based VLAN.
Protocol index	Protocol template index.
Protocol type	Protocol type or encapsulation format specified by the protocol template.

Related commands

display protocol-vlan interface

port hybrid protocol-vlan

protocol-vlan

10.5.3. port hybrid protocol-vlan

Use **port hybrid protocol-vlan** to associate a port with the specified protocol-based VLAN.

Use **undo port hybrid protocol-vlan** to disassociate a port from the specified protocol-based VLAN.

Syntax

port hybrid protocol-vlan vlan *vlan-id* { *protocol-index* [**to** *protocol-end*] | **all** }

undo hybrid protocol-vlan { **vlan** *vlan-id* { *protocol-index* [**to** *protocol-end*] | **all** } | **all** }

Default

A port is not associated with a protocol-based VLAN.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

vlan *vlan-id*: Specifies a VLAN by its ID in the range of 1 to 4094.

protocol-index: Specifies a beginning protocol template index in the range of 0 to 65535.

to *protocol-end*: Specifies an end protocol template index of a protocol template range, in the range of 0 to 65535. The value for this argument must be greater than or equal to the beginning protocol template index.

all: Specifies all protocol templates.

Usage guidelines

For this command to take effect, perform the following tasks:

1. Create a VLAN and associate it with the specified protocol templates.
2. Set the port link type to hybrid.
3. Configure the port to allow the protocol-based VLAN to pass through.

When you execute the **undo port hybrid protocol-vlan** command on a port, follow these guidelines:

- If you specify both the *vlan-id* argument and the **all** keyword, this command disassociates the port from all protocol templates of the specified VLAN.
- If you specify only the **all** keyword, this command disassociates the port from all protocol templates of all VLANs.

Examples

Configure GigabitEthernet 1/0/1 as a hybrid port, assign it to VLAN 2 as an untagged member, and associated it with protocol template 1 in VLAN 2.

```
<Switch> system-view
[Switch] vlan 2
[Switch-vlan2] protocol-vlan 1 ipv4
[Switch-vlan2] quit
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type hybrid
[Switch-GigabitEthernet1/0/1] port hybrid vlan 2 untagged
[Switch-GigabitEthernet1/0/1] port hybrid protocol-vlan vlan 2 1
```

Configure Layer 2 aggregate interface Bridge-Aggregation 1 as a hybrid port, assign it to VLAN 2 as an untagged member, and associated it with protocol template 1 in VLAN 2.

```
<Switch> system-view
[Switch] vlan 2
[Switch-vlan2] protocol-vlan 1 ipv4
[Switch-vlan2] quit
[Switch] interface bridge-aggregation 1
[Switch-Bridge-Aggregation1] port link-type hybrid
[Switch-Bridge-Aggregation1] port hybrid vlan 2 untagged
[Switch-Bridge-Aggregation1] port hybrid protocol-vlan vlan 2 1
```

10.5.4. protocol-vlan

Use **protocol-vlan** to associate a VLAN with the specified protocol template.

Use **undo protocol-vlan** to disassociate a VLAN from the specified protocol template.

Syntax

protocol-vlan [*protocol-index*] { **at** | **ipv4** | **ipv6** | **ipx** { **ethernetii** | **llc** | **raw** | **snap** } | **mode** { **ethernetii etype** *etype-id* | **llc** { **dsap** *dsap-id* [**ssap** *ssap-id*] | **ssap** *ssap-id* } | **snap etype** *etype-id* } }

undo protocol-vlan { *protocol-index* [**to** *protocol-end*] | **all** }

Default

A VLAN is not associated with a protocol template.

Views

VLAN view

Predefined user roles

network-admin

Parameters

at: Specifies the AppleTalk-based VLAN.

ipv4: Specifies the IPv4-based VLAN.

ipv6: Specifies the IPv6-based VLAN.

ipx: Specifies the IPX-based VLAN. The keywords **ethernetii**, **llc**, **raw**, and **snap** specify IPX encapsulation formats.

mode: Configures a user-defined protocol template for the VLAN. The keywords **ethernetii**, **llc**, and **snap** specify the available encapsulation formats.

ethernetii etype *etype-id*: Matches the Ethernet II encapsulation format and the specified protocol type ID. The *etype-id* argument specifies the protocol type ID of inbound packets, in the range of 600 to ffff in hexadecimal notation, excluding 800, 86dd, 809b, and 8137.

llc: Matches the LLC encapsulation format.

dsap *dsap-id*: Specifies the destination service access point in hexadecimal notation, in the range of 0 to ff.

ssap *ssap-id*: Specifies the source service access point in hexadecimal notation, in the range of 0 to ff.

snap etype *etype-id*: Matches the SNAP encapsulation format and the specified protocol type value. The *etype-id* argument specifies the Ethernet type of inbound packets, in the range of 600 to ffff in hexadecimal notation, excluding 8137.

protocol-index: Specifies a protocol template index that is associated with the VLAN. The value range for this argument is 0 to 65535. The system will automatically assign an index if you do not specify this argument.

to *protocol-end*: Specifies an end protocol template index of a protocol template range, in the range of 0 to 65535. The value for the *protocol-end* argument must be greater than or equal to the value for the *protocol-index* argument.

all: Specifies all protocols associated with the VLAN.

Usage guidelines

CAUTION:
IP uses ARP for address resolution in Ethernet. To prevent communication failures, configure the IP and ARP templates in the same VLAN and associate them with the same port.

When you use the **mode** keyword to configure a protocol template, follow these restrictions and guidelines:

- Do not set the *etype-id* argument in the **ethernetii etype** *etype-id* option to the following hexadecimal values:
  - **800**—Specifies the IPv4 protocol in Ethernet II encapsulation.
  - **809b**—Specifies the AppleTalk protocol in Ethernet II encapsulation.

- **8137**—Specifies the IPX protocol in Ethernet II encapsulation.
- **86dd**—Specifies the IPv6 protocol in Ethernet II encapsulation.

- Do not set both the *dsap-id* and *ssap-id* arguments to any of the following hexadecimal values:
  - **e0**—Specifies the 802.2 LLC encapsulation format for IPX packets.
  - **ff**—Specifies the 802.3 raw encapsulation format for IPX packets.
  - **aa**—Specifies the 802.2 SNAP encapsulation format.

  When either of the *dsap-id* and *ssap-id* arguments is configured, the system assigns the hexadecimal value **aa** to the other argument.
- Do not set the *etype-id* argument in the **snap etype** *etype-id* option to the hexadecimal value 8137. Otherwise, the template format will be the same as that of the IPX protocol. You can set the *etype-id* argument to the hexadecimal value 800, 809b, or 86dd. The hexadecimal values 800, 809b, and 86dd correspond to IPv4, AppleTalk, and IPv6, respectively.

Examples

Assign ARP packets in Ethernet II encapsulation and IPv4 packets to VLAN 3 for transmission. (The protocol type ID for ARP is 0806 in hexadecimal notation.)

```
<Switch> system-view
[Switch] vlan 3
[Switch-vlan3] protocol-vlan 1 ipv4
[Switch-vlan3] protocol-vlan 2 mode ethernetii etype 0806
```

Related commands

display protocol-vlan interface

display protocol-vlan vlan

port protocol-vlan

Contents

A page of this section is **3-x-x**

11. Private VLAN commands 11-1
11.1. Private VLAN commands 11-1
11.1.1. display private-vlan 11-1
11.1.2. port private-vlan host 11-3
11.1.3. port private-vlan promiscuous 11-5
11.1.4. port private-vlan trunk promiscuous 11-7
11.1.5. port private-vlan trunk secondary 11-9
11.1.6. private-vlan (VLAN interface view) 11-13
11.1.7. private-vlan (VLAN view) 11-14
11.1.8. private-vlan isolated 11-16
11.1.9. private-vlan primary 11-17

11. Private VLAN commands

11.1. Private VLAN commands

11.1.1. display private-vlan

Use **display private-vlan** to display information about primary VLANs and their associated secondary VLANs.

Syntax

display private-vlan [*primary-vlan-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

primary-vlan-id: Specifies a primary VLAN ID in the range of 1 to 4094. If you do not specify a primary VLAN ID, this command displays information about all primary VLANs and their associated secondary VLANs.

Examples

Display information about primary VLANs and their associated secondary VLANs.

```
<Switch> display private-vlan
 Primary VLAN ID: 2
 Secondary VLAN ID: 3-4

 VLAN ID: 2
 VLAN type: Static
 Private VLAN type: Primary
 Route interface: Configured
 IPv4 address: 1.1.1.1
 IPv4 subnet mask: 255.255.255.0
 IPv6 global unicast addresses:
   2001::1, subnet is 2001::/64 [TENTATIVE]
 Description: VLAN 0002
 Name: VLAN 0002
 Tagged ports:   None
 Untagged ports:
    GigabitEthernet1/0/2
    GigabitEthernet1/0/3
    GigabitEthernet1/0/4

 VLAN ID: 3
```

```
VLAN type: Static
Private VLAN type: Secondary
Route interface: Not configured
Description: VLAN 0003
Name: VLAN 0003
Tagged ports:   None
Untagged ports:
   GigabitEthernet1/0/2
   GigabitEthernet1/0/3

VLAN ID: 4
VLAN type: Static
Private VLAN type: Secondary
Route interface: Not configured
Description: VLAN 0004
Name: VLAN 0004
Tagged ports:   None
Untagged ports:
   GigabitEthernet1/0/2
   GigabitEthernet1/0/4
```

Table 11-1 Command output

Field	Description
VLAN type	VLAN type, dynamic or static.
Private VLAN type	Private VLAN type: • **Primary**—Primary VLAN. • **Secondary**—Secondary VLAN. • **Isolated secondary**—Secondary VLAN configured with port isolation at Layer 2.
Route interface	Whether a VLAN interface is created for the VLAN: • Configured. • Not configured.
IPv4 address	Primary IPv4 address of the VLAN interface. This field is displayed only when an IPv4 address is configured for the VLAN interface. When the VLAN interface is also configured with secondary IPv4 addresses, you can view them by using one of the following commands: • **`display interface vlan-interface`**. • **`display this`** (VLAN interface view).
IPv4 subnet mask	Subnet mask for the primary IPv4 address of the VLAN interface. This field is displayed only when an IPv4 address is configured for the VLAN interface.
IPv6 global unicast addresses	Global unicast IPv6 address of the VLAN interface. This field is not displayed when no IPv6 address is configured for the VLAN interface. The IPv6 address states are as follows: • **TENTATIVE**—Initial state. DAD is being performed or is to be performed on the address. An address in this state

Field	Description
	cannot be used as the source address or destination address of packets. • **DUPLICATE**—DAD has been completed for the address. The address is not unique on the link and cannot be used. • **PREFERRED**—The address is preferred and can be used as the source or destination address of a packet. If an address is in this state, the command does not display the address state. • **DEPRECATED**—The address is beyond the preferred lifetime but within the valid lifetime. It is valid, but it cannot be used as the source address for a new connection. Packets destined to the address are processed correctly.
Description	VLAN description.
Name	VLAN name.
Tagged ports	Tagged members of the VLAN.
Untagged ports	Untagged members of the VLAN.

Related commands

`private-vlan` (VLAN view)

`private-vlan primary`

11.1.2. port private-vlan host

Use **`port private-vlan host`** to configure a port as a host port.

Use **`undo port private-vlan`** to restore the default.

Syntax

`port private-vlan host`

`undo port private-vlan`

Default

A port is not a host port.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

If the port has been assigned to a secondary VLAN, the command assigns the port to the primary VLAN associated with the secondary VLAN. Also, the following events occur:

- For an access port, the device performs the following operations:
  - Changes the port link type to hybrid.
  - Configures the secondary VLAN as the PVID.

  - Assigns the port to the primary VLAN as an untagged member.
- For a trunk port, the device does not change the port link type or PVID.
- For a hybrid port, the device does not change the port link type or PVID.
  - If the hybrid port has been a tagged or untagged member of the primary VLAN, this member attribute remains in the primary VLAN.
  - If the hybrid port does not allow the primary VLAN, the device assigns the port to the primary VLAN as an untagged member.

You can assign the port to a secondary VLAN before or after you execute this command.

The **undo port private-vlan** command does not change the VLAN attributes (allowed VLANs, port link type, and PVID) of the port.

The **port private-vlan host** command is mutually exclusive with the **port private-vlan trunk promiscuous** and **port private-vlan trunk secondary** commands.

Examples

In this example, VLAN 20 is a secondary VLAN and is associated with primary VLAN 2.

Configure GigabitEthernet 1/0/1 as a host port, and then verify the configuration.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port private-vlan host
[Switch-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port private-vlan host
#
return
```

The output show that GigabitEthernet 1/0/1 is operating in bridge mode and is a host port.

Assign GigabitEthernet 1/0/1 to VLAN 20, and then verify the configuration.

```
[Switch-GigabitEthernet1/0/1] port access vlan 20
[Switch-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port private-vlan host
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 2 20 untagged
 port hybrid pvid vlan 20
#
return
```

The output shows that:

- GigabitEthernet 1/0/1 is an untagged member of secondary VLAN 20 and primary VLAN 2.
- The port link type of GigabitEthernet 1/0/1 is hybrid and its PVID is VLAN 20.

Related commands

port private-vlan promiscuous

port private-vlan trunk promiscuous

port private-vlan trunk secondary

private-vlan (VLAN view)

private-vlan primary

11.1.3. port private-vlan promiscuous

Use **port private-vlan promiscuous** to configure a port as a promiscuous port of the specified VLAN and assign the port to the VLAN.

Use **undo port private-vlan** to restore the default.

Syntax

port private-vlan *vlan-id* **promiscuous**

undo port private-vlan

Default

A port is not a promiscuous port of any VLANs.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

vlan-id: Specifies a VLAN ID in the range of 1 to 4094. Though VLAN 1 is in the valid value range, it cannot be configured in the command.

Usage guidelines

If the specified VLAN is a primary VLAN that has been associated with secondary VLANs, the command assigns the port to the associated secondary VLANs. Also, the following events occur:

- For an access port, the device performs the following operations:
  - Changes the port link type to hybrid.
  - Configures the primary VLAN as the PVID.
  - Assigns the port to the primary VLAN and its associated secondary VLANs as an untagged member.
- For a trunk port, the device does not change the port link type or PVID.
- For a hybrid port, the device does not change the port link type or PVID.
  - If the hybrid port has been a tagged or untagged member of the primary VLAN and part of its associated secondary VLANs, this member attribute remains in these VLANs. The device assigns the hybrid port to the rest of the associated secondary VLANs as an untagged member.
  - If the hybrid port does not allow any of the primary VLAN and its associated secondary VLANs, the command assigns the port to these VLANs as an untagged member.

If you execute this command on a promiscuous port multiple times, the most recent configuration takes effect.

The **undo port private-vlan** command does not change the VLAN attributes (allowed secondary VLANs, link type, and PVID) of the port. When you execute the **undo port**

private-vlan command on a promiscuous port of a VLAN, the command removes the port from the VLAN.

You can configure the VLAN as a primary VLAN before or after you execute the **port private-vlan promiscuous** command.

This command is mutually exclusive with the **port private-vlan trunk promiscuous** and **port private-vlan trunk secondary** commands.

Examples

In this example, VLAN 2 is a primary VLAN, and it is associated with secondary VLAN 20.

Display information about GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
 port link-mode bridge
#
return
```

Configure GigabitEthernet 1/0/1 as a promiscuous port of VLAN 2, and then verify the configuration.

```
[Switch-GigabitEthernet1/0/1] port private-vlan 2 promiscuous
[Switch-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type hybrid
 port private-vlan 2 promiscuous
 undo port hybrid vlan 1
 port hybrid vlan 2 20 untagged
 port hybrid pvid vlan 2
#
return
```

The output shows that:

- GigabitEthernet 1/0/1 is a promiscuous port of VLAN 2.
- GigabitEthernet 1/0/1 is an untagged member of primary VLAN 2 and secondary VLAN 20.
- The port link type of GigabitEthernet 1/0/1 is hybrid and its PVID is VLAN 2.

Execute the **undo port private-vlan** command on GigabitEthernet 1/0/1, and then verify the configuration.

```
[Switch-GigabitEthernet1/0/1] undo port private-vlan
[Switch-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 20 untagged
 port hybrid pvid vlan 2
```

```
#
return
```

The output shows that:

- GigabitEthernet 1/0/1 is removed from primary VLAN 2.
- GigabitEthernet 1/0/1 is an untagged member of VLAN 20.
- The link type and PVID of GigabitEthernet 1/0/1 do not change.

Related commands

port private-vlan host

port private-vlan trunk promiscuous

port private-vlan trunk secondary

private-vlan (VLAN view)

private-vlan primary

11.1.4. port private-vlan trunk promiscuous

Use **port private-vlan trunk promiscuous** to configure a port as a trunk promiscuous port of the specified VLANs and assign the port to these VLANs.

Use **undo port private-vlan trunk promiscuous** to cancel the trunk promiscuous attribute of a port in the specified VLANs.

Syntax

port private-vlan *vlan-id-list* **trunk promiscuous**

undo port private-vlan *vlan-id-list* **trunk promiscuous**

Default

A port is not a trunk promiscuous port of any VLANs.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

vlan-id-list: Specifies a space-separated list of up to 10 primary VLAN items. Each item specifies a primary VLAN ID or a range of primary VLAN IDs in the form of *vlan-id1* **to** *vlan-id2*. The value range for primary VLAN IDs is 1 to 4094. The value for the *vlan-id2* argument must be equal to or greater than the value for the *vlan-id1* argument. Though the system default VLAN (VLAN 1) is in the valid value range, it cannot be configured in the command.

Usage guidelines

If the specified VLANs are primary VLANs that have been associated with secondary VLANs, the command assigns the port to the associated secondary VLANs. Also, the following events occur:

- For an access port, the device performs the following operations:
  - Changes the port link type to hybrid. The PVID of the port does not change.
  - Assigns the port to the primary VLANs and the associated secondary VLANs as a tagged member.

- For a trunk port, the device does not change the port link type or PVID.
- For a hybrid port, the device does not change the port link type or PVID.
  - If the hybrid port has been a tagged or untagged member of part of the primary VLANs and their associated secondary VLANs, this member attribute remains in these VLANs. The device assigns the hybrid port to the rest of the primary VLANs and their associated secondary VLANs as a tagged member.
  - If the hybrid port does not allow any of the primary VLANs and their associated secondary VLANs, the device assigns the port to these VLANs as a tagged member.

The **undo** form of this command does not change the VLAN attributes (allowed secondary VLANs, port link type, and PVID) of the port.

If you execute the **undo** form of this command on a trunk promiscuous port, the command removes the port from the VLANs specified by the *vlan-id-list* argument.

You can configure the specified VLANs as primary VLANs before or after you execute this command.

This command is mutually exclusive with the **port private-vlan host**, **port private-vlan promiscuous** and **port private-vlan trunk secondary** commands.

For an uplink port to permit multiple primary VLANs, use the **port private-vlan trunk promiscuous** command to assign the port to these VLANs. The port can then transmit packets from these primary VLANs with VLAN tags. For an uplink port to permit only one primary VLAN, use the **port private-vlan promiscuous** command to assign the port to the VLAN. The port can then transmit packets from the primary VLAN without VLAN tags.

Examples

In this example, VLANs 2 and 3 are primary VLANs. VLAN 2 is associated with secondary VLAN 20. VLAN 3 is associated with secondary VLAN 30.

Display information about GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
 port link-mode bridge
#
return
```

Configure GigabitEthernet 1/0/1 as a trunk promiscuous port of VLANs 2 and 3, and then verify the configuration.

```
[Switch-GigabitEthernet1/0/1] port private-vlan 2 3 trunk promiscuous
[Switch-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type hybrid
 port private-vlan 2 3 trunk promiscuous
 port hybrid vlan 2 3 20 30 tagged
 port hybrid vlan 1 untagged
#
return
```

The output shows that:

- GigabitEthernet 1/0/1 is a trunk promiscuous port of VLANs 2 and 3.
- GigabitEthernet1/0/1 is a tagged member of VLANs 2, 3, 20, and 30.
- The port link type of GigabitEthernet 1/0/1 is hybrid.

Execute the **undo port private-vlan trunk promiscuous** command on GigabitEthernet 1/0/1, and then verify the configuration.

```
[Switch-GigabitEthernet1/0/1] undo port private-vlan 2 3 trunk promiscuous
[Switch-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type hybrid
 port hybrid vlan 20 30 tagged
 port hybrid vlan 1 untagged
#
return
```

The output shows that:

- GigabitEthernet 1/0/1 is removed from VLANs 2 and 3.
- GigabitEthernet 1/0/1 is a tagged member of VLANs 20 and 30.
- The port link type and PVID of GigabitEthernet 1/0/1 do not change.

Related commands

port private-vlan host

port private-vlan promiscuous

port private-vlan trunk secondary

private-vlan (VLAN view)

private-vlan primary

11.1.5. port private-vlan trunk secondary

Use **port private-vlan trunk secondary** to configure a port as a trunk secondary port of the specified VLANs and assign the port to these VLANs.

Use **undo port private-vlan trunk secondary** to cancel the trunk secondary attribute of a port in the specified VLANs.

Syntax

port private-vlan *vlan-id-list* **trunk secondary**

undo port private-vlan *vlan-id-list* **trunk secondary**

Default

A port is not a trunk secondary port of any VLANs.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

vlan-id-list: Specifies a space-separated list of up to 10 secondary VLAN items. Each item specifies a secondary VLAN ID or a range of secondary VLAN IDs in the form of *vlan-id1* **to** *vlan-id2*. The value range for secondary VLAN IDs is 1 to 4094. The value for the *vlan-id2* argument must be equal to or greater than the value for the *vlan-id1* argument. Though the system default VLAN (VLAN 1) is in the valid value range, it cannot be configured in the command.

Usage guidelines

If the specified VLANs are secondary VLANs that have been associated with primary VLANs, the command also assigns the port to the associated primary VLANs. Also, the following events occur:

- For an access port, the device performs the following operations:
  - Changes the port link type to hybrid. The PVID of the port does not change.
  - Assigns the port to the secondary VLANs and the associated primary VLANs as a tagged member.
- For a trunk port, the device does not change the port link type or PVID.
- For a hybrid port, the device does not change the port link type or PVID.
  - If the port has been an untagged or tagged member of part of the secondary VLANs and their associated primary VLANs, this member attribute remains in these VLANs. The device assigns the port to the rest of the secondary VLANs and their associated primary VLANs as a tagged member.
  - If the hybrid port does not allow any of the secondary VLANs and their associated primary VLANs, the device assigns the port to these VLANs as a tagged member.

A trunk secondary port can join only one secondary VLAN among all secondary VLANs associated with a primary VLAN. However, it can join multiple secondary VLANs that are associated with different primary VLANs.

The **undo** form of this command does not change the VLAN attributes (allowed primary VLANs, port link type, and PVID) of the port.

When you execute the **undo** form of this command on a trunk secondary port of the VLANs specified by the *vlan-id-list* argument, one of the following events occurs:

- If the port is an access port, the device does not change the VLAN configuration of the port.
- If the port is a trunk or hybrid port, the device removes the port from the specified VLANs.

You can associate the specified VLANs with their respective primary VLANs before or after you execute this command.

This command does not take effect on the specified VLAN if any of the following conditions applies:

- The specified VLAN does not exist.
- The specified VLAN is not a secondary VLAN and is used for other purposes.
- The specified VLAN shares the same primary VLAN with other secondary VLANs, and the current port has been configured as a trunk secondary port in one of the other secondary VLANs.

This command is mutually exclusive with the **port private-vlan host**, **port private-vlan promiscuous** and **port private-vlan trunk promiscuous** commands.

For a downlink port to permit multiple secondary VLANs associated with different primary VLANs, use the **port private-vlan trunk secondary** command to assign the port to these secondary VLANs. The port can then transmit packets from these secondary VLANs with VLAN tags. For a downlink port to permit only one secondary VLAN, use the **port private-vlan host** command to assign the port to the secondary VLAN. The port can then transmit packets from the secondary VLAN without VLAN tags.

Examples

- In this example, VLANs 2 and 3 are primary VLANs. VLAN 2 is associated with secondary VLAN 20. VLAN 3 is associated with secondary VLAN 30.

  # Display information about GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
 port link-mode bridge
#
return
```

  # Configure GigabitEthernet 1/0/1 as a trunk secondary port of VLANs 20 and 30, and then verify the configuration.

```
[Switch-GigabitEthernet1/0/1] port private-vlan 20 30 trunk secondary
[Switch-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type hybrid
 port hybrid vlan 2 3 20 30 tagged
 port hybrid vlan 1 untagged
 port private-vlan 20 30 trunk secondary
#
return
```

  The output shows that:

  - GigabitEthernet 1/0/1 is a trunk secondary port of VLANs 20 and 30.
  - GigabitEthernet 1/0/1 is a tagged member of VLANs 2, 3, 20, and 30.
  - The port link type of GigabitEthernet 1/0/1 is hybrid.

  # Execute the **undo port private-vlan trunk secondary** command on GigabitEthernet 1/0/1, and then verify the configuration.

```
[Switch-GigabitEthernet1/0/1] undo port private-vlan 20 30 trunk secondary
[Switch-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type hybrid
 port hybrid vlan 2 3 tagged
 port hybrid vlan 1 untagged
#
return
```

  The output shows that:

  - GigabitEthernet 1/0/1 is removed from VLANs 20 and 30.
  - GigabitEthernet 1/0/1 is a tagged member of VLANs 2 and 3.
  - The port link type and PVID of GigabitEthernet 1/0/1 do not change.

- In this example, VLAN 10 is not a secondary VLAN.

Display information about GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
 port link-mode bridge
#
return
```

Configure GigabitEthernet 1/0/1 as a trunk secondary port of VLAN 10, and then verify the configuration.

```
[Switch-GigabitEthernet1/0/1] port private-vlan 10 trunk secondary
[Switch-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type hybrid
 port hybrid vlan 10 tagged
 port hybrid vlan 1 untagged
 port private-vlan 10 trunk secondary
#
return
```

The output shows that:

- GigabitEthernet 1/0/1 is a trunk secondary port of VLAN 10.
- GigabitEthernet 1/0/1 is a tagged member of VLAN 10.
- The port link type of GigabitEthernet 1/0/1 is hybrid.

Execute the **undo port private-vlan trunk secondary** command on GigabitEthernet1/0/1, and then verify the configuration.

```
[Switch-GigabitEthernet1/0/1] undo port private-vlan 10 trunk secondary
[Switch-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type hybrid
 port hybrid vlan 1 untagged
#
return
```

The output shows that:

- GigabitEthernet 1/0/1 is removed from VLAN 10.
- The port link type and PVID of GigabitEthernet 1/0/1 do not change.

Related commands

port private-vlan host

port private-vlan promiscuous

port private-vlan trunk promiscuous

private-vlan (VLAN view)

private-vlan isolated

private-vlan primary

11.1.6. private-vlan (VLAN interface view)

Use **private-vlan secondary** to enable Layer 3 communication between secondary VLANs that are associated with a primary VLAN.

Use **undo private-vlan** to cancel the Layer 3 communication configuration for secondary VLANs that are associated with a primary VLAN.

Syntax

private-vlan secondary *vlan-id-list*

undo private-vlan [**secondary** *vlan-id-list*]

Default

Secondary VLANs are isolated at Layer 3.

Views

VLAN interface view

Predefined user roles

network-admin

Parameters

vlan-id-list: Specifies a space-separated list of up to 10 secondary VLAN items. Each item specifies a secondary VLAN ID or a range of secondary VLAN IDs in the form of *vlan-id1* **to** *vlan-id2*. The value range for secondary VLAN IDs is 1 to 4094. The value for the *vlan-id2* argument must be equal to or greater than the value for the *vlan-id1* argument.

Usage guidelines

This command takes effect only when the following conditions exist:

- This command is executed in VLAN interface view of the primary VLAN interface.
- Secondary VLANs are associated with the primary VLAN.
- No VLAN interfaces are created for secondary VLANs.
- An IP address is assigned to the primary VLAN interface.
- Local proxy ARP is enabled on the primary VLAN interface.

You can create VLAN interfaces for secondary VLANs that are not enabled with Layer 3 communication. If secondary VLANs are enabled with Layer 3 communication, do not create VLAN interfaces for them.

When you execute this command in the same primary VLAN interface view multiple times, all the specified secondary VLANs are interoperable at Layer 3.

When you execute the **undo private-vlan** command, follow these guidelines:

- If you specify the **secondary** *vlan-id-list* option, this command cancels the Layer 3 communication configuration only for the specified secondary VLANs.
- If you do not specify the **secondary** *vlan-id-list* option, this command cancels the Layer 3 communication configuration for all secondary VLANs of the primary VLAN.

Examples

This example shows how to meet the following requirements:

- VLAN 4 is a secondary VLAN, and it is associated with primary VLAN 2.
- The uplink port (GigabitEthernet 1/0/2) is a promiscuous port of VLAN 2.
- Downlink ports GigabitEthernet 1/0/3 and GigabitEthernet 1/0/4 are host ports of VLANs 3 and 4, respectively.
- Secondary VLANs 3 and 4 can communicate at Layer 3.

Configure VLAN 2 as a primary VLAN and associate it with secondary VLANs 3 and 4.

```
<Switch> system-view
[Switch] vlan 3 to 4
[Switch] vlan 2
[Switch-vlan2] private-vlan primary
[Switch-vlan2] private-vlan secondary 3 to 4
[Switch-vlan2] quit
```

Configure the uplink port (GigabitEthernet 1/0/2) as a promiscuous port of VLAN 2.

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port private-vlan 2 promiscuous
[Switch-GigabitEthernet1/0/2] quit
```

Assign downlink port GigabitEthernet 1/0/3 to VLAN 3 and configure the port as a host port.

```
[Switch] interface gigabitethernet 1/0/3
[Switch-GigabitEthernet1/0/3] port access vlan 3
[Switch-GigabitEthernet1/0/3] port private-vlan host
[Switch-GigabitEthernet1/0/3] quit
```

Assign downlink port GigabitEthernet 1/0/4 to VLAN 4 and configure the port as a host port.

```
[Switch] interface gigabitethernet 1/0/4
[Switch-GigabitEthernet1/0/4] port access vlan 4
[Switch-GigabitEthernet1/0/4] port private-vlan host
[Switch-GigabitEthernet1/0/4] quit
```

Create VLAN-interface 2 and enable Layer 3 communication between secondary VLANs 3 and 4.

```
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] private-vlan secondary 3 to 4
```

Assign an IP address to VLAN-interface 2.

```
[Switch-Vlan-interface2] ip address 192.168.1.1 255.255.255.0
```

Enable local proxy ARP on VLAN-interface 2.

```
[Switch-Vlan-interface2] local-proxy-arp enable
```

Related commands

private-vlan (VLAN view)

private-vlan primary

11.1.7. private-vlan (VLAN view)

Use **private-vlan** to associate a primary VLAN with the specified secondary VLANs.

Use **undo private-vlan** to dissociate a primary VLAN from the specified secondary VLANs.

Syntax

private-vlan secondary *vlan-id-list*

undo private-vlan [**secondary** *vlan-id-list*]

Default

A primary VLAN is not associated with any secondary VLANs.

Views

VLAN view

Predefined user roles

network-admin

Parameters

secondary *vlan-id-list*: Specifies a space-separated list of up to 10 secondary VLAN items. Each item specifies a secondary VLAN ID or a range of secondary VLAN IDs in the form of *vlan-id1* **to** *vlan-id2*. The value range for secondary VLAN IDs is 1 to 4094. The value for the *vlan-id2* argument must be equal to or greater than the value for the *vlan-id1* argument. Though the system default VLAN (VLAN 1) is in the valid value range, it cannot be configured in the command.

Usage guidelines

A primary VLAN can be associated with multiple secondary VLANs. When you execute this command in the same VLAN view multiple times, all the specified secondary VLANs are associated with the primary VLAN.

The configuration synchronization is triggered based on the interface configuration when the following conditions exist:

- This command is configured for a primary VLAN.
- Ports on the device are promiscuous, trunk promiscuous, or host ports.

When you execute the **undo private-vlan** command, follow these guidelines:

- If you specify the **secondary** *vlan-id-list* option, this command dissociates the primary VLAN from the specified secondary VLANs.
- If you do not specify the **secondary** *vlan-id-list* option, this command dissociates the primary VLAN from all secondary VLANs.

Examples

Associate primary VLAN 2 with secondary VLANs 3 and 4.

```
<Switch> system-view
[Switch] vlan 3 to 4
[Switch] vlan 2
[Switch-vlan2] private-vlan primary
[Switch-vlan2] private-vlan secondary 3 to 4
```

Related commands

port private-vlan host

port private-vlan promiscuous

port private-vlan trunk promiscuous

port private-vlan trunk secondary

primary-vlan primary

11.1.8. private-vlan isolated

Use **private-vlan isolated** to isolate ports in a secondary VLAN at Layer 2.

Use **undo private-vlan isolated** to restore the default.

Syntax

private-vlan isolated

undo private-vlan isolated

Default

Ports in the same secondary VLAN can communicate with each other at Layer 2.

Views

VLAN view

Predefined user roles

network-admin

Usage guidelines

This command takes effect when the following conditions exist:

- The secondary VLAN is associated with a primary VLAN.
- The ports are configured as host ports or trunk secondary ports of the secondary VLAN.

This command is mutually exclusive with the primary VLAN, and sub-VLAN configuration commands.

Examples

This example shows how to meet the following requirements:

- VLAN 4 is a secondary VLAN, and it is associated with primary VLAN 2.
- GigabitEthernet 1/0/1 is a promiscuous port of VLAN 2.
- GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 are host ports.
- GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 are isolated at Layer 2 in secondary VLAN 4.

Configure VLAN 2 as a primary VLAN and associate it with secondary VLAN 4.

```
<Switch> system-view
[Switch] vlan 4
[Switch-vlan4] quit
[Switch] vlan 2
[Switch-vlan2] private-vlan primary
[Switch-vlan2] private-vlan secondary 4
[Switch-vlan2] quit
```

Configure GigabitEthernet 1/0/1 as a promiscuous port of VLAN 2.

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port private-vlan 2 promiscuous
[Switch-GigabitEthernet1/0/1] quit
```

Assign GigabitEthernet 1/0/2 to VLAN 4 and configure the port as a host port.

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port access vlan 4
[Switch-GigabitEthernet1/0/2] quit
[Switch-GigabitEthernet1/0/2] port private-vlan host
```

Assign GigabitEthernet 1/0/3 to VLAN 4 and configure the port as a host port.

```
[Switch] interface gigabitethernet 1/0/3
[Switch-GigabitEthernet1/0/3] port access vlan 4
[Switch-GigabitEthernet1/0/3] port private-vlan host
```

Configure port isolation at Layer 2 in secondary VLAN 4.

```
[Switch] vlan 4
[Switch-vlan4] private-vlan isolated
```

Related commands

private-vlan (VLAN view)

private-vlan primary

11.1.9. private-vlan primary

Use **private-vlan primary** to configure a VLAN as a primary VLAN.

Use **undo private-vlan primary** to restore the default.

Syntax

private-vlan primary

undo private-vlan primary

Default

A VLAN is not a primary VLAN.

Views

VLAN view

Predefined user roles

network-admin

Usage guidelines

The configuration synchronization is triggered based on the interface configuration when the following conditions exist:

- This command is configured for a VLAN that has been associated with secondary VLANs.
- Ports on the device are promiscuous, trunk promiscuous, host, or trunk secondary ports.

Examples

Configure VLAN 5 as a primary VLAN.

```
<Switch> system-view
[Switch] vlan 5
[Switch-vlan5] private-vlan primary
```

Related commands

port private-vlan host

port private-vlan promiscuous

port private-vlan trunk promiscuous

port private-vlan trunk secondary

private-vlan primary

Contents

A page of this section is **3-x-x**

12. Voice VLAN commands 12-1
12.1. Voice VLAN commands 12-1
12.1.1. display voice-vlan mac-address 12-1
12.1.2. display voice-vlan state 12-1
12.1.3. voice-vlan aging 12-2
12.1.4. voice-vlan enable 12-3
12.1.5. voice-vlan mac-address 12-4
12.1.6. voice-vlan mode auto 12-5
12.1.7. voice-vlan qos 12-6
12.1.8. voice-vlan qos trust 12-6
12.1.9. voice-vlan security enable 12-7

12. Voice VLAN commands

12.1. Voice VLAN commands

12.1.1. display voice-vlan mac-address

Use **display voice-vlan mac-address** to display the OUI addresses supported on the device.

Syntax

display voice-vlan mac-address

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display the OUI addresses supported on the device.

```
<Switch> display voice-vlan mac-address
OUI Address     Mask            Description
0001-e300-0000  ffff-ff00-0000  Siemens phone
0003-6b00-0000  ffff-ff00-0000  Cisco phone
0004-0d00-0000  ffff-ff00-0000  Avaya phone
000f-e200-0000  ffff-ff00-0000  Aolynk phone
0060-b900-0000  ffff-ff00-0000  Philips/NEC phone
00d0-1e00-0000  ffff-ff00-0000  Pingtel phone
00e0-7500-0000  ffff-ff00-0000  Polycom phone
00e0-bb00-0000  ffff-ff00-0000  3Com phone
```

Table 12-1 Command output

Field	Description
OUI Address	OUI address allowed on the device.
Mask	Mask of the OUI address.
Description	Description of the OUI address.

Related commands

voice-vlan mac-address

12.1.2. display voice-vlan state

Use **display voice-vlan state** to display voice VLAN information.

Syntax

display voice-vlan state

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display voice VLAN information.

```
<Switch> display voice-vlan state
 Current voice VLANs: 1
 Voice VLAN security mode: Security
 Voice VLAN aging time: 1440 minutes
 Voice VLAN enabled ports and their modes:
 Port                        VLAN        Mode        CoS         DSCP
 GE1/0/1                     111         Auto        6           46
```

Table 12-2 Command output

Field	Description
Current Voice VLANs	Number of existing voice VLANs.
Voice VLAN security mode	Voice VLAN mode: • Security. • Normal.
Voice VLAN aging time	Voice VLAN aging timer. **No aging** indicates that the voice VLAN does not age out.
Voice VLAN enabled ports and their modes	Voice VLAN-enabled ports and their voice VLAN assignment modes.
Port	Name of the voice VLAN-enabled port.
VLAN	ID of the voice VLAN enabled on the port.
Mode	Voice VLAN assignment mode of the port: • Manual. • Automatic.

Related commands

voice-vlan aging

voice-vlan enable

voice-vlan mode auto

voice-vlan security enable

12.1.3. voice-vlan aging

Use **voice-vlan aging** to set the voice VLAN aging timer.

Use **undo voice-vlan aging** to restore the default.

Syntax

voice-vlan aging *minutes*

undo voice-vlan aging

Default

The voice VLAN aging timer is 1440 minutes (24 hours).

Views

System view

Predefined user roles

network-admin

Parameters

minutes: Sets the voice VLAN aging timer to 0 minutes or a value in the range of 5 to 43200 minutes. If you set the voice VLAN aging timer to 0 minutes, the voice VLAN does not age out.

Usage guidelines

In automatic voice VLAN assignment mode, the device starts an aging timer for a voice VLAN when assigning a port to the voice VLAN. If no voice packets are received on the port before the timer expires, the device removes the port from the voice VLAN.

Set the voice VLAN aging timer only when the voice VLAN assignment mode is automatic.

Examples

Set the voice VLAN aging timer to 100 minutes.

```
<Switch> system-view
[Switch] voice-vlan aging 100
```

Related commands

display voice-vlan state

12.1.4. voice-vlan enable

Use **voice-vlan enable** to enable the voice VLAN feature on a port.

Use **undo voice-vlan enable** to disable the voice VLAN feature on a port.

Syntax

voice-vlan *vlan-id* **enable**

undo voice-vlan [*vlan-id*] **enable**

Default

The voice VLAN feature is disabled on ports.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

vlan-id: Specifies a voice VLAN ID in the range of 2 to 4094.

Usage guidelines

Use this command only on a hybrid or trunk port operating in automatic voice VLAN assignment mode.

Before you execute this command, make sure the specified VLAN already exists.

Examples

Enable the voice VLAN feature on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] voice-vlan 2 enable
```

Related commands

display voice-vlan state

voice-vlan mode auto

12.1.5. voice-vlan mac-address

Use **voice-vlan mac-address** to configure the OUI address information for voice packet identification.

Use **undo voice-vlan mac-address** to delete an OUI address.

Syntax

voice-vlan mac-address *mac-address* **mask** *oui-mask* [**description** *text*]

undo voice-vlan mac-address *oui*

Default

System default OUI addresses exist.

Table 12-3 System default OUI addresses

Number	OUI address	Vendor
1	0001-e300-0000	Siemens phone
2	0003-6b00-0000	Cisco phone
3	0004-0d00-0000	Avaya phone
4	000f-e200-0000	Aolynk phone
5	0060-b900-0000	Philips/NEC phone
6	00d0-1e00-0000	Pingtel phone
7	00e0-7500-0000	Polycom phone
8	00e0-bb00-0000	3Com phone

Views

System view

Predefined user roles

network-admin

Parameters

mac-address: Specifies a source MAC address of voice traffic, in the format of H-H-H. For example, 1234-1234-1234.

mask *oui-mask*: Specifies the valid length of the OUI address by using a mask in the format of H-H-H. The mask contains consecutive 1s and 0s. For example, ffff-0000-0000. To match the voice devices of a vendor, set the mask to ffff-ff00-0000.

description *text*: Specifies the OUI address description, a case-sensitive string of 1 to 30 characters.

oui: Specifies an OUI address to delete, in the format of H-H-H. For example, 1234-1200-0000. An OUI address is the logical AND result of the *mac-address* and *oui-mask* arguments. It cannot be a broadcast address, a multicast address, or an all-zero address.

Usage guidelines

You can manually delete or add the system default OUI addresses.

The device supports a maximum of 128 OUI addresses.

Examples

Add OUI address **1234-1200-0000** by specifying the MAC address as 1234-1234-1234 and the mask as fff-ff00-0000. Configure the OUI address description as **PhoneA**.

```
<Switch> system-view
[Switch] voice-vlan mac-address 1234-1234-1234 mask ffff-ff00-0000 description PhoneA
```

Related commands

display voice-vlan mac-address

12.1.6. voice-vlan mode auto

Use **voice-vlan mode auto** to configure a port to operate in automatic voice VLAN assignment mode.

Use **undo voice-vlan mode auto** to configure a port to operate in manual voice VLAN assignment mode.

Syntax

voice-vlan mode auto

undo voice-vlan mode auto

Default

A port operates in automatic voice VLAN assignment mode.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

To make a voice VLAN take effect on a port operating in manual mode, you must manually assign the port to the voice VLAN.

Examples

Configure GigabitEthernet 1/0/1 to operate in manual voice VLAN assignment mode.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] undo voice-vlan mode auto
```

Related commands

display voice-vlan state

12.1.7. voice-vlan qos

Use **voice-vlan qos** to configure a port to modify the CoS and DSCP values for incoming voice VLAN packets.

Use **undo voice-vlan qos** to restore the default.

Syntax

voice-vlan qos *cos-value dscp-value*

undo voice-vlan qos

Default

A port modifies the CoS and DSCP values for incoming voice VLAN packets to 6 and 46, respectively.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

cos-value: Specifies a CoS value in the range of 0 to 7. A bigger CoS value represents a higher priority.

dscp-value: Specifies a DSCP value in the range of 0 to 63. A bigger DSCP value represents a higher priority.

Usage guidelines

If you execute both the **voice-vlan qos** and **voice-vlan qos trust** commands multiple times, the most recent configuration takes effect.

Examples

Configure GigabitEthernet 1/0/1 to modify the CoS and DSCP values for voice VLAN packets to 5 and 45, respectively.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] voice-vlan qos 5 45
```

Related commands

voice-vlan qos trust

12.1.8. voice-vlan qos trust

Use **voice-vlan qos trust** to configure a port to trust the priority settings in incoming voice VLAN packets.

Use **undo voice-vlan qos** to restore the default.

Syntax

voice-vlan qos trust

undo voice-vlan qos

Default

A port modifies the CoS and DSCP values for incoming voice VLAN packets to 6 and 46, respectively.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

When a port trusts the QoS priority settings in incoming voice VLAN packets, the port does not modify their CoS and DSCP values.

By default, a port does not trust the 802.1p priority of incoming packets. To configure the port to trust the priority settings in incoming voice VLAN packets, you must also use the **qos trust dot1p** command to set the priority trust mode to 802.1p priority on the port. For information about setting the priority trust mode, see *ACL and QoS Configuration Guide*.

If you execute both the **voice-vlan qos** and **voice-vlan qos trust** commands multiple times, the most recent configuration takes effect.

Examples

Configure GigabitEthernet 1/0/1 to trust the priority settings in incoming voice VLAN traffic.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] voice-vlan qos trust
```

Related commands

voice-vlan qos

12.1.9. voice-vlan security enable

Use **voice-vlan security enable** to enable the voice VLAN security mode.

Use **undo voice-vlan security enable** to disable the voice VLAN security mode.

Syntax

voice-vlan security enable

undo voice-vlan security enable

Default

The voice VLAN security mode is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

In security mode, a voice VLAN transmits only voice packets whose source MAC addresses match the OUI addresses of the device.

In normal mode, a voice VLAN transmits voice packets and non-voice packets.

Examples

Disable the voice VLAN security mode.

```
<Switch> system-view
[Switch] undo voice-vlan security enable
```

Related commands

display voice-vlan state

Contents

A page of this section is **3-x-x**

13. QinQ commands 13-1
13.1. QinQ commands 13-1
13.1.1. display qinq 13-1
13.1.2. qinq enable 13-2
13.1.3. qinq ethernet-type (interface view) 13-2
13.1.4. qinq ethernet-type (system view) 13-4
13.1.5. qinq transparent-vlan 13-5

13. QinQ commands

13.1. QinQ commands

Do not configure QinQ and Ethernet service instance-to-VSI binding on the same Layer 2 Ethernet interface or Layer 2 aggregate interface. Do not configure QinQ on a Layer 2 Ethernet interface or Layer 2 aggregate interface that acts as the source interface of a VXLAN tunnel. Otherwise, these features might not take effect. For more information about VXLAN and VSI, see *VXLAN Configuration Guide*.

This document uses the following terms:

- **CVLAN**—Customer network VLANs, also called inner VLANs, refer to VLANs that a customer uses on the private network.
- **SVLAN**—Service provider network VLANs, also called outer VLANs, refer to VLANs that a service provider uses to transmit VLAN tagged traffic for customers.

13.1.1. display qinq

Use **display qinq** to display QinQ-enabled interfaces.

Syntax

display qinq [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays all QinQ-enabled interfaces.

Usage guidelines

If QinQ is not enabled on any interfaces, this command does not provide any output.

Examples

Enable QinQ on GigabitEthernet 1/0/1. Then, verify that QinQ is enabled on the interface.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] qinq enable
[Switch-GigabitEthernet1/0/1] display qinq interface gigabitethernet 1/0/1
Interface
 GigabitEthernet1/0/1
```

Enable QinQ on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/3. Then, verify that QinQ is enabled on the interfaces.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
```

```
[Switch-GigabitEthernet1/0/1] qinq enable
[Switch-GigabitEthernet1/0/1] quit
[Switch] interface gigabitethernet 1/0/3
[Switch-GigabitEthernet1/0/3] qinq enable
[Switch-GigabitEthernet1/0/3] display qinq
Interface
 GigabitEthernet1/0/1
 GigabitEthernet1/0/3
```

Related commands

qinq enable

13.1.2. qinq enable

Use **qinq enable** to enable QinQ on an interface.

Use **undo qinq enable** to disable QinQ on an interface.

Syntax

qinq enable

undo qinq enable

Default

QinQ is disabled on interfaces.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Examples

Enable QinQ on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] qinq enable
```

Related commands

display qinq

13.1.3. qinq ethernet-type (interface view)

Use **qinq ethernet-type** to set the TPID value in SVLAN tags on an interface.

Use **undo qinq ethernet-type** to restore the default TPID value in SVLAN tags on an interface.

Syntax

qinq ethernet-type service-tag *hex-value*

undo qinq ethernet-type service-tag

Default

The TPID value in SVLAN tags is 8100 in hexadecimal notation.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

service-tag: Sets the TPID value in the SVLAN tag.

hex-value: Sets a hexadecimal TPID value in the range of 1 to ffff, excluding the reserved EtherType values listed in Table 13-1 .

Table 13-1 Reserved EtherType values

Protocol type	Value
ARP	0x0806
PUP	0x0200
RARP	0x8035
IP	0x0800
IPv6	0x86dd
PPPoE	0x8863/0x8864
MPLS	0x8847/0x8848
IPX/SPX	0x8137
IS-IS	0x8000
LACP	0x8809
LLDP	0x88cc
802.1X	0x888e
802.1ag	0x8902
Cluster	0x88a7
Reserved	0xfffd/0xfffe/0xffff

Usage guidelines

A port without QinQ enabled uses the SVLAN TPID to match incoming tagged frames. The port modifies the TPID in the SVLAN tag of outgoing frames as the configured value.

Examples

Set the TPID value in SVLAN tags to 9100 (hexadecimal) on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] qinq ethernet-type service-tag 9100
```

Related commands

qinq ethernet-type (system view)

13.1.4. qinq ethernet-type (system view)

Use **qinq ethernet-type** to set the TPID value in CVLAN tags.

Use **undo qinq ethernet-type** to restore the default TPID value in CVLAN tags.

Syntax

qinq ethernet-type customer-tag *hex-value*

undo qinq ethernet-type customer-tag

Default

The TPID value in CVLAN tags is 8100 in hexadecimal notation.

Views

System view

Predefined user roles

network-admin

Parameters

customer-tag: Sets the TPID value in the CVLAN tag.

hex-value: Sets a hexadecimal TPID value in the range of 1 to ffff, excluding the reserved EtherType values listed in Table 13-2 .

Table 13-2 Reserved EtherType values

Protocol type	Value
ARP	0x0806
PUP	0x0200
RARP	0x8035
IP	0x0800
IPv6	0x86dd
PPPoE	0x8863/0x8864
MPLS	0x8847/0x8848
IPX/SPX	0x8137
IS-IS	0x8000
LACP	0x8809
LLDP	0x88cc
802.1X	0x888e
802.1ag	0x8902
Cluster	0x88a7
Reserved	0xfffd/0xfffe/0xffff

Examples

Set the TPID value in CVLAN tags to 8200 (hexadecimal).

```
<Switch> system-view
```

```
[Switch] qinq ethernet-type customer-tag 8200
```

Related commands

qinq ethernet-type (interface view)

13.1.5. qinq transparent-vlan

Use **qinq transparent-vlan** to enable transparent transmission for a list of VLANs on a port.

Use **undo qinq transparent-vlan** to disable transparent transmission for a list of VLANs on a port.

Syntax

qinq transparent-vlan *vlan-id-list*

undo qinq transparent-vlan { *vlan-id-list* | **all** }

Default

Transparent transmission is disabled for all VLANs.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

vlan-id-list: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a single VLAN ID or a VLAN ID range in the form of *vlan-id1* **to** *vlan-id2*. The value range for VLAN IDs is 1 to 4094. The end VLAN ID must be equal to or greater than the start VLAN ID.

all: Specifies all VLANs.

Usage guidelines

By default, QinQ tags all incoming frames with the PVID on a port. This command disables QinQ to tag incoming traffic from a list of VLANs. These VLANs are called transparent VLANs.

You can repeat this command to add VLANs to the list of transparent VLANs.

To ensure successful transmission for a transparent VLAN, follow these configuration guidelines:

- Set the link type of the port to trunk or hybrid, and assign the port to the transparent VLAN.
- Do not configure any other VLAN manipulation actions for the transparent VLAN on the port.
- Make sure all ports on the traffic path permit the transparent VLAN to pass through.
- If you use both transparent VLANs and VLAN mappings on an interface, the transparent VLANs cannot be the following VLANs:
  - Original or translated VLANs of one-to-one or one-to-two VLAN mappings.
  - Original or translated outer VLANs of two-to-two VLAN mappings.

Examples

Configure GigabitEthernet 1/0/1 as a trunk port, and assign the port to VLAN 2, VLAN 3, and VLANs 50 through 100. Enable QinQ on GigabitEthernet 1/0/1, and configure the port to transparently transmit frames from VLAN 2.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
```

```
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 2 3 50 to 100
[Switch-GigabitEthernet1/0/1] qinq enable
[Switch-GigabitEthernet1/0/1] qinq transparent-vlan 2
```

Contents

A page of this section is **3-x-x**

14. VLAN mapping commands 14-1
14.1. VLAN mapping commands 14-1
14.1.1. display vlan mapping 14-1
14.1.2. vlan mapping 14-2

14. VLAN mapping commands

14.1. VLAN mapping commands

Do not configure VLAN mapping and Ethernet service instance-to-VSI binding on the same Layer 2 Ethernet interface or Layer 2 aggregate interface. Do not configure VLAN mapping on a Layer 2 Ethernet interface or Layer 2 aggregate interface that acts as the source interface of a VXLAN tunnel. Otherwise, these features might not take effect. For more information about VXLAN and VSI, see *VXLAN Configuration Guide*.

14.1.1. display vlan mapping

Use **display vlan mapping** to display VLAN mapping information.

Syntax

display vlan mapping [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, the command displays VLAN mapping information on all interfaces.

Examples

Display VLAN mapping information on all interfaces.

```
<Switch> display vlan mapping

Interface GigabitEthernet1/0/1:
  Outer VLAN    Inner VLAN    Translated Outer VLAN    Translated Inner VLAN
  10            N/A           120                      N/A
  Outer VLAN    Inner VLAN    Nested VLAN
  200           100           300

Interface GigabitEthernet1/0/3:
  Outer VLAN    Inner VLAN    Translated Outer VLAN    Translated Inner VLAN
  12            N/A           110                      12

Interface GigabitEthernet1/0/4:
  Outer VLAN    Inner VLAN    Translated Outer VLAN    Translated Inner VLAN
  11            30            130                      40
```

Table 14-1 Command output

Field	Description
Outer VLAN	Original outer VLAN. This field indicates the original VLAN for one-to-one VLAN mapping and one-to-two VLAN mapping.
Inner VLAN	Original inner VLAN. This field displays **N/A** for one-to-one VLAN mapping and one-to-two VLAN mapping.
Translated Outer VLAN	Translated outer VLAN. This field indicates the translated VLAN for one-to-one VLAN mapping.
Translated Inner VLAN	Translated inner VLAN. This field displays **N/A** for one-to-one VLAN mapping.

Related commands

vlan mapping

14.1.2. vlan mapping

Use **vlan mapping** to configure VLAN mapping on an interface.

Use **undo vlan mapping** to cancel the VLAN mapping configuration.

Syntax

vlan mapping { *vlan-id* **translated-vlan** *vlan-id* | **nest** { **range** *vlan-range-list* | **single** *vlan-id-list* } **nested-vlan** *vlan-id* | **tunnel** *outer-vlan-id inner-vlan-id* **translated-vlan** *outer-vlan-id inner-vlan-id* }

undo vlan mapping { *vlan-id* **translated-vlan** *vlan-id* | **all** | **nest** { **range** *vlan-range-list* | **single** *vlan-id-list* } **nested-vlan** *vlan-id* | **tunnel** *outer-vlan-id inner-vlan-id* **translated-vlan** *outer-vlan-id inner-vlan-id* }

Default

No VLAN mapping is configured on an interface.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

vlan-id **translated-vlan** *vlan-id*: Specifies the original VLAN and translated VLAN for a one-to-one VLAN mapping. The value range for the *vlan-id* argument is 1 to 4094. The original VLAN and the translated VLAN cannot be the same.

nest range *vlan-range-list* **nested-vlan** *vlan-id*: Specifies the CVLAN ranges and the SVLAN for a one-to-two VLAN mapping. The *vlan-range-list* argument specifies a space-separated list of up to 10 CVLAN items. Each item specifies a CVLAN ID or a range of CVLAN

IDs in the format of *vlan-id1* **to** *vlan-id2*. The value range for CVLAN IDs is 1 to 4094. The value for the *vlan-id2* argument must be greater than the value for the *vlan-id1* argument. Different CVLAN ranges cannot overlap. The *vlan-id* argument specifies the SVLAN ID in the range of 1 to 4094.

nest single *vlan-id-list* **nested-vlan** *vlan-id*: Specifies the CVLANs and the SVLAN for a one-to-two VLAN mapping. The *vlan-id-list* argument specifies a space-separated list of up to 10 CVLAN IDs, each of which is in the range of 1 to 4094. The *vlan-id* argument specifies the SVLAN ID in the range of 1 to 4094.

tunnel *outer-vlan-id inner-vlan-id* **translated-vlan** *outer-vlan-id inner-vlan-id*: Specifies the original outer VLAN ID, original inner VLAN ID, translated outer VLAN ID, and translated inner VLAN ID for a two-to-two VLAN mapping. The value ranges for the *outer-vlan-id* argument and the *inner-vlan-id* argument are both 1 to 4094.

all: Deletes all VLAN mapping configurations from the interface.

Usage guidelines

VLAN mapping takes effect only on VLAN-tagged packets received on an interface.

The original and translated VLANs in VLAN mappings on an interface must meet the following requirements:

- Different types of VLAN mapping entries cannot include the same original VLANs or translated VLANs.
- Different one-to-one or two-to-two VLAN mapping entries cannot include the same translated VLANs. If you configure multiple one-to-one or two-to-two VLAN mapping entries for the same original VLANs, the most recent configuration takes effect.

The configuration restrictions between QinQ and VLAN mappings are as follows:

- Before you enable or disable QinQ on a port, you must remove all VLAN mappings on the port.
- You cannot configure two-to-two VLAN mappings on a QinQ-enabled port.

If you use both transparent VLANs and VLAN mappings on an interface, the transparent VLANs cannot be the following VLANs:

- Original or translated VLANs of one-to-one and one-to-two VLAN mappings.
- Original or translated outer VLANs of two-to-two VLAN mappings.

The MTU of an interface is 1500 bytes by default. After a VLAN tag is added to a packet, the packet length is added by 4 bytes. As a best practice, set the MTU to a minimum of 1504 bytes for ports on the forwarding path of the packet on the service provider network.

VLAN mapping is supported only for Layer 2 switching and is not supported for Layer 3 routing.

If you create a VLAN interface for the original VLAN and set an IP address, do not configure VLAN mapping on the interface that sends and receives the Layer 3 routing traffic.

Examples

Configure a one-to-one VLAN mapping on GigabitEthernet 1/0/1 to map VLAN 1 to VLAN 101.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] vlan mapping 1 translated-vlan 101
```

Configure one-to-two VLAN mappings on GigabitEthernet 1/0/4 to add SVLAN tag 101 to packets carrying VLAN tags 1 through 10 and VLAN tag 80.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/4
[Switch-GigabitEthernet1/0/4] vlan mapping nest range 1 to 10 nested-vlan 101
[Switch-GigabitEthernet1/0/4] vlan mapping nest single 80 nested-vlan 101
```

Configure a two-to-two VLAN mapping on GigabitEthernet 1/0/5 to map SVLAN 101 and CVLAN 1 to SVLAN 201 and CVLAN 10.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/5
[Switch-GigabitEthernet1/0/5] vlan mapping tunnel 101 1 translated-vlan 201 10
```

Related commands

display vlan mapping

Contents

A page of this section is **3-x-x**

15. LLDP commands ····· 15-1
15.1. LLDP commands ····· 15-1
15.1.1. display lldp local-information ····· 15-1
15.1.2. display lldp neighbor-information ····· 15-6
15.1.3. display lldp statistics ····· 15-12
15.1.4. display lldp status ····· 15-14
15.1.5. display lldp tlv-config ····· 15-17
15.1.6. lldp admin-status ····· 15-20
15.1.7. lldp check-change-interval ····· 15-21
15.1.8. lldp compliance admin-status cdp ····· 15-22
15.1.9. lldp compliance cdp ····· 15-23
15.1.10. lldp enable ····· 15-24
15.1.11. lldp encapsulation snap ····· 15-24
15.1.12. lldp fast-count ····· 15-25
15.1.13. lldp global enable ····· 15-26
15.1.14. lldp hold-multiplier ····· 15-26
15.1.15. lldp management-address ····· 15-27
15.1.16. lldp management-address-format string ····· 15-28
15.1.17. lldp notification remote-change enable ····· 15-29
15.1.18. lldp timer notification-interval ····· 15-30
15.1.19. lldp timer reinit-delay ····· 15-30
15.1.20. lldp timer tx-interval ····· 15-31
15.1.21. lldp tlv-enable ····· 15-31

15. LLDP commands

15.1. LLDP commands

15.1.1. display lldp local-information

Use **display lldp local-information** to display local LLDP information.

Syntax

display lldp local-information [**global** | **interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

global: Displays the global local LLDP information.

interface *interface-type interface-number*: Specifies a port by its type and number.

Usage guidelines

If you do not specify any keywords or arguments, the command displays all local LLDP information, which includes the following:

- The global LLDP information.
- The LLDP information about the LLDP-enabled ports in up state.

Examples

Display all local LLDP information.

```
<Switch> display lldp local-information
Global LLDP local-information:
 Chassis ID          : f474-8800-5600
 System name         : Switch
 System description  :
   Copyright (c) 2004-2017 New H3C Technologies Co., Ltd. All rights reserved.
 System capabilities supported  : Bridge, Router, Customer Bridge, Service Bridge
 System capabilities enabled    : Bridge, Router, Service Bridge

 MED information:
 Device class               : Connectivity device
 MED inventory information of master board:
 HardwareRev                : REV.A
 FirmwareRev                : 109
 SoftwareRev                : 7.1.070
 SerialNum                  : NONE
```

```
 Manufacturer name          : NEC
 Model name                 : QX-S5624GT-4X1C
 Asset tracking identifier  : Unknown
LLDP local-information of port 52[GigabitEthernet1/0/3]:
 Port ID type       : Interface name
 Port ID            : GigabitEthernet1/0/3
 Port description   : GigabitEthernet1/0/3 Interface
 LLDP agent nearest-bridge management address:
 Management address type           : IPv4
 Management address                 : 192.168.80.60
 Management address interface type : IfIndex
 Management address interface ID   : Unknown
 Management address OID             : 0
 LLDP agent nearest-nontpmr management address:
 Management address type           : IPv4
 Management address                 : 192.168.80.61
 Management address interface type : IfIndex
 Management address interface ID   : Unknown
 Management address OID             : 0
 LLDP agent nearest-customer management address:
 Management address type           : IPv4
 Management address                 : 192.168.80.62
 Management address interface type : IfIndex
 Management address interface ID   : Unknown
 Management address OID             : 0
 Port VLAN ID(PVID): 1
 Port and protocol VLAN ID(PPVID) : 12
 Port and protocol VLAN supported : Yes
 Port and protocol VLAN enabled   : Yes
 VLAN name of VLAN 12: VLAN 0012
 Management VLAN ID  : 5
 Link aggregation supported : Yes
 Link aggregation enabled   : Yes
 Aggregation port ID        : 52
 Auto-negotiation supported : Yes
 Auto-negotiation enabled   : Yes
 OperMau                    : Speed(1000)/Duplex(Full)
 Power port class           : PSE
 PSE power supported        : NO
 PSE power enabled          : NO
 PSE pairs control ability  : NO
 Power pairs                : Signal
 Port power classification  : Class 0
 Power type                 : Type 2 PSE
 Power source               : Primary
 Power priority             : Unknown
 PD requested power value   : 0.0 w
 PSE allocated power value  : 0.0 w
```

```
Maximum frame size          : 10000
Transmit Tw                 : 0 us
Receive Tw                  : 0 us
Fallback Tw                 : 0 us
Echo Transmit Tw            : 0 us
Echo Receive Tw             : 0 us
PoE PSE power source        : Primary
Port PSE priority           : Critical
Port available power value : 0.0 w
```

Table 15-1 Command output

Field	Description
Chassis ID	Bridge MAC address of the device.
System capabilities supported	Supported capabilities: • **Bridge**—Switching is supported. • **Router**—Routing is supported. • **Repeater**—Signal repeating is supported. • **Telephone**—The local device can act as a telephone. • **DocsisCableDevice**—The local device can act as a DOCSIS-compliant cable device. • **StationOnly**—The local device can act as a station only. • **Customer Bridge**—The customer bridge feature is supported. • **Service Bridge**—The service bridge feature is supported. • **TPMR**—The TPMR feature is supported. • **Other**—Features other than those listed above are supported.
System capabilities enabled	Enabled capabilities: • **Bridge**—Switching is enabled. • **Router**—Routing is enabled. • **Repeater**—Signal repeating is enabled. • **Telephone**—The local device is acting as a telephone. • **DocsisCableDevice**—The local device is acting as a DOCSIS-compliant cable device. • **StationOnly**—The local device is acting as a station only. • **Customer Bridge**—The customer bridge feature is enabled. • **Service Bridge**—The service bridge feature is enabled. • **TPMR**—The TPMR feature is enabled. • **Other**—Features other than those listed above are enabled.
Device class	MED device class: • **Connectivity device**—Network device. • **Class I**—Normal terminal device. It requires the basic LLDP discovery services. • **Class II**—Media terminal device. It supports media streams, and can also act as a normal terminal device. • **Class III**—Communication terminal device. It supports the IP communication systems of end users, and can

Field	Description
	also act as a normal terminal device or media terminal device.
MED inventory information of master board	MED inventory information about the .
HardwareRev	Hardware version.
FirmwareRev	Firmware version.
SoftwareRev	Software version.
SerialNum	Serial number.
Manufacturer name	Device manufacturer.
Model name	Device model.
Port ID type	Port ID type: • MAC address. • Interface name.
Port ID	Port ID, the value of which depends on the port ID type.
Management address interface type	Numbering type of the interface identified by the management address.
Management address interface ID	Index of the interface identified by the management address.
Management address OID	Management address object ID.
Port VLAN ID(PVID)	Port VLAN ID.
Port and protocol VLAN ID(PPVID)	Port protocol VLAN ID.
Port and protocol VLAN supported	Indicates whether protocol VLAN is supported on the port.
Port and protocol VLAN enabled	Indicates whether protocol VLAN is enabled on the port.
Link aggregation supported	Indicates whether link aggregation is supported on the port.
Link aggregation enabled	Indicates whether link aggregation is enabled on the port.
Aggregation port ID	Member port ID, which is 0 when link aggregation is disabled.
Auto-negotiation supported	Indicates whether autonegotiation is supported on the port.
Auto-negotiation enabled	Indicates whether autonegotiation is enabled on the port.
OperMau	Speed and duplex state of the port.
Power port class	PoE port class: • **PSE**—Power sourcing equipment. • **PD**—Powered device.
PSE power supported	Indicates whether the device can operate as a PSE.
PSE power enabled	Indicates whether the device is operating as a PSE.
PSE pairs control ability	Indicates whether the pair selection ability is available.
Power pairs	Power supply mode: • **Signal**—Uses data pairs to supply power. • **Spare**—Uses spare pairs to supply power.

Field	Description
Port power classification	Power class of the PD: • Class 0. • Class 1. • Class 2. • Class 3. • Class 4.
Power type	Power supply type: • Type 1 PD. • Type 2 PD. • Type 1 PSE. • Type 2 PSE.

Power source	Power source:
	• When the power supply type is PSE, options are:
	  ○ **Unknown**—Unknown power supply.
	  ○ **Primary**—Primary power supply.
	  ○ **Backup**—Backup power supply.
	  ○ **Reserved**.
	• When the power supply type is PD, options are:
	  ○ **Unknown**—Unknown power supply.
	  ○ **PSE**—PSE power supply.
	  ○ **Local**—Local power supply.
	  ○ **PSE and local**—PSE and local power supplies.

Power priority	• Unknown. • Critical. • High. • Low.
PD requested power value	PD requested power in watts.
PSE allocated power value	PSE allocated power value.
PoE PSE power source	PSE power source type: • **Unknown**—Unknown power supply. • **Primary**—Primary power supply. • **Backup**—Backup power supply.
PoE PD power source	PD power source type: • **Unknown**—Unknown power supply. • **PSE**—PSE power supply. • **Local**—Local power supply. • **PSE and local**—PSE and local power supplies.
Port PSE priority	PoE power supply priority of PSE ports: • Unknown. • Critical. • High. • Low.
Port PD priority	PoE power receiving priority of PD ports: • Unknown. • Critical. • High.

Field	Description
	• Low.
Port available power value	Available PoE power on PSE ports, or power needed on PD ports, in watts.
Transmit Tw	Sleep time of the local client, in μs.
Receive Tw	Sleep time of the peer client expected by the local client, in μs.
Fallback Tw	Candidate sleep time of the peer client expected by the local client, in μs.
Echo Transmit Tw	Sleep time of the peer client, in μs. This field displays zero when one of the following cases occurs: • The local client has not received the sleep time of the peer client. • The sleep time of the peer client is 0 μs.
Echo Receive Tw	Sleep time of the local client expected by the peer client, in μs. This field displays zero when one of the following cases occurs: • The local client has not received the expected sleep time from the peer client. • The sleep time of the local client expected by the peer client is 0 μs.

15.1.2. display lldp neighbor-information

Use **display lldp neighbor-information** to display the LLDP information received from the neighboring devices.

Syntax

display lldp neighbor-information [[[**interface** *interface-type interface-number*] [**agent** { **nearest-bridge** | **nearest-customer** }] [**verbose**]] | **list** [**system-name** *system-name*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number. If you do not specify this option, the command displays the LLDP information that all ports receive from the neighboring devices.

agent: Specifies an agent type. If you do not specify an agent type, the command displays the LLDP information that all LLDP agents receive from the neighboring devices.

nearest-bridge: Specifies nearest bridge agents.

nearest-customer: Specifies nearest customer bridge agents.

verbose: Displays the detailed LLDP information that the local device receives from the neighboring devices. If you do not specify this keyword, the command displays the brief LLDP information that the local device receives from the neighboring devices.

list: Displays the LLDP information that the local device receives from the neighboring devices in the form of a list.

system-name *system-name*: Displays the LLDP information that the local device receives from a neighboring device specified by its system name. The *system-name* argument is a string of 1 to 255 characters. If you do not specify this option, the command displays the LLDP information that the local device receives from all neighboring devices in a list.

Examples

Display detailed LLDP information that the nearest bridge agents on all ports received from the neighboring devices.

```
<Switch> display lldp neighbor-information agent nearest-bridge verbose
LLDP neighbor-information of port 1[GigabitEthernet1/0/1]:
LLDP agent nearest-bridge:
 LLDP Neighbor index : 1
 Update time         : 0 days, 0 hours, 1 minutes, 1 seconds
 Chassis type        : MAC address
 Chassis ID          : 000f-0055-0002
 Port ID type        : Interface name
 Port ID             : GigabitEthernet1/0/1
 Time to live        : 121
 Port description    : GigabitEthernet1/0/1 Interface
 System name         : Switch
 System description  :
   Copyright (c) 2004-2017 New H3C Technologies Co., Ltd. All rights reserved.
 System capabilities supported : Bridge, Router, Customer Bridge, Service Bridge
 System capabilities enabled   : Bridge, Router, Customer Bridge
 Management address type           : IPv4
 Management address                : 192.168.1.55
 Management address interface type : IfIndex
 Management address interface ID   : Unknown
 Management address OID            : 0
 Port VLAN ID(PVID): 1
 Port and protocol VLAN ID(PPVID) : 12
 Port and protocol VLAN supported : Yes
 Port and protocol VLAN enabled   : Yes
 VLAN name of VLAN 12: VLAN 0012
 Link aggregation supported : Yes
 Link aggregation enabled   : Yes
 Aggregation port ID        : 52
 Management VLAN ID  : 5
 Auto-negotiation supported : Yes
 Auto-negotiation enabled   : Yes
 OperMau                    : Speed(1000)/Duplex(Full)
 Power port class           : PD
 PSE power supported        : Yes
```

```
 PSE power enabled          : Yes
 PSE pairs control ability  : Yes
 Power pairs                : Signal
 Port power classification  : Class 0
 Power type                 : Type 2 PD
 Power source               : PSE and local
 Power priority             : High
 PD requested power value   : 21.1 w
 PSE allocated power value  : 15.3 w
 Maximum frame size         : 10000
```

Display brief LLDP information that all LLDP agents received from all neighboring devices.

```
<Switch> display lldp neighbor-information
LLDP neighbor-information of port 52[GigabitEthernet1/0/3]:
LLDP agent nearest-bridge:
 LLDP neighbor index : 3
 ChassisID/subtype   : 0011-2233-4400/MAC address
 PortID/subtype      : 000c-29f5-c71f/MAC address
 Capabilities        : Bridge, Router, Customer Bridge

 LLDP neighbor index : 6
 ChassisID/subtype   : 0011-2233-4400/MAC address
 PortID/subtype      : 000c-29f5-c715/MAC address
 Capabilities        : None

CDP neighbor-information of port 52[GigabitEthernet1/0/3]:
LLDP agent nearest-bridge:
 CDP neighbor index  : 4
 Chassis ID          : SEP00260B5C0548
 Port ID             : Port 1

 CDP neighbor index  : 5
 Chassis ID          : 0011-2233-4400
 Port ID             : GigabitEthernet1/0/4

LLDP neighbor-information of port 52[GigabitEthernet1/0/3]:
LLDP agent nearest-nontpmr:
 LLDP neighbor index : 6
 ChassisID/subtype   : 0011-2233-4400/MAC address
 PortID/subtype      : 000c-29f5-c715/MAC address
 Capabilities        : None
```

Display brief LLDP information that all LLDP agents received from the neighboring devices in a list.

```
<Switch> display lldp neighbor-information list
Chassis ID : * -- --Nearest nontpmr bridge neighbor
             # -- --Nearest customer bridge neighbor
             Default -- -- Nearest bridge neighbor
LocalIf         Nbr chassis ID  Nbr port ID                    Nbr system name
GE1/0/1         000f-e25d-ee91  GigabitEthernet1/0/1           System1
```

Table 15-2 Command output

Field	Description
LLDP neighbor-information of port 1	LLDP information received through port 1.
Update time	Time when LLDP information about a neighboring device was last updated.
LLDP mac type	Type of the neighbor MAC address: • Nearest bridge. • Nearest customer bridge. • Nearest non-TPMR bridge.
Chassis type	Chassis ID type: • **Chassis component**. • **Interface alias**. • **Port component**. • **MAC address**. • **Network address (ipv4)**. • **Interface name**. • **Locally assigned**—Locally-defined chassis type other than those listed above.
Nbr chassis ID	ID that identifies the LLDP sending device, which can be a MAC address, a network address, an interface, or some other value, depending on the chassis ID type of the neighboring device.
Port ID type	Port ID type: • **Interface alias**. • **Port component**. • **MAC address**. • **Network address (ipv4)**. • **Interface name**. • **Agent circuit ID**. • **Locally assigned**—Locally-defined port ID type other than those listed above.
Nbr port ID	Value of the type of the port ID.
Nbr system name	System name of the neighboring device.
System description	System description of the neighboring device.
System capabilities supported	Capabilities supported on the neighboring device: • **Repeater**—Signal repeating is supported. • **Bridge**—Switching is supported. • **Router**—Routing is supported. • **Telephone**—The neighboring device can act as a telephone. • **DocsisCableDevice**—The neighboring device can act as a DOCSIS-compliant cable device. • **StationOnly**—The neighboring device can act as a station only. • **Customer Bridge**—The customer bridge feature is enabled. • **Service Bridge**—The service bridge feature is enabled.

Field	Description
	• **TPMR**—The TPMR feature is enabled. • **Other**—Features other than those listed above are supported.
System capabilities enabled	Capabilities enabled on the neighboring device: • **Repeater**—Signal repeating is enabled. • **Bridge**—Switching is enabled. • **Router**—Routing is enabled. • **Telephone**—The neighboring device is acting as a telephone. • **DocsisCableDevice**—The neighboring device is acting as a DOCSIS-compliant cable device. • **StationOnly**—The neighboring device is acting as a station only. • **Customer Bridge**—The customer bridge feature is enabled. • **Service Bridge**—The service bridge feature is enabled. • **TPMR**—The TPMR feature is enabled. • **Other**—Features other than those listed above are supported.
Management address OID	Management address object ID.
Port and protocol VLAN ID(PPVID)	Port and protocol VLAN ID.
Port and protocol VLAN supported	Indicates whether protocol VLAN is supported on the port.
Port and protocol VLAN enabled	Indicates whether protocol VLAN is enabled on the port.
VLAN name of VLAN 12	Name of VLAN 12.
Link aggregation supported	Indicates whether link aggregation is supported.
Link aggregation enabled	Indicates whether link aggregation is enabled.
Aggregation port ID	Member port ID, which is 0 when link aggregation is disabled.
Auto-negotiation supported	Indicates whether autonegotiation is supported on the port.
Auto-negotiation enabled	Indicates whether autonegotiation is enabled on the port.
OperMau	Speed and duplex state on the port.
Power port class	PoE port class: • **PSE**—Power sourcing equipment. • **PD**—Powered device.
PSE power supported	Indicates whether the device can operate as a PSE.
PSE power enabled	Indicates whether the device is operating as a PSE.
PSE pairs control ability	Indicates whether the pair selection ability is available.
Power pairs	Power supply mode: • **Signal**—Uses data pairs to supply power. • **Spare**—Uses spare pairs to supply power.

Field	Description
Port power classification	Power class of the PD: • Class 0. • Class 1. • Class 2. • Class 3. • Class 4.
Power type	Power supply type: • Type 1 PD. • Type 2 PD. • Type 1 PSE. • Type 2 PSE.
Power source	Power source: • When the power supply type is PSE, options are: o **Unknown**—Unknown power supply. o **Primary**—Primary power supply. o **Backup**—Backup power supply. o **Reserved**. • When the power supply type is PD, options are:: o **Unknown**—Unknown power supply. o **PSE**—PSE power supply. o **Local**—Local power supply. o **PSE and local**—PSE and local power supplies.
Power priority	• Unknown. • Critical. • High. • Low.
PD requested power value	PD requested power in watts.
PSE allocated power value	PSE allocated power in watts.
PoE PSE power source	PSE power source type: • **Unknown**—Unknown power supply. • **Primary**—Primary power supply. • **Backup**—Backup power supply.
PoE PD power source	PD power source type: • **Unknown**—Unknown power supply. • **PSE**—PSE power supply. • **Local**—Local power supply. • **PSE and local**—PSE and local power supplies.
Port PSE priority	PoE power supply priority of PSE ports: • Unknown. • Critical. • High. • Low.
Port PD priority	PoE power receiving priority of PD ports: • Unknown. • Critical. • High.

Field	Description
	• Low.
Port available power value	Available PoE power on PSE ports, or power needed on PD ports, in watts.
TLV type	Unknown basic TLV type.
TLV information	Information contained in the unknown basic TLV type.
Unknown organizationally-defined TLV	Unknown organizationally specific TLV.
TLV OUI	OUI of the unknown organizationally specific TLV.
TLV subtype	Unknown organizationally specific TLV subtype.
Index	Unknown organization index.
Capabilities	Capabilities enabled on the neighboring device: • **Repeater**—Signal repeating is enabled. • **Bridge**—Switching is enabled. • **Router**—Routing is enabled. • **Telephone**—The neighboring device is acting as a telephone. • **DocsisCableDevice**—The neighboring device is acting as a DOCSIS-compliant cable device. • **StationOnly**—The neighboring device is acting as a station only. • **Other**—Features other than those listed above are supported. • **None**—The neighboring device does not advertise this TLV.
LocalIf	Local interface on which the LLDP frame was received.
Chassis ID : * -- -- Nearest nontpmr bridge neighbor #-- -- Nearest customer bridge neighbor	Chassis ID flag: • An asterisk (*) indicates the nearest non-TPMR bridge neighbor. • A pound sign (#) indicates the nearest customer bridge neighbor.

15.1.3. display lldp statistics

Use **display lldp statistics** to display the global LLDP statistics or the LLDP statistics of a port.

Syntax

display lldp statistics [**global** | [**interface** *interface-type interface-number*] [**agent** { **nearest-bridge** | **nearest-customer** }]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

global: Displays the global LLDP statistics.

interface *interface-type interface-number*: Specifies a port by its type and number.

agent: Specifies an LLDP agent type. If you do not specify an agent type, the command displays the statistics for all LLDP agents.

nearest-bridge: Specifies nearest bridge agents.

nearest-customer: Specifies nearest customer bridge agents.

Usage guidelines

If you do not specify any keywords or arguments, the command displays the global LLDP statistics and the LLDP statistics of all ports.

Examples

Display the global LLDP statistics and the LLDP statistics of all ports.

```
<Switch> display lldp statistics
LLDP statistics global information:
LLDP neighbor information last change time:0 days, 0 hours, 4 minutes, 40 seconds
The number of LLDP neighbor information inserted : 1
The number of LLDP neighbor information deleted  : 1
The number of LLDP neighbor information dropped  : 0
The number of LLDP neighbor information aged out : 1

LLDP statistics information of port 1 [GigabitEthernet1/0/1]:
LLDP agent nearest-bridge:
The number of LLDP frames transmitted           : 0
The number of LLDP frames received              : 0
The number of LLDP frames discarded             : 0
The number of LLDP error frames                 : 0
The number of LLDP TLVs discarded               : 0
The number of LLDP TLVs unrecognized            : 0
The number of LLDP neighbor information aged out : 0
The number of CDP frames transmitted            : 0
The number of CDP frames received               : 0
The number of CDP frames discarded              : 0
The number of CDP error frames                  : 0

LLDP agent nearest-nontpmr:
The number of LLDP frames transmitted           : 0
The number of LLDP frames received              : 0
The number of LLDP frames discarded             : 0
The number of LLDP error frames                 : 0
The number of LLDP TLVs discarded               : 0
The number of LLDP TLVs unrecognized            : 0
The number of LLDP neighbor information aged out : 0
The number of CDP frames transmitted            : 0
The number of CDP frames received               : 0
The number of CDP frames discarded              : 0
```

```
The number of CDP error frames                  : 0

LLDP agent nearest-customer:
The number of LLDP frames transmitted           : 0
The number of LLDP frames received              : 0
The number of LLDP frames discarded             : 0
The number of LLDP error frames                 : 0
The number of LLDP TLVs discarded               : 0
The number of LLDP TLVs unrecognized            : 0
The number of LLDP neighbor information aged out : 0
The number of CDP frames transmitted            : 0
The number of CDP frames received               : 0
The number of CDP frames discarded              : 0
The number of CDP error frames                  : 0
```

Display the LLDP statistics for the nearest customer bridge agents on GigabitEthernet 1/0/1.

```
<Switch> display lldp statistics interface GigabitEthernet1/0/1 agent nearest-customer
LLDP statistics information of port 1 [GigabitEthernet1/0/1]:
LLDP agent nearest-customer:
The number of LLDP frames transmitted           : 0
The number of LLDP frames received              : 0
The number of LLDP frames discarded             : 0
The number of LLDP error frames                 : 0
The number of LLDP TLVs discarded               : 0
The number of LLDP TLVs unrecognized            : 0
The number of LLDP neighbor information aged out : 0
The number of CDP frames transmitted            : 0
The number of CDP frames received               : 0
The number of CDP frames discarded              : 0
The number of CDP error frames                  : 0
```

Table 15-3 Command output

Field	Description
LLDP statistics global information	Global LLDP statistics.
LLDP neighbor information last change time	Time when the neighbor information was last updated.
The number of LLDP neighbor information inserted	Number of times neighbor information was added.
The number of LLDP neighbor information deleted	Number of times neighbor information was removed.
The number of LLDP neighbor information dropped	Number of times neighbor information was dropped due to lack of available memory space.

15.1.4. display lldp status

Use **display lldp status** to display LLDP status.

Syntax

display lldp status [**interface** *interface-type interface-number*] [**agent** { **nearest-bridge** | **nearest-customer** }]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number. If you do not specify this option, the command displays the global LLDP status and the LLDP status of all ports.

agent: Specifies an LLDP agent type. If you do not specify an agent type, the command displays the status information for all LLDP agents.

nearest-bridge: Specifies nearest bridge agents.

nearest-customer: Specifies nearest customer bridge agents.

Examples

Display the global LLDP status and the LLDP status of each port.

```
<Switch> display lldp status
Global status of LLDP: Enable
Bridge mode of LLDP: customer-bridge
The current number of LLDP neighbors: 5
The current number of CDP neighbors: 0
LLDP neighbor information last changed time: 0 days, 0 hours, 4 minutes, 40 seconds
Transmit interval              : 30s
Fast transmit interval         : 1s
Transmit max credit            : 5
Hold multiplier                : 4
Reinit delay                   : 2s
Trap interval                  : 5s
Fast start times               : 3

LLDP status information of port 1 [GigabitEthernet1/0/1]:
LLDP agent  nearest-bridge:
Port status of LLDP            : Enable
Admin status                   : TX_RX
Trap flag                      : No
MED trap flag                  : No
Polling interval               : 0s
Number of LLDP neighbors       : 5
Number of MED neighbors        : 2
Number of CDP neighbors        : 0
Number of sent optional TLV    : 12
Number of received unknown TLV : 5
```

```
LLDP agent nearest-nontpmr:
Port status of LLDP            : Enable
Admin status                   : TX_RX
Trap flag                      : No
MED trap flag                  : No
Polling interval               : 0s
Number of LLDP neighbors       : 5
Number of MED neighbors        : 2
Number of CDP neighbors        : 0
Number of sent optional TLV    : 12
Number of received unknown TLV : 5

LLDP agent nearest-customer:
Port status of LLDP            : Enable
Admin status                   : TX_RX
Trap flag                      : No
MED trap flag                  : No
Polling interval               : 0s
Number of LLDP neighbors       : 5
Number of MED neighbors        : 2
Number of CDP neighbors        : 0
Number of sent optional TLV    : 12
Number of received unknown TLV : 5
```

Table 15-4 Command output

Field	Description
Bridge mode of LLDP	LLDP bridge mode: service-bridge or customer-bridge.
Global status of LLDP	Indicates whether LLDP is globally enabled.
LLDP neighbor information last changed time	Time when the neighbor information was last updated.
Transmit interval	LLDP frame transmission interval.
Hold multiplier	TTL multiplier.
Reinit delay	LLDP reinitialization delay.
Transmit max credit	Token bucket size for sending LLDP frames.
Trap interval	Trap transmission interval.
Fast start times	Number of LLDP frames sent each time fast LLDP frame transmission is triggered.
Port 1	LLDP status of port 1.
Port status of LLDP	Indicates whether LLDP is enabled on the port.
Admin status	LLDP operating mode of the port: • **TX_RX**—The port can send and receive LLDP frames. • **Rx_Only**—The port can only receive LLDP frames. • **Tx_Only**—The port can only send LLDP frames. • **Disable**—The port cannot send or receive LLDP

Field	Description
	frames.
Trap Flag	Indicates whether trapping is enabled.
Polling interval	LLDP polling interval, which is 0 when LLDP polling is disabled.
Number of neighbors	Number of LLDP neighbors connecting to the port.
Number of MED neighbors	Number of MED neighbors connecting to the port.
Number of CDP neighbors	Number of CDP neighbors connecting to the port.
Number of sent optional TLV	Number of optional TLVs contained in an LLDP frame sent through the port.
Number of received unknown TLV	Number of unknown TLVs contained in a received LLDP frame.

15.1.5. display lldp tlv-config

Use **display lldp tlv-config** to display the types of advertisable optional LLDP TLVs of a port.

Syntax

display lldp tlv-config [**interface** *interface-type interface-number*] [**agent** { **nearest-bridge** | **nearest-customer** }]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number. If you do not specify this option, the command displays the types of advertisable optional TLVs of all ports.

agent: Specifies an LLDP agent type. If you do not specify an agent type, the command displays the types of advertisable optional LLDP TLVs for all LLDP agents.

nearest-bridge: Specifies nearest bridge agents.

nearest-customer: Specifies nearest customer bridge agents.

Examples

Display the types of advertisable optional LLDP TLVs of GigabitEthernet 1/0/1.

```
<Switch> display lldp tlv-config interface gigabitethernet 1/0/1
LLDP tlv-config of port 1[GigabitEthernet1/0/1]:
LLDP agent nearest-bridge:
NAME                              STATUS    DEFAULT
Basic optional TLV:
 Port Description TLV             YES       YES
 System Name TLV                  YES       YES
```

```
 System Description TLV           YES       YES
 System Capabilities TLV          YES       YES
 Management Address TLV           YES       YES
IEEE 802.1 extend TLV:
 Port VLAN ID TLV                 YES       YES
 Port And Protocol VLAN ID TLV    NO        NO
 VLAN Name TLV                    NO        NO
 DCBX TLV                         NO        NO
 EVB TLV                          NO        NO
 Link Aggregation TLV             YES       YES
 Management VID TLV               NO        NO
 Congestion notification TLV      NO        NO
IEEE 802.3 extend TLV:
 MAC-Physic TLV                   YES       YES
 Power via MDI TLV                YES       YES
 Maximum Frame Size TLV           YES       YES
LLDP-MED extend TLV:
 Capabilities TLV                 YES       YES
 Network Policy TLV               YES       YES
 Location Identification TLV      NO        NO
 Extended Power via MDI TLV       YES       YES
 Inventory TLV                    YES       YES

LLDP agent nearest-nontpmr:
NAME                              STATUS    DEFAULT
Basic optional TLV:
 Port Description TLV             NO        NO
 System Name TLV                  NO        NO
 System Description TLV           NO        NO
 System Capabilities TLV          NO        NO
 Management Address TLV           NO        NO
IEEE 802.1 extend TLV:
 Port VLAN ID TLV                 NO        NO
 Port And Protocol VLAN ID TLV    NO        NO
 VLAN Name TLV                    NO        NO
 DCBX TLV                         NO        NO
 EVB TLV                          YES       YES
 Link Aggregation TLV             NO        NO
 Management VID TLV               NO        NO
 Congestion notification TLV      NO        NO
IEEE 802.3 extend TLV:
 MAC-Physic TLV                   NO        NO
 Power via MDI TLV                NO        NO
 Maximum Frame Size TLV           NO        NO
LLDP-MED extend TLV:
 Capabilities TLV                 NO        NO
 Network Policy TLV               NO        NO
 Location Identification TLV      NO        NO
```

```
 Extended Power via MDI TLV       NO        NO
 Inventory TLV                    NO        NO

LLDP agent nearest-customer:
NAME                              STATUS    DEFAULT
Basic optional TLV:
 Port Description TLV             YES       YES
 System Name TLV                  YES       YES
 System Description TLV           YES       YES
 System Capabilities TLV          YES       YES
 Management Address TLV           YES       YES
IEEE 802.1 extend TLV:
 Port VLAN ID TLV                 YES       YES
 Port And Protocol VLAN ID TLV    NO        NO
 VLAN Name TLV                    NO        NO
 DCBX TLV                         NO        NO
 EVB TLV                          NO        NO
 Link Aggregation TLV             YES       YES
 Management VID TLV               NO        NO
 Congestion notification TLV      NO        NO
IEEE 802.3 extend TLV:
 MAC-Physic TLV                   NO        NO
 Power via MDI TLV                NO        NO
 Maximum Frame Size TLV           NO        NO
LLDP-MED extend TLV:
 Capabilities TLV                 NO        NO
 Network Policy TLV               NO        NO
 Location Identification TLV      NO        NO
 Extended Power via MDI TLV       NO        NO
 Inventory TLV                    NO        NO
```

Table 15-5 Command output

Field	Description
LLDP tlv-config of port 1	Advertisable optional TLVs of port 1.
NAME	TLV type.
STATUS	Indicates whether the type of TLV is sent through a port.
DEFAULT	Indicates whether the type of TLV is sent through a port by default.
Basic optional TLV	Basic optional TLVs: • Port Description TLV. • System Name TLV. • System Description TLV. • System Capabilities TLV. • Management Address TLV. • Congestion notification TLV. The device does not support congestion notification TLVs in the current software version.

Field	Description
IEEE 802.1 extended TLV	IEEE 802.1 organizationally specific TLVs: • Port VLAN ID TLV. • Port and protocol VLAN ID TLV. • VLAN name TLV. • DCBX TLV. The device does not support DCBX TLVs in the current software version. • EVB TLV. • Management VID TLV.
IEEE 802.3 extended TLV	IEEE 802.3 organizationally specific TLVs: • MAC-Physic TLV. • Power via MDI TLV. • Link aggregation TLV. • Maximum frame size TLV.
LLDP-MED extend TLV	LLDP-MED TLVs: • Capabilities TLV. • Network Policy TLV. • Extended Power-via-MDI TLV. • Location Identification TLV. • Inventory TLV.
Inventory TLV	Inventory TLVs: • Hardware Revision TLV. • Firmware Revision TLV. • Software Revision TLV. • Serial Number TLV. • Manufacturer Name TLV. • Model name TLV. • Asset ID TLV.

15.1.6. lldp admin-status

Use **lldp admin-status** to set the LLDP operating mode.

Use **undo lldp admin-status** to restore the default.

Syntax

In Layer 2/Layer 3 Ethernet interface view or management Ethernet interface view:

lldp [**agent nearest-customer**] **admin-status** { **disable** | **rx** | **tx** | **txrx** }

undo lldp [**agent nearest-customer** }] **admin-status**

In Layer 2 aggregate interface view:

lldp agent nearest-customer admin-status { **disable** | **rx** | **tx** | **txrx** }

undo lldp agent nearest-customer admin-status

In IRF physical interface view:

lldp admin-status { **disable** | **rx** | **tx** | **txrx** }

undo lldp admin-status

Default

The nearest bridge agent operates in **TxRx** mode, and the nearest customer bridge agent operate in **Disable** mode.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Management Ethernet interface view

Layer 2 aggregate interface view

IRF physical interface view

Predefined user roles

network-admin

Parameters

agent: Specifies an LLDP agent type. If you do not specify an agent type in Ethernet or management Ethernet interface view, the command sets the operating mode for nearest bridge agents.

nearest-customer: Specifies nearest customer bridge agents.

disable: Specifies the **Disable** mode. A port in this mode cannot send or receive LLDP frames.

rx: Specifies the **Rx** mode. A port in this mode can only receive LLDP frames.

tx: Specifies the **Tx** mode. A port in this mode can only send LLDP frames.

txrx: Specifies the **TxRx** mode. A port in this mode can send and receive LLDP frames.

Usage guidelines

In IRF physical interface view, only nearest bridge agents are supported.

Examples

Set the LLDP operating mode to **Rx** for the nearest customer bridge agents on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] lldp agent nearest-customer admin-status rx
```

15.1.7. lldp check-change-interval

Use **lldp check-change-interval** to enable LLDP polling and set the polling interval.

Use **undo lldp check-change-interval** to disable LLDP polling.

Syntax

In Layer 2/Layer 3 Ethernet interface view or management Ethernet interface view:

lldp [**agent nearest-customer**] **check-change-interval** *interval*

undo lldp [**agent nearest-customer**] **check-change-interval**

In Layer 2 aggregate interface view:

lldp agent nearest-customer check-change-interval *interval*

undo lldp agent nearest-customer check-change-interval

In IRF physical interface view:

lldp check-change-interval *interval*

undo lldp check-change-interval

Default

LLDP polling is disabled.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Management Ethernet interface view

Layer 2 aggregate interface view

IRF physical interface view

Predefined user roles

network-admin

Parameters

agent: Specifies an LLDP agent type. If you do not specify an agent type in Ethernet or management Ethernet interface view, the command enables LLDP polling and sets the polling interval for nearest bridge agents.

nearest-customer: Specifies nearest customer bridge agents.

interval: Sets the LLDP polling interval in the range of 1 to 30 seconds.

Examples

Enable LLDP polling and set the polling interval to 30 seconds for the nearest customer bridge agents on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] lldp agent nearest-customer check-change-interval 30
```

15.1.8. lldp compliance admin-status cdp

Use **lldp compliance admin-status cdp** to set the operating mode of CDP-compatible LLDP.

Use **undo lldp compliance admin-status cdp** to restore the default.

Syntax

lldp compliance admin-status cdp { **disable** | **txrx** }

undo lldp compliance admin-status cdp

Default

CDP-compatible LLDP operates in **Disable** mode.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Management Ethernet interface view

Predefined user roles

network-admin

Parameters

disable: Specifies the **Disable** mode. CDP-compatible LLDP in this mode cannot receive or transmit CDP packets.

txrx: Specifies the **TxRx** mode. CDP-compatible LLDP in this mode can send and receive CDP packets.

Usage guidelines

For your device to work with Cisco IP phones, you must perform the following tasks:

- Enable CDP-compatible LLDP globally.
- Configure CDP-compatible LLDP to operate in TxRx mode on the specified ports.

Examples

Enable CDP-compatible LLDP globally and configure CDP-compatible LLDP to operate in **TxRx** mode on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] lldp compliance cdp
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] lldp compliance admin-status cdp txrx
```

Related commands

lldp compliance cdp

15.1.9. lldp compliance cdp

Use **lldp compliance cdp** to enable CDP compatibility.

Use **undo lldp compliance cdp** to disable CDP compatibility.

Syntax

lldp compliance cdp

undo lldp compliance cdp

Default

CDP compatibility is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

The maximum TTL that CDP allows is 255 seconds. To make CDP-compatible LLDP work correctly with Cisco IP phones, set the LLDP frame transmission interval to be no more than 1/3 of the TTL value.

Examples

Enable CDP compatibility.

```
<Switch> system-view
```

```
[Switch] lldp compliance cdp
```

Related commands

lldp hold-multiplier

lldp timer tx-interval

15.1.10. lldp enable

Use **lldp enable** to enable LLDP on a port.

Use **undo lldp enable** to disable LLDP on a port.

Syntax

lldp enable

undo lldp enable

Default

LLDP is enabled on a port.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Management Ethernet interface view

Layer 2 aggregate interface view

IRF physical interface view

Predefined user roles

network-admin

Usage guidelines

LLDP takes effect on a port only when LLDP is enabled both globally and on the port.

Examples

Disable LLDP on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] undo lldp enable
```

Related commands

lldp global enable

15.1.11. lldp encapsulation snap

Use **lldp encapsulation snap** to set the encapsulation format for LLDP frames to SNAP.

Use **undo lldp encapsulation** to restore the default.

Syntax

In Layer 2/Layer 3 Ethernet interface view or management Ethernet interface view:

lldp [**agent nearest-customer**] **encapsulation snap**

undo lldp [**agent nearest-customer**] **encapsulation**

In Layer 2 aggregate interface view:

lldp agent nearest-customer encapsulation snap

undo lldp agent nearest-customer encapsulation

In IRF physical interface view:

lldp encapsulation snap

undo lldp encapsulation

Default

The encapsulation format for LLDP frames is Ethernet II.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Management Ethernet interface view

Layer 2 aggregate interface view

IRF physical interface view

Predefined user roles

network-admin

Parameters

agent: Specifies an LLDP agent type. If you do not specify an agent type in Ethernet or management Ethernet interface view, the command sets the LLDP frame encapsulation format for nearest bridge agents.

nearest-customer: Specifies nearest customer bridge agents.

Usage guidelines

LLDP-CDP packets use only SNAP encapsulation.

Examples

Set the encapsulation format for LLDP frames to SNAP on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] lldp encapsulation snap
```

15.1.12. lldp fast-count

Use **lldp fast-count** to set the number of LLDP frames sent each time fast LLDP frame transmission is triggered.

Use **undo lldp fast-count** to restore the default.

Syntax

lldp fast-count *count*

undo lldp fast-count

Default

Four LLDP frames are sent each time fast LLDP frame transmission is triggered.

Views

System view

Predefined user roles

network-admin

Parameters

count: Sets the number of LLDP frames sent each time fast LLDP frame transmission is triggered. The value range is 1 to 8.

Examples

Configure the device to send five LLDP frames each time fast LLDP frame transmission is triggered.

```
<Switch> system-view
[Switch] lldp fast-count 5
```

15.1.13. lldp global enable

Use **lldp global enable** to enable LLDP globally.

Use **undo lldp global enable** to disable LLDP globally.

Syntax

lldp global enable

undo lldp global enable

Default

LLDP is disabled globally.

Views

System view

Predefined user roles

network-admin

Usage guidelines

LLDP takes effect on a port only when LLDP is enabled both globally and on the port.

Examples

Disable LLDP globally.

```
<Switch> system-view
[Switch] undo lldp global enable
```

Related commands

lldp enable

15.1.14. lldp hold-multiplier

Use **lldp hold-multiplier** to set the TTL multiplier.

Use **undo lldp hold-multiplier to** restore the default.

Syntax

lldp hold-multiplier *value*

undo lldp hold-multiplier

Default

The TTL multiplier is 4.

Views

System view

Predefined user roles

network-admin

Parameters

value: Sets the TTL multiplier in the range of 2 to 10.

Usage guidelines

The TTL TLV carried in an LLDPDU determines how long the device information carried in the LLDPDU can be saved on a recipient device.

By setting the TTL multiplier, you can set the TTL of locally sent LLDP frames. The TTL is expressed by using the following formula:

TTL = Min (65535, (TTL multiplier × LLDP frame transmission interval + 1))

As the expression shows, the TTL can be up to 65535 seconds.

Examples

Set the TTL multiplier to 6.

```
<Switch> system-view
[Switch] lldp hold-multiplier 6
```

Related commands

lldp timer tx-interval

15.1.15. lldp management-address

Use **lldp management-address** to enable the device to generate an ARP or ND entry after receiving an LLDP frame that carries a management address TLV.

Use **undo lldp management-address** to restore the default.

Syntax

lldp management-address { **arp-learning** | **nd-learning** } [**vlan** *vlan-id*]

undo lldp management-address { **arp-learning** | **nd-learning** }

Default

The device does not generate an ARP or ND entry after receiving an LLDP frame that carries a management address TLV.

Views

Layer 3 Ethernet interface view

Default command level

network-admin

Parameters

arp-learning: Generates an ARP entry if the received management address TLV contains an IPv4 address.

nd-learning: Generates an ND entry if the received management address TLV contains an IPv6 address.

vlan *vlan-id*: Specifies a VLAN ID in the range of 1 to 4094. Include this option in the command to generate the ARP or ND entry for the Layer 3 Ethernet subinterface identified by *interface-number.subnumber,* where *subnumber* is the specified VLAN ID. If the Layer 3 Ethernet subinterface does not exist or if this option is not specified, the device generates the entry for the Layer 3 Ethernet interface.

Usage guidelines

You can enable the device to generate both ARP entries and ND entries.

Examples

Configure GigabitEthernet 1/0/1 to generate an ARP entry after receiving an LLDP frame carrying an IPv4 management address TLV.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] lldp management-address arp-learning
```

NOTE:

`nd-learning` option is not supported in the current software version.

15.1.16. lldp management-address-format string

Use **lldp management-address-format string** to set the encoding format of the management address to string.

Use **undo lldp management-address-format** to restore the default.

Syntax

In Layer 2/Layer 3 Ethernet interface view/management Ethernet interface view:

lldp [**agent nearest-customer**] **management-address-format string**

undo lldp [**agent nearest-customer**] **management-address-format**

In Layer 2 aggregate interface view:

lldp agent nearest-customer management-address-format string

undo lldp agent nearest-customer management-address-format

Default

The encoding format of the management address is numeric.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Management Ethernet interface view

Predefined user roles

network-admin

Parameters

agent: Specifies an LLDP agent type. If you do not specify an agent type in Ethernet or management Ethernet interface view, the command sets the encoding format of the management address for nearest bridge agents.

nearest-customer: Specifies nearest customer bridge agents.

Usage guidelines

LLDP neighbors must use the same encoding format for the management address.

The device supports only the numeric encoding format for IPv6 management addresses.

Examples

Set the encoding format of the management address to string for the nearest customer bridge agents on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] lldp agent nearest-customer management-address-format
string
```

15.1.17. lldp notification remote-change enable

Use **lldp notification remote-change enable** to enable LLDP trapping.

Use **undo lldp notification remote-change enable** to disable LLDP trapping.

Syntax

In Layer 2/Layer 3 Ethernet interface view/management Ethernet interface view:

lldp [**agent nearest-customer**] **notification remote-change enable**

undo lldp [**agent nearest-customer**] **notification remote-change enable**

In Layer 2 aggregate interface view:

lldp agent nearest-customer notification remote-change enable

undo lldp agent nearest-customer notification remote-change enable

In IRF physical interface view:

lldp notification remote-change enable

undo lldp notification remote-change enable

Default

LLDP trapping is disabled.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Management Ethernet interface view

Layer 2 aggregate interface view

IRF physical interface view

Predefined user roles

network-admin

Parameters

agent: Specifies an LLDP agent type. If you do not specify an agent type in Ethernet or management Ethernet interface view, the command enables LLDP trapping for nearest bridge agents.

nearest-customer: Specifies nearest customer bridge agents.

Examples

Enable LLDP trapping for the nearest customer bridge agent on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface GigabitEthernet 1/0/1
[Switch-GigabitEthernet1/0/1] lldp agent nearest-customer notification remote-change
enable
```

15.1.18. lldp timer notification-interval

Use **lldp timer notification-interval** to set the LLDP trap and LLDP-MED trap transmission interval.

Use **undo lldp timer notification-interval** to restore the default.

Syntax

lldp timer notification-interval *interval*

undo lldp timer notification-interval

Default

The LLDP trap and LLDP-MED trap transmission interval is 30 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Sets the LLDP trap and LLDP-MED trap transmission interval in the range of 5 to 3600 seconds.

Examples

Set both the LLDP trap and LLDP-MED trap transmission interval to 8 seconds.

```
<Switch> system-view
[Switch] lldp timer notification-interval 8
```

15.1.19. lldp timer reinit-delay

Use **lldp timer reinit-delay** to set the LLDP reinitialization delay.

Use **undo lldp timer reinit-delay** to restore the default.

Syntax

lldp timer reinit-delay *delay*

undo lldp timer reinit-delay

Default

The LLDP reinitialization delay is 2 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

delay: Sets the LLDP reinitialization delay in the range of 1 to 10 seconds.

Examples

Set the LLDP reinitialization delay to 4 seconds.

```
<Switch> system-view
[Switch] lldp timer reinit-delay 4
```

15.1.20. lldp timer tx-interval

Use **lldp timer tx-interval** to set the LLDP frame transmission interval.

Use **undo lldp timer tx-interval** to restore the default.

Syntax

lldp timer tx-interval *interval*

undo lldp timer tx-interval

Default

The LLDP frame transmission interval is 30 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Sets the LLDP frame transmission interval in the range of 1 to 32768 seconds.

Examples

Set the LLDP frame transmission interval to 20 seconds.

```
<Switch> system-view
[Switch] lldp timer tx-interval 20
```

15.1.21. lldp tlv-enable

Use **lldp tlv-enable** to configure the types of advertisable TLVs on a port.

Use **undo lldp tlv-enable** to disable the advertising of the specified types of TLVs on a port.

Syntax

In Layer 2 Ethernet interface view:

- For nearest bridge agents:

  lldp tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [*ip-address*] } | **dot1-tlv** { **all** | **port-vlan-id** | **link-aggregation** | **protocol-vlan-id** [*vlan-id*] | **vlan-name** [*vlan-id*] | **management-vid** [*mvlan-id*] } | **dot3-tlv** { **all** | **mac-physic** | **max-frame-size** | **power** } | **med-tlv** { **all** | **capability** | **inventory** | **network-policy** [*vlan-id*] | **power-over-ethernet** | **location-id** { **civic-address** *device-type country-code* { *ca-type ca-value* }&<1-10> | **elin-address** *tel-number* } } }

  undo lldp tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [*ip-address*] } | **dot1-tlv** { **all** | **port-vlan-id** | **link-aggregation** | **protocol-vlan-id** | **vlan-name** | **management-vid** } | **dot3-tlv** { **all** | **mac-physic** | **max-frame-size** | **power** } | **med-tlv** { **all** | **capability** | **inventory** | **network-policy** [*vlan-id*] | **power-over-ethernet** | **location-id** } }

- For nearest customer bridge agents:

  lldp agent nearest-customer tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [*ip-address*] } | **dot1-tlv** { **all** | **port-vlan-id** | **link-aggregation** } }

  undo lldp agent nearest-customer tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [*ip-address*] } | **dot1-tlv** { **all** | **port-vlan-id** | **link-aggregation** } }

In Layer 3 Ethernet interface view:

lldp tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [*ip-address*] } | **dot1-tlv** { **all** | **link-aggregation** } | **dot3-tlv** { **all** | **mac-physic** | **max-frame-size** | **power** } | **med-tlv** { **all** | **capability** | **inventory** | **power-over-ethernet** | **location-id** { **civic-address** *device-type country-code* { *ca-type ca-value* }&<1-10> | **elin-address** *tel-number* } } }

lldp agent nearest-customer tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [*ip-address*] } | **dot1-tlv** { **all** | **link-aggregation** } }

undo lldp tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [*ip-address*] } | **dot1-tlv** { **all** | **link-aggregation** } | **dot3-tlv** { **all** | **mac-physic** | **max-frame-size** | **power** } | **med-tlv** { **all** | **capability** | **inventory** | **power-over-ethernet** | **location-id** } }

undo lldp agent nearest-customer tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [*ip-address*] } | **dot1-tlv** { **all** | **link-aggregation** } }

In management Ethernet interface view:

lldp tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [*ip-address*] } | **dot1-tlv** { **all** | **link-aggregation** } | **dot3-tlv** { **all** | **mac-physic** | **max-frame-size** | **power** } | **med-tlv** { **all** | **capability** | **inventory** |

power-over-ethernet | **location-id** { **civic-address** *device-type country-code* { *ca-type ca-value* }&<1-10> | **elin-address** *tel-number* } } }

lldp agent nearest-customer tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [*ip-address*] } | **dot1-tlv** { **all** | **link-aggregation** } }

undo lldp tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [*ip-address*] } | **dot1-tlv** { **all** | **link-aggregation** } | **dot3-tlv** { **all** | **mac-physic** | **max-frame-size** | **power** } | **med-tlv** { **all** | **capability** | **inventory** | **power-over-ethernet** | **location-id** } }

undo lldp agent nearest-customer tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [*ip-address*] } | **dot1-tlv** { **all** | **link-aggregation** } }

In Layer 2 aggregate interface view:

lldp agent nearest-customer tlv-enable { **basic-tlv** { **all** | **management-address-tlv** [*ip-address*] | **port-description** | **system-capability** | **system-description** | **system-name** } | **dot1-tlv** { **all** | **port-vlan-id** } }

lldp tlv-enable dot1-tlv { **protocol-vlan-id** [*vlan-id*] | **vlan-name** [*vlan-id*] | **management-vid** [*mvlan-id*] }

undo lldp agent nearest-customer tlv-enable { **basic-tlv** { **all** | **management-address-tlv** [*ip-address*] | **port-description** | **system-capability** | **system-description** | **system-name** } | **dot1-tlv** { **all** | **port-vlan-id** } }

undo lldp tlv-enable dot1-tlv { **protocol-vlan-id** | **vlan-name** | **management-vid** }

In IRF physical interface view:

lldp tlv-enable basic-tlv { **port-description** | **system-capability** | **system-description** | **system-name** }

undo lldp tlv-enable basic-tlv { **port-description** | **system-capability** | **system-description** | **system-name** }

Default

On Layer 2 Ethernet interfaces:

- Nearest bridge agents can advertise all types of LLDP TLVs except the following types:
  - Location identification TLVs.
  - Port and protocol VLAN ID TLVs.
  - VLAN name TLVs.
  - Management VLAN ID TLVs.
- Nearest customer bridge agents can advertise basic TLVs and IEEE 802.1 organizationally specific TLVs.

On Layer 3 Ethernet interfaces or management Ethernet interfaces:

- Nearest bridge agents can advertise all types of LLDP TLVs except network policy TLVs. Among all the 802.1 organizationally specific TLVs, only the link aggregation TLV is supported.

- Nearest customer bridge agents can advertise basic TLVs and IEEE 802.1 organizationally specific TLVs (only link aggregation TLV is supported).

On management Ethernet interfaces:

- Nearest bridge agents can advertise all types of LLDP TLVs except network policy TLVs. Among all the 802.1 organizationally specific TLVs, only the link aggregation TLV is supported.
- Nearest customer bridge agents can advertise basic TLVs and IEEE 802.1 organizationally specific TLVs (only link aggregation TLV is supported).

On Layer 2 aggregate interfaces:

- Nearest customer bridge agents can advertise basic TLVs and IEEE 802.1 organizationally specific TLVs. Among the IEEE 802.1 organizationally specific TLVs, only port and protocol VLAN ID TLVs, VLAN name TLVs, and management VLAN ID TLVs are supported.

IRF physical interfaces support all available types of TLVs.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Management Ethernet interface view

Layer 2 aggregate interface view

IRF physical interface view

Predefined user roles

network-admin

Parameters

agent: Specifies an LLDP agent type. If you do not specify an agent type in Ethernet or management Ethernet interface view, the command configures the types of advertisable TLVs for nearest bridge agents.

nearest-customer: Specifies nearest customer bridge agents.

all: Advertises all TLVs of the specified type. This keyword enables the interface to advertise following TLVs:

- All basic LLDP TLVs if the **all** keyword is specified for **basic-tlv**.
- All IEEE 802.1 organizationally specific LLDP TLVs if the **all** keyword is specified for **dot1-tlv**.
- All IEEE 802.3 organizationally specific LLDP TLVs if the **all** keyword is specified for **dot3-tlv**.
- All LLDP-MED TLVs except location identification TLVs if the **all** keyword is specified for **med-tlv**.

basic-tlv: Advertises basic LLDP TLVs.

management-address-tlv [*ip-address*]: Advertises management address TLVs. The *ip-address* argument specifies the management address to be advertised. By default, the following rules apply:

- When you execute the **lldp tlv-enable** command:
  - For a Layer 2 Ethernet or aggregate interface, the management address is the IPv4 address of the VLAN interface that meets the following requirements:
    - In up state.
    - The corresponding VLAN ID is the lowest among the VLANs permitted on the port.

If none of the VLAN interfaces of the permitted VLANs is assigned an IPv4 address or all VLAN interfaces are down, the MAC address of the port will be advertised.

- For a Layer 3 Ethernet interface, the IPv4 address of the port will be advertised when the following conditions exist:
  - The *ip-address* argument is not configured.
  - The specified loopback interface does not have an IPv4 address, or the specified loopback interface does not exist.

  If the port does not have an IPv4 address, the MAC address of the port will be advertised.

- When you execute the **undo lldp tlv-enable** command for a Layer 2/Layer 3 Ethernet interface, management Ethernet interface, or Layer 2 aggregate interface:
  - If you do not specify *ip-address*, the port does not advertise any management address TLVs.
  - If you specify *ip-address*, the port advertises the default management address TLVs.

port-description: Advertises port description TLVs.

system-capability: Advertises system capabilities TLVs.

system-description: Advertises system description TLVs.

system-name: Advertises system name TLVs.

dot1-tlv: Advertises IEEE 802.1 organizationally specific LLDP TLVs.

port-vlan-id: Advertises port VLAN ID TLVs.

protocol-vlan-id [*vlan-id*]: Advertises port and protocol VLAN ID TLVs. The *vlan-id* argument specifies a VLAN ID in the TLVs to be advertised. The VLAN ID is in the range of 1 to 4094, and the default is the lowest VLAN ID on the port.

vlan-name [*vlan-id*]: Advertises VLAN name TLVs. The *vlan-id* argument specifies a VLAN ID in the TLVs to be advertised. The VLAN ID is in the range of 1 to 4094, and the default is the lowest VLAN ID on the port. If you do not specify a VLAN ID and the port is not assigned to any VLAN, the PVID of the port is advertised.

management-vid [*mvlan-id*]: Advertises management VLAN ID TLVs. The *mvlan-id* argument specifies a management VLAN ID in the TLVs to be advertised. The management VLAN ID is in the range of 1 to 4094. If you do not specify this option, the value 0 is advertised, which means that the LLDP agent is not configured with a management VLAN ID.

dot3-tlv: Advertises IEEE 802.3 organizationally specific LLDP TLVs.

link-aggregation: Advertises link aggregation TLVs.

mac-physic: Advertises MAC/PHY configuration/status TLVs.

max-frame-size: Advertises maximum frame size TLVs.

power: Advertises power in MDI TLVs and power stateful control TLVs.

med-tlv: Advertises LLDP-MED TLVs.

capability: Advertises LLDP-MED capabilities TLVs.

inventory: Advertises the following TLVs: hardware revision, firmware revision, software revision, serial number, manufacturer name, model name, and asset ID.

location-id: Advertises location identification TLVs.

civic-address: Inserts the typical address information about the network device in location identification TLVs .

device-type: Sets a device type value in the range of 0 to 2:

- Value 0 specifies a DHCP server.
- Value 1 specifies a network device.
- Value 2 specifies an LLDP-MED endpoint.

country-code: Sets a country code defined in ISO 3166.

{ *ca-type ca-value* }&<1-10>: Configures address information. *ca-type* represents the address information type in the range of 0 to 255. *ca-value* represents address information, a string of 1 to 250 characters. &<1-10> indicates that you can specify up to 10 *ca-type ca-value* pairs.

elin-address: Inserts telephone numbers for emergencies in location identification TLVs.

tel-number: Sets the telephone number for emergencies, a string of 10 to 25 characters.

network-policy [*vlan-id*]: Advertises network policy TLVs. The *vlan-id* argument specifies the voice VLAN ID to be advertised, in the range of 1 to 4094.

power-over-ethernet: Advertises extended power-via-MDI TLVs.

Usage guidelines

Nearest bridge agents are not supported on aggregate interfaces.

You can enable the device to advertise multiple types of TLVs by using this command without the **all** keyword specified.

If the MAC/PHY configuration/status TLV is not advertisable, none of the LLDP-MED TLVs will be advertised whether or not they are advertisable. If the LLDP-MED capabilities TLV is not advertisable, the other LLDP-MED TLVs will not be advertised regardless of whether or not they are advertisable.

The port and protocol VLAN ID, VLAN name, and management VLAN ID TLVs in IEEE 802.1 organizationally specific LLDP TLVs can be configured only for nearest bridge agents. The configuration can be inherited by nearest customer bridge agents and nearest non-TPMR bridge agents.

Examples

Enable the nearest customer bridge agents on GigabitEthernet 1/0/1 to advertise link aggregation TLVs of the IEEE 802.1 organizationally specific TLVs.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] lldp agent nearest-customer tlv-enable dot1-tlv
link-aggregation
```

Contents

A page of this section is **3-x-x**

16. L2PT commands 16-1
16.1. L2PT commands 16-1
16.1.1. display l2protocol statistics 16-1
16.1.2. l2protocol tunnel dot1q 16-2
16.1.3. l2protocol tunnel-dmac 16-4
16.1.4. reset l2protocol statistics 16-4

16. L2PT commands

16.1. L2PT commands

16.1.1. display l2protocol statistics

Use **display l2protocol statistics** to display Layer 2 Protocol Tunneling (L2PT) statistics.

Syntax

display l2protocol statistics [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies a Layer 2 Ethernet or aggregate interface by its type and number. If you do not specify this option, the command displays L2PT statistics for all Layer 2 Ethernet and aggregate interfaces.

Examples

Display L2PT statistics for all Layer 2 Ethernet and aggregate interfaces.

```
<Switch> display l2protocol statistics
L2PT statistics information on interface Bridge-Aggregation1:
Protocol  Encapsulated      Decapsulated      Forwarded         Dropped
CDP       0                 0                 0                 0
DLDP      0                 3                 0                 0
EOAM      0                 2                 0                 0
GVRP      8                 4                 9                 2
LACP      0                 0                 0                 0
LLDP      0                 3                 0                 0
MVRP      0                 0                 0                 0
PAGP      0                 1                 0                 0
PVST      0                 0                 0                 0
STP       5                 5                 5                 0
Tunnel    N/A               N/A               100               10
VTP       0                 6                 0                 0
UDLD      0                 0                 0                 0

L2PT statistics information on interface GigabitEthernet1/0/1:
Protocol  Encapsulated      Decapsulated      Forwarded         Dropped
CDP       0                 0                 0                 0
DLDP      2                 3                 3                 0
```

```
EOAM        5                 2                 9                 0
GVRP        8                 4                 9                 2
LACP        0                 0                 0                 0
LLDP        3                 3                 3                 3
MVRP        0                 0                 0                 0
PAGP        5                 1                 7                 3
PVST        0                 0                 0                 0
STP         5                 5                 5                 0
Tunnel      N/A               N/A               100               10
VTP         0                 6                 0                 0
UDLD        0                 0                 0                 0
```

Table 16-1 Command output

Field	Description
Encapsulated	Number of encapsulated packets. The number increases by 1 when the interface receives and encapsulates a protocol packet from a customer network. For protocol **Tunnel**, which represents tunneled packets, this field displays **N/A**.
Decapsulated	Number of decapsulated packets. The number increases by 1 when the interface receives and decapsulates a tunneled packet from the service provider network. For protocol **Tunnel**, which represents tunneled packets, this field displays **N/A**.
Forwarded	Number of forwarded packets. The number increases by 1 when the interface receives a protocol packet and forwards it. The number increases by 1 for protocol **Tunnel** when the interface receives a tunneled packet and forwards it. If no interface of the PE is connected to customer networks, the number does not increase.
Dropped	Number of dropped packets. The number increases by 1 when the interface receives a protocol packet and drops it. Protocol packets dropped by hardware are not counted. The number increases by 1 for protocol **Tunnel** when the interface receives a tunneled packet and drops it.

16.1.2. l2protocol tunnel dot1q

Use **l2protocol tunnel dot1q** to enable L2PT for a protocol.

Use **undo l2protocol tunnel dot1q** to disable L2PT for a protocol.

Syntax

In Layer 2 Ethernet interface view:

l2protocol { **cdp** | **dldp** | **eoam** | **gvrp** | **lacp** | **lldp** | **mvrp** | **pagp** | **pvst** | **stp** | **udld** | **vtp** } **tunnel dot1q**

undo l2protocol { **cdp** | **dldp** | **eoam** | **gvrp** | **lacp** | **lldp** | **mvrp** | **pagp** | **pvst** | **stp** | **udld** | **vtp** } **tunnel dot1q**

In Layer 2 aggregate interface view:

MEMO:

cdp , **lacp** , **lldp** , **pagp** , **udld** option is supported from later software, including Version 7.2.23. Version 7.3.21 does not support the above options.

l2protocol { **cdp** | **lacp** | **lldp** | **gvrp** | **mvrp**| **pagp** | **pvst** | **stp** | **udld** | **vtp** } **tunnel dot1q**

undo l2protocol { **cdp** | **lacp** | **lldp** | **gvrp** | **mvrp**| **pagp** | **pvst** | **stp** | **udld** | **vtp** } **tunnel dot1q**

Default

L2PT is disabled for all protocols.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

cdp: Specifies CDP.

dldp: Specifies DLDP.

eoam: Specifies EOAM.

gvrp: Specifies GVRP.

lacp: Specifies LACP.

lldp: Specifies LLDP. L2PT for LLDP supports LLDP packets from only nearest bridge agents.

mvrp: Specifies MVRP.

pagp: Specifies PAgP.

pvst: Specifies PVST.

stp: Specifies STP.

udld: Specifies UDLD.

vtp: Specifies VTP.

Usage guidelines

Before you enable L2PT for a protocol on a port, perform the following tasks:

- Enable the protocol on the CE, and disable the protocol on the port.
- Enable L2PT only on customer-facing PE ports. If you enable L2PT on ports connected to the service provider network, L2PT determines that the ports are connected to a customer network.

Do not enable L2PT on a port that is going to join a service loopback group. All configuration is removed after the port joins the group.

You can enable L2PT on member ports of a Layer 2 aggregation group, but the configuration does not take effect.

The **l2protocol tunnel dot1q** command and the **l2protocol drop** command overwrite each other.

Examples

Disable STP and enable L2PT for STP on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] undo stp enable
[Switch-GigabitEthernet1/0/1] l2protocol stp tunnel dot1q
```

Disable STP and enable L2PT for STP on Bridge-Aggregation 1.

```
<Switch> system-view
[Switch] interface bridge-aggregation 1
[Switch-Bridge-Aggregation1] undo stp enable
[Switch-Bridge-Aggregation1] l2protocol stp tunnel dot1q
```

Related commands

l2protocol drop

16.1.3. l2protocol tunnel-dmac

Use **l2protocol tunnel-dmac** to set the destination multicast MAC address for tunneled packets.

Use **undo l2protocol tunnel-dmac** to restore the default.

Syntax

l2protocol tunnel-dmac *mac-address*

undo l2protocol tunnel-dmac

Default

The tunneled packets use 010f-e200-0003 as the destination multicast MAC address.

Views

System view

Predefined user roles

network-admin

Parameters

mac-address: Specifies a destination multicast MAC address. The available addresses are 0100-0ccd-cdd0, 0100-0ccd-cdd1, 0100-0ccd-cdd2, and 010f-e200-0003.

Examples

Set the destination multicast MAC address to 0100-0ccd-cdd0 for tunneled packets.

```
<Switch> system-view
[Switch] l2protocol tunnel-dmac 0100-0ccd-cdd0
```

16.1.4. reset l2protocol statistics

Use **reset l2protocol statistics** to clear L2PT statistics.

Syntax

reset l2protocol statistics [**interface** *interface-type interface-number*]

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies a Layer 2 Ethernet or aggregate interface by its type and number. If you do not specify this option, the command clears L2PT statistics on all Layer 2 Ethernet and aggregate interfaces.

Examples

Clear L2PT statistics on all Layer 2 Ethernet and aggregate interfaces.

```
<Switch> reset l2protocol statistics
```

Contents

A page of this section is 3-x-x

17. M-LAG commands 17-1
17.1. M-LAG commands 17-1
17.1.1. display m-lag consistency-check status 17-1
17.1.2. display m-lag drcp statistics 17-2
17.1.3. display m-lag keepalive 17-4
17.1.4. display m-lag mad verbose 17-6
17.1.5. display m-lag role 17-8
17.1.6. display m-lag summary 17-10
17.1.7. display m-lag system 17-12
17.1.8. display m-lag troubleshooting 17-14
17.1.9. display m-lag verbose 17-15
17.1.10. m-lag auto-recovery reload-delay 17-18
17.1.11. m-lag drcp period short 17-19
17.1.12. m-lag keepalive { ip | ipv6 } 17-19
17.1.13. m-lag keepalive interval 17-21
17.1.14. m-lag mad default-action 17-21
17.1.15. m-lag mad exclude interface 17-23
17.1.16. m-lag mad exclude logical-interfaces 17-24
17.1.17. m-lag mad include interface 17-25
17.1.18. m-lag mad persistent 17-26
17.1.19. m-lag mad restore 17-27
17.1.20. m-lag restore-delay 17-27
17.1.21. m-lag role priority 17-28
17.1.22. m-lag standalone enable 17-29
17.1.23. m-lag system-mac 17-30
17.1.24. m-lag system-number 17-31
17.1.25. m-lag system-priority 17-32
17.1.26. port m-lag group 17-32
17.1.27. port m-lag peer-link 17-33
17.1.28. port m-lag virtual-ip 17-34

17. M-LAG commands

NOTE:

This function is supported on Ver7.4.37 and later.

When used in combination with UNIVERGE Network Operation Engine Overlay Network Extension, this function is supported on Ver7.4.30 and later.

17.1. M-LAG commands

17.1.1. display m-lag consistency-check status

Use **display m-lag consistency-check status** to display the configuration consistency check status.

Syntax

display m-lag consistency-check status

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display the configuration consistency check status.

```
<Sysname> display m-lag consistency-check status
              Global Consistency Check Configuration
Local status     : Enabled          Peer status     : Enabled
Local check mode : Strict           Peer check mode : Strict

              Consistency Check on Modules
Module          Type1          Type2
LAGG            Check          Check
VLAN            Check          Check
STP             Check          Check
MAC             Not Check      Check
L2VPN           Not Check      Check

              Type1 Consistency Check Result
Global consistency check result: SUCCESS
Inconsistent global modules: -

M-LAG interface    M-LAG group ID    Check Result     Inconsistency modules
BAGG4              4                 SUCCESS          -
```

Table 17-1 Command output

Field	Description
Local status	Status of configuration consistency check at the local end: • **Enabled**. • **Disabled**.
Peer status	Status of configuration consistency check at the peer end: • **Enabled**. • **Disabled**.
Local check mode	Configuration consistency check mode at the local end: • **Loose**. • **Strict**.
Peer check mode	Configuration consistency check mode at the peer end: • **Loose**. • **Strict**.
Module	Feature module name.
Type1	Whether M-LAG checks the module for a type 1 configuration inconsistency: • **Check**. • **Not Check**.
Type2	Whether M-LAG checks the module for a type 2 configuration inconsistency: • **Check**. • **Not Check**.
Global consistency check result	Result of global configuration consistency check: • **FAILURE**. • **SUCCESS**.
Inconsistent global modules	Modules that failed global configuration consistency check. If the check succeeded, this field displays a hyphen (**-**).
M-LAG interface	Abbreviated name of the M-LAG interface.
Inconsistency modules	Modules that failed interface configuration consistency check. If the check succeeded, this field displays a hyphen (**-**).

17.1.2. display m-lag drcp statistics

Use **display m-lag drcp statistics** to display DRCPDU statistics.

Syntax

display m-lag drcp statistics [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies a Layer 2 aggregate interface or VXLAN tunnel interface by its type and number. If you do not specify this option, the command displays the DRCPDU statistics about the M-LAG peer-link interface and all M-LAG interfaces.

Examples

Display DRCPDU statistics.

```
<Sysname> display m-lag drcp statistics
 * indicates the port is the M-LAG peer-link interface .
Interface type:
BAGG -- Bridge-Aggregation, Tun -- Tunnel
Interface     State     Sent     Received(Normal/Error/Unknown)
*BAGG3        UP        30       26/0/0
 BAGG4        UP        29       26/0/0
```

Display DRCPDU statistics about Bridge-Aggregation 4.

```
<Sysname> display m-lag drcp statistics interface bridge-aggregation 4
* indicates the port is the M-LAG peer-link interface .
Interface type:
BAGG -- Bridge-Aggregation, Tun -- Tunnel
Interface  : BAGG4
State      : UP
Sent       : 31
Received (Normal/Error/Unknown): 28/0/0
Last received packet information:
  Source MAC address: 3cd4-437d-0300
  Time: 2019/09/11 09:19:58
  Action: Accept
```

Table 17-2 Command output

Field	Description
Interface	Abbreviated interface name. The name of the M-LAG peer-link interface is prefixed with an asterisk (*).
State	Physical state of the interface: • **UP**. • **DOWN**.
Sent	Number of sent DRCPDUs.
Received (Normal/Error/Unknown)	Numbers of received normal, error, and unrecognized DRCPDUs.
Last received packet information	Information about the most recently received DRCPDU.

Field	Description
Time	Date and time when the DRCPDU was received, in the YYYY/MM/DD hh:mm:ss format.
Action	Action taken on the DRCPDU: • **Accept**. • **Drop**. If the DRCPDU was dropped, this field also displays the reason for dropping the DRCPDU.

Related commands

reset m-lag drcp statistics

17.1.3. display m-lag keepalive

Use **display m-lag keepalive** to display M-LAG keepalive packet statistics.

Syntax

display m-lag keepalive

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display M-LAG keepalive packet statistics.

```
<Sysname> display m-lag keepalive
Neighbor keepalive link status (cause): Up
Neighbor is alive for: 135642 s 501 ms
Keepalive packet transmission status:
  Sent: Successful
  Received: Successful
Last received keepalive packet information:
  Source IP address: 1.1.1.1
  Time: 2019/09/11 09:21:51
  Action: Accept

Distributed relay keepalive parameters:
Destination IP address: 10.0.0.2
Source IP address: 10.0.0.1
Keepalive UDP port : 6400
Keepalive VPN name : vpn1
Keepalive interval : 1000 ms
Keepalive timeout  : 5 sec
Keepalive hold time: 3 sec
```

Table 17-3 Command output

Field	Description
Neighbor keepalive link status (cause)	State of the M-LAG peer: • **Unknown**—No M-LAG peer is detected because the destination IP address of keepalive packets is not specified. • **Up**—The M-LAG peer is up. • **Down**—The M-LAG peer is down. Cause of the keepalive link down event: • **M-LAG system init**—M-LAG system initialization. • **Local IP not configured**—The local end does not have source and destination IP address settings for the keepalive link. • **Local Tx failed**—Packet transmission failed on the local end. • **Local Rx timeou**t—Packet reception timed out on the local end. • **Peer Rx timeout**—Packet reception timed out on the peer end.
Neighbor is alive for	Time period for which the M-LAG peer has been up.
Last received keepalive packet information	Information about the most recently received keepalive packet.
Time	Date and time when the keepalive packet was received, in the YYYY/MM/DD hh:mm:ss format. If the device has not received any keepalive packets, this field displays **N/A**.
Action	Action taken on the keepalive packet: • **Accept**. • **Drop**. If the keepalive packet was dropped, this field also displays the reason for dropping the packet.
Destination IP address	Destination IP address of keepalive packets sent by the device.
Source IP address	Source IP address of keepalive packets sent by the device.
Keepalive UDP port	Destination UDP port of keepalive packets.
Keepalive VPN name	VPN instance for keepalive packets. If no VPN instance is configured for keepalive packets, this field displays **N/A**.
Keepalive interval	Interval at which the device sends keepalive packets.
Keepalive timeout	Keepalive timeout timer.
Keepalive hold time	Keepalive hold timer setting. The keepalive hold timer specifies the amount of time that the device uses to identify the cause of an

Field	Description
	M-LAG peer-link down event.

Related commands

m-lag keepalive { **ip** | **ipv6** }

m-lag keepalive hold-time

m-lag keepalive interval

17.1.4. display m-lag mad verbose

Use **display m-lag mad verbose** to display detailed M-LAG MAD information.

Syntax

display m-lag mad verbose

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display detailed M-LAG MAD information.

```
<Sysname> display m-lag mad verbose
M-LAG MAD DOWN state    : No
Restore delay         : 30 s
Remaining restore delay: -
M-LAG MAD default action: DOWN
M-LAG MAD DOWN persistence: Disabled
Excluding logical interfaces: Disabled
Port configuration for M-LAG MAD DOWN action:
 Included ports(user-configured):
   Bridge-Aggregation1
   GigabitEthernet1/0/5(ineffective)
 Included ports(system-configured):
   Member interfaces of M-LAG Bridge-Aggregation3:
     GigabitEthernet 1/0/3
 Excluded ports(user-configured):
   Bridge-Aggregation2
   GigabitEthernet1/0/4
 Excluded ports(system-configured):
   Management interfaces:
     M-GigabitEthernet0/0/0
   M-LAG interfaces:
     Bridge-Aggregation4
   M-LAG peer-link interface :
     Bridge-Aggregation3
```

```
Member interfaces of M-LAG peer-link interface  Bridge-Aggregation3:
  GigabitEthernet1/0/1
  GigabitEthernet1/0/2
```

Table 17-4 Command output

Field	Description
M-LAG MAD DOWN state	Whether the network interfaces on the device are in M-LAG MAD DOWN state: • **Yes**—The device has network interfaces placed in M-LAG MAD DOWN state. • **No**—No network interfaces are in M-LAG MAD DOWN state. If this field displays **Yes**, check the M-LAG peer-link for the link down issue to remove multi-active collision.
Restore delay	Data restoration interval, in seconds.
Remaining restore delay	The remaining time (in seconds) before the data restoration interval expires. If the data restoration interval has not started, this field displays a hyphen (**-**).
M-LAG MAD default action	Default action to take on network interfaces when the M-LAG system splits: • **DOWN**—Shut down interfaces and place them in M-LAG MAD DOWN state. • **NONE**—M-LAG MAD does not take action on interfaces.
M-LAG MAD DOWN persistence	M-LAG MAD DOWN state persistence: • **Enabled**—The M-LAG member device does not bring up the network interfaces in M-LAG MAD DOWN state when its role changes from secondary to primary. • **Disabled**—The M-LAG member device brings up the network interfaces in M-LAG MAD DOWN state when its role changes from secondary to primary.
Excluding logical interfaces	Whether all logical interfaces are excluded from the shutdown action by M-LAG MAD: • **Enabled**. • **Disabled**.
Included ports(user-configured)	Network interfaces manually configured to be shut down by M-LAG MAD when the M-LAG system splits. An interface entry will be marked as ineffective if the system does not allow the specified interface to be shut down by M-LAG MAD. M-LAG MAD will not shut down interfaces in ineffective entries when the M-LAG system splits. The following are interfaces not allowed to be shut down by M-LAG MAD: • Interfaces automatically excluded from being shut down by M-LAG MAD. • Interfaces manually or automatically excluded from being shut down by IRF MAD.

Field	Description
	• Interfaces used for special purposes.
Included ports(system-configured)	Network interfaces automatically set by the system to shut down by M-LAG MAD when the M-LAG system splits. Aggregation member ports of M-LAG interfaces are in this category of interfaces.
Excluded ports(user-configured)	Network interfaces manually configured to not be shut down by M-LAG MAD. An interface entry will be marked as ineffective if the specified interface is in the list of ports excluded by the system from the M-LAG MAD shutdown action. In this situation, the manual configuration does not take effect.
Excluded ports(system-configured)	Network interfaces set by the system to not shut down by M-LAG MAD, including: • **Management interfaces**. • **M-LAG interfaces.** • **M-LAG peer-link interface** . • Aggregation member interfaces if a Layer 2 aggregate interface is used as the M-LAG peer-link interface .

Related commands

m-lag mad default-action

m-lag mad exclude logical-interfaces

m-lag mad exclude interface

m-lag mad include interface

m-lag mad persistent

17.1.5. display m-lag role

Use **display m-lag role** to display M-LAG role information.

Syntax

display m-lag role

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display M-LAG role information.

```
<Sysname> display m-lag role
                 Effective role information
Factors              Local                Peer
Effective role        Primary              Secondary
```

```
Initial role           None                 None
MAD DOWN state         Yes                  Yes
Health level           0                    0
Role priority          32768                32768
Bridge MAC             3cd4-3ce1-0200       3cd4-437d-0300
Effective role trigger: M-LAG peer-link calculation
Effective role reason: Bridge MAC

                Configured role information
Factors              Local                Peer
Configured role      Primary              Secondary
Role priority        32768                32768
Bridge MAC           3cd4-3ce1-0200       3cd4-437d-0300
```

Table 17-5 Command output

Field	Description
Factors	Factors used in role calculation.
Local	Local configuration.
Peer	Peer configuration.
Effective role	Effective device role: • **None**. • **Primary**. • **Secondary**.
Initial role	Device role before role calculation: • **None**. • **Primary**. • **Secondary**.
MAD DOWN state	Whether there were interfaces in M-LAG MAD DOWN state during role calculation: • **Yes**. • **No**. This field displays **N/A** if no peer exists.
Health level	Health level of the device during role calculation. The member device with a lower value is healthier. This field displays **N/A** if no peer exists.
Effective role trigger	Why effective role calculation was triggered: • **M-LAG system init**—M-LAG system initialization. • **M-LAG peer-link down and all local M-LAG interfaces down**—The M-LAG peer-link and all local M-LAG interfaces went down. • **M-LAG peer-link down and all peer M-LAG interfaces down**—The M-LAG peer-link and all peer M-LAG interfaces went down. • **M-LAG peer-link and keepalive link down**—Both the M-LAG peer-link and

Field	Description
	keepalive link went down. • **M-LAG peer-link calculation**—The local device role was calculated over the M-LAG peer-link. • **M-LAG peer-link down and role calculation based on keepalive link**—The M-LAG peer-link went down, and the local device role was calculated over the keepalive link.
Effective role reason	Factor that determined the effective device role: • No peer existed. In this situation, a hyphen (-) is displayed. • Single None role. One M-LAG member device had the None role, and the other M-LAG member device had the Primary role. • MAD status. • Health level. • Role priority. • Bridge MAC.
Configured role	Manually assigned device role: • **None**. • **Primary**. • **Secondary**.

Related commands

m-lag role priority

17.1.6. display m-lag summary

Use **display m-lag summary** to display summary information about the M-LAG peer-link interface and M-LAG interfaces.

Syntax

display m-lag summary

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display summary information about the M-LAG peer-link interface and M-LAG interfaces. In this example, global configuration consistency check was successful.

```
<Sysname> display m-lag summary
Flags: A -- Aggregate interface down, B -- No peer M-LAG interface configured
       C -- Configuration consistency check failed
```

```
M-LAG peer-link interface : BAGG3
M-LAG peer-link interface  state (cause): UP
Keepalive link state (cause): UP

                  M-LAG interface information
M-LAG interface  M-LAG group  Local state (cause)  Peer state  Remaining down time(s)
BAGG4        4        UP                UP         -
```

Table 17-6 Command output

Field	Description
M-LAG peer-link interface	Abbreviated name of the M-LAG peer-link interface .
M-LAG peer-link interface state (cause)	State of the M-LAG peer-link interface : • **UP**. • **DOWN**. If the M-LAG peer-link interface is down, this field also displays the cause of the down state.
Keepalive link state (cause)	State of the keepalive link: • **UP**. • **DOWN**. Cause of the keepalive link down event: • **M-LAG system init**—M-LAG system initialization. • **Local IP not configured**—The local end does not have source and destination IP address settings for the keepalive link. • **Local Tx failed**—Packet transmission failed on the local end. • **Local Rx timeou**t—Packet reception timed out on the local end. • **Peer Rx timeout**—Packet reception timed out on the peer end.
M-LAG interface	Name of the M-LAG interface.
Local state (cause)	State of the M-LAG interface: • **UP**. • **DOWN**. If the M-LAG interface is down, this field also displays the cause of the down state: • **A**—The aggregate interface went down. • **B**—The peer M-LAG interface did not exist. • **C**—Configuration consistency check failed.
Peer state	State of the peer M-LAG interface: • **UP**. • **DOWN**—No peer M-LAG interface exists or the peer M-LAG interface is down.

Field	Description
	• **UNKNOWN**—The state of the peer M-LAG interface is unknown when the M-LAG peer-link is down.
Remaining down time (s)	Remaining time (in seconds) during which the M-LAG interface will stay in M-LAG MAD DOWN state. If the M-LAG interface is not in M-LAG MAD DOWN state, this field displays a hyphen (-).

17.1.7. display m-lag system

Use **display m-lag system** to display the M-LAG system settings.

Syntax

display m-lag system

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display the M-LAG system settings.

```
<Sysname> display m-lag system
                  System information
Local system number: 1                  Peer system number: 2
Local system MAC: 0001-0001-0001          Peer system MAC: 0001-0001-0001
Local system priority: 123               Peer system priority: 123
Local bridge MAC: 3cd4-3ce1-0200          Peer bridge MAC: 3cd4-437d-0300
Local effective role: Primary             Peer effective role: Secondary
Health level: 0
Standalone mode on split: Enabled
In standalone mode: Yes

                  System timer information
Timer                   State      Value (s)    Remaining time (s)
Auto recovery            Disabled    -            -
Restore delay            Disabled    30           -
Consistency-check delay    Disabled    15           -
Standalone delay          Disabled    -            -
Role to None delay        Disabled    60           -
```

Table 17-7 Command output

Field	Description
Local system number	Local M-LAG system number. If the parameter is not configured, this field

Field	Description
	displays **N/A**.
Peer system number	Peer M-LAG system number. If the parameter is not configured or the peer does not exist, this field displays **N/A**.
Local system MAC	Local M-LAG system MAC address. If the parameter is not configured, this field displays **N/A**.
Peer system MAC	Peer M-LAG system MAC address. If the parameter is not configured or the peer does not exist, this field displays **N/A**.
Local system priority	Local M-LAG system priority. If the parameter is not configured, this field displays **N/A**.
Peer system priority	Peer M-LAG system priority. If the parameter is not configured or the peer does not exist, this field displays **N/A**.
Local bridge MAC	Local bridge MAC address.
Peer bridge MAC	Peer bridge MAC address. If the peer does not exist, this field displays **N/A**.
Local effective role	Effective role of the local device: • **None**. • **Primary**. • **Secondary**.
Peer effective role	Effective role of the peer device: • **None**. • **Primary**. • **Secondary**.
Health level	Health level of the device. The member device with a lower value is healthier.
Standalone mode on split	Whether M-LAG standalone mode is enabled: • **Enabled**. • **Disabled**.
In standalone state	Whether the device is in M-LAG standalone mode: • **Yes**. • **No**.
Timer	Timer type: • **Auto recovery**—Reload delay timer. • **Restore delay**—Data restoration interval. • **Consistency check delay**—Configuration consistency check delay timer. • **Standalone delay**—Delay that the device must wait before changing to M-LAG standalone mode. • **Role to None delay**—Delay that the device must wait before setting its role

Field	Description
	to None.
State	State of the timer: • **Enabled**. • **Disabled**.
Value (s)	Value of the timer, in seconds.
Remaining time (s)	Remaining time of the timer, in seconds. If the timer has not started, this field displays a hyphen (**-**).

17.1.8. display m-lag troubleshooting

Use **display m-lag troubleshooting** to display M-LAG troubleshooting information.

Syntax

display m-lag troubleshooting [**m-lag** | **peer-link** | **keepalive**] [**history**] [*count*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

m-lag: Displays M-LAG interface troubleshooting information.

peer-link: Displays M-LAG peer-link interface troubleshooting information.

keepalive: Displays keepalive link troubleshooting information.

history: Displays troubleshooting records. If you do not specify this keyword, the command displays current troubleshooting information.

count: Specifies the number of events to display, in the range of 1 to 200. If you do not specify this argument, the command displays the most recent 20 events.

Usage guidelines

If you do not specify the **m-lag-interface**, **peer-link**, or **keepalive** keywords, this command displays troubleshooting information about M-LAG interfaces, the M-LAG peer-link interface , and the keepalive link.

Examples

Display M-LAG troubleshooting records.

```
<Sysname> display m-lag troubleshooting history
Total: 3

Time                    Event description
2019-09-10 14:13:53.103  M-LAG peer-link interface  BAGG10 went down because the M-LAG
peer-link interface  role of the
                        interface was removed. Please reconfigure an interface
```

```
                    as the M-LAG peer-link interface .
2019-09-10 14:23:53.102  Keepalive link went down because the peer keepalive
                    timeout timer expired. Please check the keepalive
                    packet transmission and reception status at the two
                    ends.
2019-09-10 14:53:53.103  Local M-LAG interface state of BAGG1024 in M-LAG group 1024
                    changed to down because the aggregate interface went
                    down. Please check the aggregate link status.
```

Related commands

reset m-lag troubleshooting history

17.1.9. display m-lag verbose

Use **display m-lag verbose** to display detailed information about the M-LAG peer-link interface and M-LAG interfaces.

Syntax

display m-lag verbose [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies a M-LAG interface or the M-LAG peer-link interface by its number. The interface number must already exist. If you do not specify an interface, the command displays detailed information about the M-LAG peer-link interface and all M-LAG interfaces.

Usage guidelines

If the specified interface is not the M-LAG peer-link interface or a M-LAG interface, no information is displayed.

Examples

Display detailed information about M-LAG interface Bridge-Aggregation 1.

```
<Sysname> display m-lag verbose interface bridge-aggregation 1
Flags: A -- Home_Gateway, B -- Neighbor_Gateway, C -- Other_Gateway,
      D -- M-LAG peer-link interface _Activity, E -- DRCP_Timeout, F -- Gateway_Sync,
      G -- Port_Sync, H -- Expired

M-LAG interface/M-LAG group ID: BAGG1/1
Local M-LAG interface state: UP
Peer M-LAG interface state: UP
M-LAG group state: UP
Local M-LAG interface down cause: -
Remaining M-LAG DOWN time: -
Local M-LAG interface LACP MAC: Config=0001-0001-0001, Effective=0001-0001-0001
```

```
Peer M-LAG interface LACP MAC: Config=0001-0001-0001, Effective=0001-0001-0001
Local M-LAG interface LACP priority: Config=200, Effective=200
Peer M-LAG interface LACP priority: Config=200, Effective=200
Local DRCP flags/Peer DRCP flags: ABDFG/ABDFG
Local Selected ports (index): GE1/0/1 (260), GE1/0/2 (261)
Peer Selected ports indexes: 260, 261
```

Display detailed information about M-LAG peer-link interface Bridge-Aggregation 2.

```
<Sysname> display m-lag verbose interface bridge-aggregation 2
Flags: A -- Home_Gateway, B -- Neighbor_Gateway, C -- Other_Gateway,
      D -- M-LAG peer-link interface _Activity, E -- DRCP_Timeout, F -- Gateway_Sync,
      G -- Port_Sync, H -- Expired

M-LAG peer-link interface /M-LAG peer-link interface  ID: BAGG2/1
State: UP
Cause: -
Local DRCP flags/Peer DRCP flags: ABDFG/ABDFG
Local Selected ports (index): GE1/0/1 (258), GE1/0/2 (259)
Peer Selected ports indexes: 258, 259
```

Table 17-8 Command output

Field	Description
Flags	DRCP state flags. The flag field is one byte long, represented by ABCDEFGH from the lowest bit to the highest bit. A letter is displayed when its bit is 1 and is not displayed when its bit is 0. • **A**—Indicates whether DRCP is enabled on the local device. 1 indicates enabled. 0 indicates disabled. • **B**—Indicates whether DRCP is enabled on the M-LAG peer. 1 indicates enabled. 0 indicates disabled. • **C**—Indicates whether DRCP is enabled on a third M-LAG member device. 1 indicates enabled. 0 indicates disabled. • **D**—Indicates whether the local M-LAG peer-link interface has determined that DRCP is enabled on the M-LAG peer. 1 indicates yes. 0 indicates no. • **E**—Indicates the DRCP timeout timer. 1 indicates the short timeout timer. 0 indicates the long timeout timer. • **F**—Indicates whether the local M-LAG peer-link interface permits the packets that contain the negotiated gateway conversation IDs. 1 indicates yes. 0 indicates no. • **G**—Indicates whether the local M-LAG peer-link interface permits the packets that contain the negotiated port conversation IDs. 1 indicates yes. 0 indicates no. • **H**—Indicates whether the local DRCPDU receive machine is in default

Field	Description
	or expired state. 1 indicates yes. 0 indicates no.
M-LAG peer-link interface	Abbreviated name of the M-LAG peer-link interface .
M-LAG interface	Abbreviated name of the M-LAG interface.
Local M-LAG interface state	State of the local M-LAG interface: • **UP**—The M-LAG interface is up if it has Selected ports in its aggregation group. • **DOWN**—The M-LAG interface is down if it does not have Selected ports in its aggregation group.
Peer M-LAG interface state	State of the peer M-LAG interface: • **UP**—The M-LAG interface is up if it has Selected ports in its aggregation group. • **DOWN**—The M-LAG interface is down if it does not have Selected ports in its aggregation group. • **UNKNOWN**—The state of the peer M-LAG interface is unknown when the M-LAG peer-link is down.
M-LAG group state	State of the M-LAG group: • **UP**—The M-LAG group is up if it contains a minimum of one member M-LAG interface in UP state. • **DOWN**—The M-LAG group is down if it all its member M-LAG interfaces are in DOWN state.
Local M-LAG interface down cause	Cause of the down state of the local M-LAG interface. If the local M-LAG interface is up, this field displays a hyphen (**-**).
Remaining M-LAG DOWN time	Remaining time (in seconds) during which the M-LAG interface will stay in M-LAG MAD DOWN state. If the M-LAG interface is not in M-LAG MAD DOWN state, this field displays a hyphen (**-**).
State	State of the M-LAG peer-link interface : • **UP**. • **DOWN**.
Cause	Cause of the down state of the M-LAG peer-link interface . If the M-LAG peer-link interface is up, this field displays a hyphen (**-**).
Config	Configured value.
Effective	Effective value.
Local DRCP flags	Local DRCP state flags. If all bits are set to 0, this field displays **Unknown**.
Peer DRCP flags	Peer DRCP state flags. If all bits are set to 0 or no peer exists, this field displays **Unknown**.
Local Selected ports (index)	Abbreviated name of the Selected ports in

Field	Description
	the local aggregation group and their port indexes.
Peer Selected ports indexes	Port indexes of the Selected ports in the peer aggregation group.

17.1.10. m-lag auto-recovery reload-delay

Use **m-lag auto-recovery reload-delay** to enable M-LAG system auto-recovery and set the reload delay timer.

Use **undo m-lag auto-recovery reload-delay** to restore the default.

Syntax

m-lag auto-recovery reload-delay *delay-value*

undo m-lag auto-recovery reload-delay

Default

M-LAG system auto-recovery is disabled and the reload delay timer is not set.

Views

System view

Predefined user roles

network-admin

Parameters

delay-value: Specifies a reload delay in the range of 240 to 3600 seconds.

Usage guidelines

If only one M-LAG member device recovers after the entire M-LAG system reboots, auto-recovery enables that member device to remove its M-LAG interfaces from the M-LAG DOWN interface list.

- If that member device has up M-LAG interfaces, it takes over the primary role when the reload delay timer expires and forwards traffic.
- If that member device does not have up M-LAG interfaces, it is stuck in the None role and does not forward traffic.

If auto-recovery is disabled, that M-LAG member device will be stuck in the None role with all its M-LAG interfaces being M-LAG DOWN after it recovers.

If both M-LAG member devices recover and have up M-LAG interfaces after the entire M-LAG system reboots, active-active situation might occur if both M-LAG peer link and keepalive links were down when the reload delay timer expires. If this rare situation occurs, examine the M-LAG peer link and keepalive links and restore them.

To avoid incorrect role preemption, make sure the reload delay timer is longer than the amount of time required for the device to restart.

Examples

Enable M-LAG system auto-recovery and set the reload delay timer to 245 seconds.

```
<Sysname> system-view
[Sysname] m-lag auto-recovery reload-delay 245
```

Related commands

display m-lag role

17.1.11. m-lag drcp period short

Use **m-lag drcp period short** to enable the short DRCP timeout timer (3 seconds) on the M-LAG peer-link interface or a M-LAG interface.

Use **undo m-lag drcp period** to restore the default.

Syntax

m-lag drcp period short

undo m-lag drcp period

Default

An aggregate interface uses the long DRCP timeout timer (90 seconds).

Views

Layer 2 aggregate interface view

VXLAN tunnel interface view

Predefined user roles

network-admin

Usage guidelines

This command takes effect only on the M-LAG peer-link interface or a M-LAG interface.

DRCP uses a timeout mechanism to specify the amount of time that an M-LAG peer-link interface or M-LAG interface must wait to receive DRCPDUs before it determines that the peer interface is down. This timeout mechanism provides the following timer options:

- Short DRCP timeout timer, which is fixed at 3 seconds. If this timer is used, the peer interface sends one DRCPDU every second.
- Long DRCP timeout timer, which is fixed at 90 seconds. If this timer is used, the peer interface sends one DRCPDU every 30 seconds.

Short DRCP timeout timer enables the M-LAG member devices to detect a peer interface down event more quickly than the long DRCP timeout timer. However, this benefit is at the expense of bandwidth and system resources.

To avoid traffic interruption during an ISSU or M-LAG process restart, disable the short DRCP timeout timer before you perform an ISSU or M-LAG process restart. For more information about ISSU, see *Fundamentals Configuration Guide*.

Examples

Enable the short DRCP timeout timer on Bridge-Aggregation 1.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] m-lag drcp period short
```

17.1.12. m-lag keepalive { ip | ipv6 }

Use **m-lag keepalive** { **ip** | **ipv6** } to configure M-LAG keepalive packet parameters.

Use **undo m-lag keepalive** { **ip** | **ipv6** } to restore the default.

Syntax

m-lag keepalive { **ip** | **ipv6** } **destination** { *ipv4-address* | *ipv6-address* } [**source** { *ipv4-address* | *ipv6-address* } | **udp-port** *udp-number* | **vpn-instance** *vpn-instance-name*] *

undo m-lag keepalive { **ip** | **ipv6** }

Default

No keepalive packet parameters are configured.

Views

System view

Predefined user roles

network-admin

Parameters

ip: Specifies IPv4 addresses.

ipv6: Specifies IPv6 addresses.

destination: Specifies an IP address of the M-LAG peer as the destination IP address of keepalive packets.

source: Specifies a local IP address as the source IP address of keepalive packets. If you do not specify a source IP address, the IP address of the outgoing interface is used.

ipv4-address: Specifies an IPv4 address.

ipv6-address: Specifies an IPv6 address.

udp-port *udp-number*: Specifies the destination UDP port of keepalive packets. The value range for the *udp-number* argument is 1 to 65535. If you do not specify a UDP port number, 6400 is used.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If the keepalive packets belong to the public network, do not specify a VPN instance.

Usage guidelines

The device accepts only keepalive packets that are sourced from the specified destination IP address. The keepalive link goes down if the device receives keepalive packets sourced from any other IP addresses.

Make sure the M-LAG member devices in a M-LAG system use the same keepalive destination UDP port.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify the destination and source IP addresses of keepalive packets as 192.168.68.125 and 192.168.68.100, respectively.

```
<Sysname> system-view
[Sysname] m-lag keepalive ip destination 192.168.68.125 source 192.168.68.100
```

Related commands

display m-lag keepalive

17.1.13. m-lag keepalive interval

Use **m-lag keepalive interval** to set the M-LAG keepalive interval and timeout timer.

Use **undo m-lag keepalive interval** to restore the default.

Syntax

m-lag keepalive interval *interval* [**timeout** *timeout*]

undo m-lag keepalive interval

Default

The M-LAG keepalive interval is 1000 milliseconds, and the M-LAG keepalive timeout timer is 5 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

interval *interval*: Specifies the keepalive interval, in the range of 100 to 10000 milliseconds.

timeout *timeout*: Specifies the keepalive timeout timer, in the range of 3 to 20 seconds. The local keepalive timeout timer must be two times the keepalive interval of the peer at minimum.

Usage guidelines

The device sends keepalive packets at the specified interval to its M-LAG peer. If the device has not received a keepalive packet from the M-LAG peer before the keepalive timeout timer expires, the device determines that the keepalive link is down.

You must configure the same M-LAG keepalive interval on the M-LAG member devices in a M-LAG system.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the M-LAG keepalive interval and timeout timer to 2000 milliseconds and 6 seconds, respectively.

```
<Sysname> system-view
[Sysname] m-lag keepalive interval 2000 timeout 6
Changing the keepalive interval might cause system setup failure. Continue? [Y/N]:y
```

Related commands

display m-lag keepalive

17.1.14. m-lag mad default-action

Use **m-lag mad default-action** to configure the default M-LAG MAD action to take on network interfaces on the secondary M-LAG member device when the M-LAG system splits.

Use **undo m-lag mad default-action** to restore the default.

Syntax

m-lag mad default-action { **down** | **none** }

undo m-lag mad default-action

Default

M-LAG MAD shuts down network interfaces on the secondary M-LAG member device.

Views

System view

Predefined user roles

network-admin

Parameters

down: Sets the action to M-LAG MAD DOWN. M-LAG MAD will shut down all network interfaces on the secondary M-LAG member device when the M-LAG system splits, except the interfaces excluded manually or by the system.

none: Sets the M-LAG MAD action to NONE. M-LAG MAD will not shut down any network interfaces when the M-LAG system splits, except the interfaces configured manually or by the system to be shut down by M-LAG MAD.

Usage guidelines

In most network environments, use the M-LAG MAD DOWN action in conjunction with the **m-lag mad exclude interface** command.

- The M-LAG MAD DOWN action helps avoid network issues caused by multi-active collision, which occurs if the M-LAG peer-link goes down while the keepalive link is up.
- The **m-lag mad exclude interface** command enables you to exclude special-purpose interfaces, for example, interfaces used in M-LAG for M-LAG keepalive detection.

This configuration method is inefficient if a large number of interfaces on the secondary M-LAG member must be retained in up state after the M-LAG system splits. For example, if you use a VXLAN tunnel as the M-LAG peer-link in an EVPN environment, you must retain a large number of logical interfaces (for example, tunnel and loopback interfaces) in up state.

In these situations, use the following method to configure M-LAG MAD:

- Set the default M-LAG MAD action to NONE.
- Execute the **m-lag mad include interface** command to specify interfaces that must be shut down by M-LAG MAD in addition to those already automatically specified by the system.

The M-LAG MAD DOWN action will not take effect on the following interfaces:

- Interfaces automatically or manually excluded from being shut down by M-LAG MAD. To identify these interfaces, execute the **display m-lag mad verbose** command.
- Interfaces automatically or manually excluded from being shut down by IRF MAD. To identify these interfaces, execute the **display mad verbose** command.
- Interfaces used for special purposes, including:
  - Interfaces placed in a loopback test by using the **loopback** command.
  - Interfaces in a mirroring group.
  - Interfaces forced to stay up by using the **port-up mode** command.

Examples

Configure M-LAG MAD to shut down all network interfaces except excluded interfaces when the M-LAG system splits.

```
<Sysname> system-view
[Sysname] m-lag mad default-action down
```

Related commands

display m-lag mad verbose

display mad (*Virtual Technologies Command Reference*)

m-lag mad exclude logical-interfaces

m-lag mad exclude interface

m-lag mad include interface

loopback (*Interface Command Reference*)

mirroring-group reflector-port (*Network Management and Monitoring Command Reference*)

port up-mode (*Interface Command Reference*)

17.1.15. m-lag mad exclude interface

Use **m-lag mad exclude interface** to add an interface to the user-configured list of excluded ports, which will not be shut down by M-LAG MAD when the M-LAG system splits.

Use **undo m-lag mad exclude interface** to remove an interface from the user-configured list of excluded ports.

Syntax

m-lag mad exclude interface *interface-type interface-number*

undo m-lag mad exclude interface *interface-type interface-number*

Default

M-LAG MAD shuts down all network interfaces when detecting a multi-active collision, except for the network interfaces set by the system to not shut down.

Views

System view

Predefined user roles

network-admin

Parameters

interface-type interface-number: Specifies an interface by its type and number.

Usage guidelines

This command is typically used when the default M-LAG MAD action is set to M-LAG MAD DOWN. In this situation, when M-LAG MAD detects a multi-active collision, M-LAG sets all network interfaces on the secondary M-LAG member device to M-LAG MAD DOWN state, except for the following interfaces:

- Network interfaces excluded from the shutdown action by IRF MAD.
- Network interfaces manually configured to not shut down by M-LAG MAD.
- Network interfaces set by the system to not shut down by M-LAG MAD, including:
  - Peer-Link.
  - Aggregation member interfaces if a Layer 2 aggregate interface is used as the Peer-Link.
  - M-LAG interfaces.
  - Management interfaces.

You must exclude the following interfaces from the shutdown action by M-LAG MAD:

- For correct keepalive detection, you must exclude the interfaces used for keepalive detection from the shutdown action.
- For M-LAG member devices to synchronize ARP entries, you must exclude the VLAN interfaces of the VLANs to which the M-LAG interfaces and Peer-Link belong from the shutdown action.
- If the Peer-Link is a tunnel interface, you must exclude the traffic outgoing interface for the tunnel from the shutdown action. To view the traffic outgoing interface for a tunnel, use the **display fib** *ip-address* or **display ip routing-table** *ip-address* command. To view the destination address of a tunnel, use the **display interface tunnel** command.

Examples

Exclude GigabitEthernet 1/0/1 from the shutdown action by M-LAG MAD.

```
<Sysname> system-view
[Sysname] m-lag mad exclude interface gigabitethernet 1/0/1
```

Related commands

display m-lag mad verbose

display fib (*Layer 3—IP Services Command Reference*)

display interface tunnel (*Layer 3—IP Services Command Reference*)

display ip routing-table (*Layer 3—IP Routing Command Reference*)

m-lag mad default-action

m-lag mad exclude logical-interfaces

m-lag mad include interface

17.1.16. m-lag mad exclude logical-interfaces

Use **m-lag mad exclude logical-interfaces** to exclude all logical interfaces from the shutdown action by M-LAG MAD.

Use **undo m-lag mad exclude logical-interfaces** to restore the default.

Syntax

m-lag mad exclude logical-interfaces

undo m-lag mad exclude logical-interfaces

Default

By default, M-LAG MAD shuts down all network interfaces when it detects a multi-active collision, except for the network interfaces set by the system to not shut down.

Views

System view

Predefined user roles

network-admin

Usage guidelines

When a VXLAN tunnel is used as the M-LAG peer link on an EVPN M-LAG system, you must retain a large number of logical interfaces (for example, tunnel and loopback interfaces) in up state. To

simplify configuration, you can exclude all logical interfaces from the shutdown action by M-LAG MAD.

The **m-lag mad exclude interface** and **m-lag mad include interface** commands take precedence over the **m-lag mad exclude logical-interfaces** command.

Examples

Exclude all logical interfaces from the shutdown action by M-LAG MAD.

```
<Sysname> system-view
[Sysname] m-lag mad exclude logical-interfaces
```

Related commands

display m-lag mad verbose

m-lag mad default-action

m-lag mad exclude interface

m-lag mad include interface

17.1.17. m-lag mad include interface

Use **m-lag mad include interface** to add an interface to the user-configured list of included ports, which will be shut down by M-LAG MAD when the M-LAG system splits.

Use **undo m-lag mad include interface** to remove a network interface from the user-configured list of included ports.

Syntax

m-lag mad include interface *interface-type interface-number*

undo m-lag mad include interface *interface-type interface-number*

Default

The user-configured included port list does not contain any ports.

Views

System view

Predefined user roles

network-admin

Parameters

interface-type interface-number: Specifies an interface by its type and number.

Usage guidelines

This command is typically used when the default M-LAG MAD action is set to NONE. In this situation, M-LAG MAD does not shut down the network interfaces on the secondary M-LAG member device when the M-LAG system splits. To avoid network issues caused by multi-active collision, add network interfaces to the user-configured include port list if they are not in the system-configured included port list. M-LAG MAD on the secondary M-LAG member device will shut down the interfaces in the system-configured and user-configured included port lists when the M-LAG system splits.

For example, if you use a VXLAN tunnel as the M-LAG peer-link in an EVPN environment, you must retain a large number of logical interfaces (for example, tunnel and loopback interfaces) in up state. To improve configuration efficiency, you can set the default M-LAG MAD action to NONE and add interfaces to the user-configured include port list.

The M-LAG MAD DOWN action will not take effect on the following interfaces:

- Network interfaces automatically or manually excluded from being shut down by M-LAG MAD. To identify these interfaces, execute the **display m-lag mad verbose** command.
- Network interfaces automatically or manually excluded from being shut down by IRF MAD. To identify these interfaces, execute the **display mad verbose** command.
- Network interfaces used for special purposes, including:
  - Interfaces placed in a loopback test by using the **loopback** command.
  - Interfaces in a mirroring group.
  - Interfaces forced to stay up by using the **port-up mode** command.

Examples

Configure M-LAG MAD to shut down Bridge-Aggregation 1 on the secondary M-LAG member device when the M-LAG system splits.

```
<Sysname> system-view
[Sysname] m-lag mad include interface bridge-aggregation 1
```

Related commands

display m-lag mad verbose

display mad (*Virtual Technologies Command Reference*)

m-lag mad default-action

m-lag mad exclude logical-interfaces

m-lag mad exclude interface

loopback (*Interface Command Reference*)

mirroring-group reflector-port (*Network Management and Monitoring Command Reference*)

port up-mode (*Interface Command Reference*)

17.1.18. m-lag mad persistent

Use **m-lag mad persistent** to enable M-LAG MAD DOWN state persistence.

Use **undo m-lag mad persistent** to disable M-LAG MAD DOWN state persistence.

Syntax

m-lag mad persistent

undo m-lag mad persistent

Default

The secondary M-LAG member device brings up interfaces in M-LAG MAD DOWN state when its role changes to primary.

Views

System view

Predefined user roles

network-admin

Usage guidelines

M-LAG MAD DOWN state persistence prevents the secondary M-LAG member device from bringing up the network interfaces in M-LAG MAD DOWN state when its role change to primary. This feature

helps avoid the forwarding issues that might occur in the multi-active situation that occurs because the keepalive link goes down while the M-LAG peer link is down.

Examples

Enable M-LAG MAD DOWN state persistence.

```
<Sysname> system-view
[Sysname] m-lag mad persistent
```

Related commands

display m-lag mad verbose

m-lag mad restore

17.1.19. m-lag mad restore

Use **m-lag mad restore** to bring up the interfaces in M-LAG MAD DOWN state.

Syntax

m-lag mad restore

Views

System view

Predefined user roles

network-admin

Usage guidelines

Execute this command only when both the peer link and the keepalive link are down.

You can bring up the interfaces in M-LAG MAD DOWN state on the secondary M-LAG member device for it to forward traffic if the following conditions exist:

- The primary M-LAG member device fails while the peer link is down.
- M-LAG MAD DOWN state persists on the secondary M-LAG member device.

Examples

Bring up the interfaces in M-LAG MAD DOWN state.

<Sysname> system-view

[Sysname] m-lag mad restore

```
To avoid network issues, make sure the primary device has failed and cannot forward
traffic. Continue? [Y/N]:y
```

Related commands

display m-lag mad verbose

m-lag mad persistent

17.1.20. m-lag restore-delay

Use **m-lag restore-delay** to set the data restoration interval.

Use **undo m-lag restore-delay** to restore the default.

Syntax

m-lag restore-delay *value*

undo m-lag restore-delay

Default

The data restoration interval is 30 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

value: Specifies the data restoration interval, in the range of 1 to 3600 seconds.

Usage guidelines

The data restoration interval specifies the maximum amount of time for the secondary M-LAG member device to synchronize data with the primary M-LAG member device during M-LAG system setup. Within the data restoration interval, the secondary M-LAG member device sets all network interfaces to M-LAG MAD DOWN state, except for the following interfaces:

- M-LAG peer-link interface .
- Management Ethernet interface.
- Interfaces excluded from the MAD shutdown action.

When the data restoration interval expires, the secondary M-LAG member device brings up all network interfaces.

To avoid packet loss and forwarding failure, increase the data restoration interval if the amount of data is large or if an ISSU is to be performed between the M-LAG member devices.

Examples

Set the data restoration interval to 50 seconds.

```
<Sysname> system-view
[Sysname] m-lag restore-delay 50
```

17.1.21. m-lag role priority

Use **m-lag role priority** to set the M-LAG role priority of the device.

Use **undo m-lag role priority** to restore the default.

Syntax

m-lag role priority *priority-value*

undo m-lag role priority

Default

The M-LAG role priority of the device is 32768.

Views

System view

Predefined user roles

network-admin

Parameters

priority-value: Specifies the M-LAG role priority, in the range of 0 to 65535. The lower the value, the higher the priority.

Usage guidelines

For features that require centralized traffic processing, a M-LAG member device is assigned the primary or secondary role based on its M-LAG role priority. The secondary M-LAG member device forwards the traffic of those features to the primary M-LAG member device for processing. If the M-LAG member devices use the same M-LAG role priority, the member device with a lower bridge MAC address is assigned the primary role.

As a best practice to avoid network flapping, do not modify the M-LAG role priority of M-LAG member devices after the M-LAG system is established.

Examples

Set the M-LAG role priority of the device to 66.

```
<Sysname> system-view
[Sysname] m-lag role priority 66
```

Related commands

display m-lag role

17.1.22. m-lag standalone enable

Use **m-lag standalone enable** to enable M-LAG standalone mode.

Use **undo m-lag standalone enable** to disable M-LAG standalone mode.

Syntax

m-lag standalone enable [delay *delay-time* **]**

undo m-lag standalone enable [delay]

Default

M-LAG standalone mode is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

delay *delay-time*: Sets the delay that the device must wait before changing to M-LAG standalone mode. The value range for this delay is 0 to 3600 seconds. If you do not set this parameter, the device changes to M-LAG standalone mode without delay when both the peer link and the keepalive link go down.

Usage guidelines

Enable M-LAG standalone mode to avoid forwarding issues in the multi-active situation that might occur after both the peer link and the keepalive link are down.

M-LAG standalone mode helps avoid traffic forwarding issues in this multi-active situation by allowing only the member ports in the M-LAG interfaces on one member device to forward traffic.

An M-LAG member device does not enter M-LAG standalone mode if the M-LAG peer reboots.

If you execute this command multiple times, the most recent configuration takes effect.

As a best practice, enable M-LAG standalone mode on both primary and secondary M-LAG member devices.

To prevent member ports of M-LAG interfaces from flapping, set the M-LAG standalone mode delay to be longer than the time required for a device reboot.

In a single-level M-LAG network, before you enable M-LAG standalone mode on an M-LAG member device, make sure its LACP system priority is higher than that of the remote aggregation system. This restriction ensures that the reference port is on the remote aggregation system and prevents the interfaces attached to the M-LAG system from flapping.

An M-LAG member device changes to M-LAG standalone mode only when it detects that both the peer link and the keepalive link are down. It does not change to M-LAG standalone mode when the peer M-LAG member device reboots. As a best practice, set the delay that the device must wait before changing to M-LAG standalone mode based on the cause of simultaneous failure of the peer link and keepalive link:

Examples

Enable M-LAG standalone mode.

<Sysname> system-view

[Sysname] m-lag standalone enable

17.1.23. m-lag system-mac

Use **m-lag system-mac** to configure the M-LAG system MAC address.

Use **undo m-lag system-mac** to restore the default.

Syntax

m-lag system-mac *mac-address*

undo m-lag system-mac

Default

The M-LAG system MAC address is not configured.

Views

System view

Predefined user roles

network-admin

Parameters

mac-address: Specifies a MAC address in the H-H-H format. The MAC address cannot be a multicast MAC address, all-zero MAC address, or all-F MAC address.

Usage guidelines

CAUTION:

Changing the M-LAG system MAC address causes M-LAG system split. When you perform this task on a live network, make sure you are fully aware of its impact.

The M-LAG system MAC address uniquely identifies the M-LAG system on the network. For the M-LAG member devices to be identified as one M-LAG system, you must configure the same M-LAG system MAC address on them. As a best practice to avoid MAC address collision, use the bridge MAC address of one M-LAG member device as the M-LAG system MAC address.

Examples

Configure the M-LAG system MAC address as 0001-0001-0001.

```
<Sysname> system-view
[Sysname] m-lag system-mac 1-1-1
Changing the system MAC address might flap the intra-portal link and cause M-LAG
system setup failure. Continue? [Y/N]:y
[Sysname]
```

17.1.24. m-lag system-number

Use **m-lag system-number** to set the M-LAG system number.

Use **undo m-lag system-number** to restore the default.

Syntax

m-lag system-number *system-number*

undo m-lag system-number

Default

The M-LAG system number is not set.

Views

System view

Predefined user roles

network-admin

Parameters

system-number: Specifies the M-LAG system number. Available values are 1 and 2.

Usage guidelines

CAUTION:
Changing the M-LAG system number causes M-LAG system split. When you perform this task on a live network, make sure you are fully aware of its impact.

You must assign different M-LAG system numbers to the M-LAG member devices in a M-LAG system.

Examples

Set the M-LAG system number to 1.

```
<Sysname> system-view
[Sysname] m-lag system-number 1
Changing the system number might flap the intra-portal link and cause M-LAG system
setup failure. Continue? [Y/N]:y
[Sysname]
```

Related commands

display m-lag system

17.1.25. m-lag system-priority

Use **m-lag system-priority** to set the M-LAG system priority.

Use **undo m-lag system-priority** to restore the default.

Syntax

m-lag system-priority *priority*

undo m-lag system-priority

Default

The M-LAG system priority is 32768.

Views

System view

Predefined user roles

network-admin

Parameters

priority: Specifies a priority value in the range of 0 to 65535. The lower the value, the higher the priority.

Usage guidelines

CAUTION:

Changing the M-LAG system priority causes M-LAG system split. When you perform this task on a live network, make sure you are fully aware of its impact.

A M-LAG system uses its M-LAG system priority as the system LACP priority to communicate with the remote aggregation system.

You must configure the same M-LAG system priority for the M-LAG member devices in a M-LAG system.

Examples

Set the M-LAG system priority to 64.

```
<Sysname> system-view
[Sysname] m-lag system-priority 64
Changing the system priority might flap the intra-portal link and cause M-LAG system
setup failure. Continue? [Y/N]:y
[Sysname]
```

Related commands

display m-lag system

17.1.26. port m-lag group

Use **port m-lag group** to assign an aggregate interface to a M-LAG group.

Use **undo port m-lag group** to restore the default.

Syntax

port m-lag group *group-id*

undo port m-lag group

Default

An aggregate interface does not belong to a M-LAG group.

Views

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

group-id: Specifies a M-LAG group number in the range of 1 to 1024.

Usage guidelines

To use a Layer 2 aggregate interface as a M-LAG interface, you must assign it to a M-LAG group.

The device can have multiple M-LAG interfaces. However, you can assign a Layer 2 aggregate interface to only one M-LAG group.

A Layer 2 aggregate interface cannot operate as both M-LAG peer-link interface and M-LAG interface.

Examples

Assign Bridge-Aggregation 1 to M-LAG group 100.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] port m-lag group 100
```

Related commands

display m-lag summary

display m-lag verbose

17.1.27. port m-lag peer-link

Use **port m-lag peer-link** to specify an aggregate interface or VXLAN tunnel interface as the M-LAG peer-link interface .

Use **undo port m-lag peer-link** to restore the default.

Syntax

port m-lag peer-link *port-id*

undo port m-lag peer-link

Default

No interface is the M-LAG peer-link interface .

Views

Layer 2 aggregate interface view

VXLAN tunnel interface view

Predefined user roles

network-admin

Parameters

port-id: Specifies the M-LAG peer-link interface ID, which is fixed at 1.

Usage guidelines

A M-LAG member device can have only one M-LAG peer-link interface .

A Layer 2 aggregate interface cannot operate as both M-LAG peer-link interface and M-LAG interface.

As a best practice to reduce the impact of interface flapping on upper-layer services, execute the **link-delay** command on the M-LAG peer-link interface .

By default, MAC address learning is enabled on the M-LAG peer-link interface . This feature is not configurable on the M-LAG peer-link interface .

For M-LAG to operate correctly, you must disable the static source check feature for the MAC address table after you configure the M-LAG peer-link interface .

- With software versions earlier than Release 6510, execute the **undo mac-address static source-check enable** command on the M-LAG peer-link interface .
- With Release 6510 and later, execute the **undo mac-address static source-check enable** command in system view.

Examples

Specify Bridge-Aggregation 2 as the M-LAG peer-link interface .

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 2
[Sysname-Bridge-Aggregation2] port m-lag peer-link 1
```

Related commands

link-delay
mac-address mac-learning enable
mac-address static source-check enable

17.1.28. port m-lag virtual-ip

Use **port m-lag virtual-ip** to assign an M-LAG virtual IPv4 address to an interface.

Use **undo port m-lag virtual-ip** to restore the default.

Syntax

VLAN interface view:

port m-lag virtual-ip *ipv4-address* { *mask-length* | *mask* } [**active** | **standby**] [**virtual-mac** *mac-address*]

undo port m-lag virtual-ip [*ipv4-address*]

Loopback interface view:

port m-lag virtual-ip *ipv4-address* { *mask-length* | *mask* } [**active** | **standby**]

undo port m-lag virtual-ip [*ipv4-address*]

VSI interface view:

port m-lag virtual-ip *ipv4-address* { *mask-length* | *mask* } [**active** | **standby**]

undo port m-lag virtual-ip [*ipv4-address*]

Default

No M-LAG virtual IPv4 addresses are assigned to interfaces.

Views

CAUTION:
This command is only supported when setting up VLAN Interface view and VSI Interface view.

VLAN interface view

Loopback interface view

VSI interface view

Predefined user roles

network-admin

Parameters

ipv4-address: Specifies a virtual IPv4 address.

mask-length: Specifies the subnet mask length in the range of 0 to 32.

mask: Specifies the subnet mask in dotted decimal notation.

active: Sets the virtual IPv4 address to be active on the local device.

standby: Sets the virtual IPv4 address to be standby on the local device.

virtual-mac *mac-address*: Specifies a MAC address in the H-H-H format. The MAC address cannot be a multicast MAC address, all-zero MAC address, or all-F MAC address.

Usage guidelines

To ensure correct traffic forwarding, assign M-LAG virtual IPv4 addresses to the following interfaces on the M-LAG system:

- VLAN interfaces that act as dual-active gateways for the same VLAN.
- Loopback interfaces that offer AAA and 802.1X authentication services.
- VSI interfaces that act as distributed EVPN gateways.

If you do not specify the **active** or **standby** keyword for a virtual IPv4 address, the address is active only on the primary M-LAG member device.

If you execute the **undo port m-lag ipv4 virtual-ip** command without specifying the ipv4-address argument, the command deletes all M-LAG virtual IPv4 addresses on the interface.

When the peer-link interface fails, the standby virtual IPv4 address becomes active on the primary M-LAG member device. If no virtual MAC address is associated with the standby virtual IPv4 address, the MAC address of the interface that owns the standby virtual IPv4 address is used as the virtual MAC address. In this scenario, the devices attached to the primary M-LAG member device will refresh their ARP entries.

When you assign multiple M-LAG virtual IPv4 addresses to an interface, follow these restrictions and guidelines:

- You can assign a maximum of two virtual IPv4 addresses to an interface.
- If you configure different virtual MAC addresses for a virtual IPv4 address, the most recent configuration takes effect.
- You cannot configure the same virtual MAC address for multiple virtual IPv4 addresses.

- When you assign a virtual IPv4 address to VLAN interfaces, you must configure the same virtual MAC address for the virtual IPv4 address on both M-LAG member devices.

If you assign both virtual IPv4 and IPv6 addresses to VLAN interfaces, make sure the virtual IPv4 and IPv6 addresses that use the same virtual MAC address are in the same state on the M-LAG member devices.

When both M-LAG member devices act as gateways for dualhomed user-side devices, the gateway interfaces (VLAN or VSI interfaces) on the M-LAG member devices use the same IP address and MAC address. In this scenario, the M-LAG member devices cannot set up neighbor relationships with the user-side devices. To resolve this issue, assign virtual IPv4 addresses to the gateway interfaces and configure routing protocols such as BGP and OSPF to use the virtual IPv4 addresses for neighbor relationship setup.

For the M-LAG member devices to set up BGP peer relationships with other devices, perform the following tasks:

- Execute the **port m-lag virtual-ip** *ipv4-address* { *mask-length* | *mask* } [**active** | **standby**] [**virtual-mac** *mac-address*] command.
- Execute the **peer source-address** command to specify the virtual IPv4 address as the source IPv4 address for establishing TCP connections to peers.

For the M-LAG member devices to set up OSPF neighbor relationships with other devices, perform the following tasks:

- Execute the **port m-lag virtual-ip** *ipv4-address* { *mask-length* | *mask* } [**active** | **standby**] [**virtual-mac** *mac-address*] command.
- Execute the ospf **peer sub-address enable** command to specify the virtual IPv4 address as the secondary IPv4 address for establishing OSPF neighbor relationships.

When dual-active gateways exist on the M-LAG system, you must assign unique virtual IPv4 addresses to the gateway interfaces on the M-LAG member devices and configure both virtual IPv4 addresses to be active. When you assign a virtual MAC address to a VLAN interface, make sure the virtual MAC address is identical to the MAC address assigned to the VLAN interface by using the mac-address command.

Examples

Assign M-LAG virtual IPv4 address **10.10.10.10/24** to VLAN-interface 2 and set the state of the address to **active**.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] port m-lag virtual-ip 10.10.10.10 24 active virtual-mac 1-1-1
```

Related commands

nas-ip (*Security Command Reference*)
ospf peer sub-address enable (*Layer 3—IP Routing Command Reference*)
peer source-address (*Layer 3—IP Routing Command Reference*)
port-security m-lag load-sharing-mode (*Security Command Reference*)

QX-S5600G Series Ethernet Switches

Command References

4.Layer 3 - IP Services

This manual is including the following chapters.

01-ARP commands

02-Gratuitous ARP commands

03-Proxy ARP commands

04-ARP snooping commands

05-IP addressing commands

06-DHCP commands

07-DNS commands

08-IP forwarding basics commands

09-IP performance optimization commands

10-UDP Helper commands

11-IPv6 basics commands

12-Tunneling commands

13-HTTP redirect commands

14-ARP direct route commands

Contents

A page of this section is **4-x-x**

1. ARP commands 1-1
1.1. ARP commands 1-1
1.1.1. arp check enable 1-1
1.1.2. arp check log enable 1-1
1.1.3. arp mac-interface-consistency check enable 1-2
1.1.4. arp max-learning-num 1-3
1.1.5. arp max-learning-number 1-4
1.1.6. arp mode uni 1-4
1.1.7. arp multiport 1-5
1.1.8. arp static 1-6
1.1.9. arp timer aging 1-8
1.1.10. display arp 1-8
1.1.11. display arp *ip-address* 1-11
1.1.12. display arp timer aging 1-12
1.1.13. display arp vpn-instance 1-12
1.1.14. reset arp 1-13

1. ARP commands

1.1. ARP commands

1.1.1. arp check enable

Use **arp check enable** to enable dynamic ARP entry check.

Use **undo arp check enable** to disable dynamic ARP entry check.

Syntax

arp check enable

undo arp check enable

Default

Dynamic ARP entry check is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Dynamic ARP entry check disables a device from supporting dynamic ARP entries with multicast MAC addresses. The device cannot learn dynamic ARP entries containing multicast MAC addresses. You cannot manually add static ARP entries that contain multicast MAC addresses.

When dynamic ARP entry check is disabled, ARP entries containing multicast MAC addresses are supported. The device can learn dynamic ARP entries containing multicast MAC addresses obtained from the ARP packets sourced from a unicast MAC address. You can also manually add static ARP entries containing multicast MAC addresses.

Examples

Enable dynamic ARP entry check.

```
<Switch> system-view
[Switch] arp check enable
```

1.1.2. arp check log enable

Use **arp check log enable** to enable the ARP logging feature.

Use **undo arp check log enable** to disable the ARP logging feature.

Syntax

arp check log enable

undo arp check log enable

Default

ARP logging is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This feature enables a device to log ARP events when ARP cannot resolve IP addresses correctly. The log information helps administrators locate and solve problems. The device can log the following ARP events:

- On a proxy ARP-disabled interface, the target IP address of a received ARP packet is not one of the following IP addresses:
  - The IP address of the receiving interface.
  - The virtual IP address of the VRRP group.
- The sender IP address of a received ARP reply conflicts with one of the following IP addresses:
  - The IP address of the receiving interface.
  - The virtual IP address of the VRRP group.

The device sends ARP log messages to the information center. You can use the **info-center source** command to specify the log output rules for the information center. For more information about information center, see *Network Management and Monitoring Configuration Guide*.

The device can generate a large number of ARP logs. To conserve system resources, enable ARP logging only when you are auditing or troubleshooting ARP events.

Examples

Enable ARP logging.

```
<Switch> system-view
[Switch] arp check log enable
```

1.1.3. arp mac-interface-consistency check enable

Use **arp mac-interface-consistency check enable** to enable interface consistency check for ARP and MAC address entries.

Use **undo arp mac-interface-consistency check enable** to disable this feature.

Syntax

arp mac-interface-consistency check enable

undo arp mac-interface-consistency check enable

Default

Enabling interface consistency check for ARP and MAC address entries is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

In an instable network, the receiving interface for packets from a user might change. The interface in the MAC address entry can be updated immediately while the interface in the ARP entry cannot. In

this case, the packets matching the ARP entry will be sent out of an incorrect interface. To solve this problem, you can use this feature to periodically check the interface consistency for the ARP and MAC address entry of a user. If the interfaces are not the same, ARP sends ARP requests in the VLAN of the ARP entry and updates the entry with the ARP reply receiving interface.

Use **display mac-address** to display MAC address entries.

Examples

Enable interface consistency check for ARP and MAC address entries.

```
<Switch> system-view
[Switch] arp mac-interface-consistency check enable
```

Related commands

display mac-address

1.1.4. arp max-learning-num

Use **arp max-learning-num** to set the dynamic ARP learning limit for an interface.

Use **undo arp max-learning-num** to restore the default.

Syntax

arp max-learning-num *max-number*

undo arp max-learning-num

Default

An interface can learn a maximum of 16384 dynamic ARP entries.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Layer 3 Ethernet interface view

VXLAN VSI interface view

VLAN interface view

Predefined user roles

network-admin

Parameters

max-number: Specifies the maximum number of dynamic ARP entries for an interface. The value range for this argument is 0 to 16384.

Usage guidelines

An interface can dynamically learn ARP entries. To prevent an interface from holding too many ARP entries, you can set the maximum number of dynamic ARP entries that the interface can learn. When the maximum number is reached, the interface stops learning ARP entries.

When the *number* argument is set to 0, the interface is disabled from learning dynamic ARP entries.

Examples

Specify VLAN-interface 40 to learn a maximum of 10 dynamic ARP entries.

```
<Switch> system-view
[Switch] interface vlan-interface 40
```

```
[Switch-Vlan-interface40] arp max-learning-num 10
```

Specify GigabitEthernet 1/0/1 to learn a maximum of 10 dynamic ARP entries.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] arp max-learning-num 10
```

Specify Layer 2 aggregate interface Bridge-Aggregation 1 to learn a maximum of 10 dynamic ARP entries.

```
<Switch> system-view
[Switch] interface bridge-aggregation 1
[Switch-Bridge-Aggregation1] arp max-learning-num 10
```

1.1.5. arp max-learning-number

Use **arp max-learning-number** to set the dynamic ARP learning limit for a device.

Use **undo arp max-learning-number** to restore the default.

Syntax

arp max-learning-number *max-number* **slot** *slot-number*

undo arp max-learning-number slot *slot-number*

Default

A device can learn a maximum of 16384 dynamic ARP entries.

Views

System view

Predefined user roles

network-admin

Parameters

max-number: Specifies the maximum number of dynamic ARP entries for a device. The value range for this argument is 0 to 16384.

slot *slot-number*: Specifies an IRF member device by its member ID.

Usage guidelines

A device can dynamically learn ARP entries. To prevent a device from holding too many ARP entries, you can set the maximum number of dynamic ARP entries that the device can learn. When the maximum number is reached, the device stops learning ARP entries.

When the *number* argument is set to 0, the device is disabled from learning dynamic ARP entries.

Examples

Set the dynamic ARP learning limit to 64 for slot 1.

```
<Switch> system-view
[Switch] arp max-learning-number 64 slot 1
```

1.1.6. arp mode uni

Use **arp mode uni** to configure a port as a customer-side port.

Use **undo arp mode** to restore the default.

Syntax

arp mode uni

undo arp mode

Default

A port operates as a network-side port.

Views

VLAN interface view

VXLAN VSI interface view

Predefined user roles

network-admin

Usage guidelines

By default, the device associates an ARP entry with routing information when the device learns an ARP entry. The ARP entry provides the next hop information for routing. To save hardware resources, you can use this command to specify a port that connects to a user terminal as a customer-side port. The device will not associate the routing information with the learned ARP entries.

Examples

Configure VLAN-interface 2 as a customer-side port.

```
<Switch> system-view
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] arp mode uni
```

1.1.7. arp multiport

Use **arp multiport** to configure a multiport ARP entry.

Use **undo arp** to delete an ARP entry.

Syntax

arp multiport *ip-address mac-address vlan-id* [**vpn-instance** *vpn-instance-name*]

undo arp *ip-address* [*vpn-instance-name*]

Default

No multiport ARP entries exist.

Views

System view

Predefined user roles

network-admin

Parameters

ip-address: Specifies an IP address for the multiport ARP entry.

mac-address: Specifies a MAC address for the multiport ARP entry, in the format of H-H-H.

vlan-id: Specifies a VLAN for the multiport ARP entry, in the range of 1 to 4094. The specified VLAN must already exist.

vpn-instance *vpn-instance-name*: Specifies a VPN instance to which the multiport ARP entry belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. The specified VPN instance must already exist. To specify a multiport ARP entry on the public network, do not specify this option.

Usage guidelines

If the VLAN or the corresponding VLAN interface is deleted, the multiport ARP entry is also deleted.

To make the multiport ARP entry effective for packet forwarding, you must configure a multicast or multiport unicast MAC address entry to specify multiple output interfaces. The MAC address entry must have the same MAC address and VLAN ID as the multiport ARP entry. In addition, the IP address in the multiport ARP entry must reside on the same subnet as the VLAN interface of the specified VLAN.

Examples

Configure a multiport ARP entry that contains IP address 202.38.10.2 and MAC address f474-8801-0000 in VLAN 10.

```
<Switch> system-view
[Switch] arp multiport 202.38.10.2 f474-8801-0000 10
```

Related commands

display arp multiport

reset arp multiport

1.1.8. arp static

Use **arp static** to configure a static ARP entry.

Use **undo arp** to delete an ARP entry.

Syntax

arp static *ip-address mac-address* [*vlan-id interface-type interface-number* | **vsi-interface** *vsi-interface-id* **tunnel** *number* **vsi** *vsi-name* | **vsi-interface** *vsi-interface-id interface-type interface-number* **service-instance** *instance-id* **vsi** *vsi-name*] [**vpn-instance** *vpn-instance-name*]

undo arp *ip-address* [*vpn-instance-name*]

Default

No static ARP entries exist.

Views

System view

Predefined user roles

network-admin

Parameters

ip-address: Specifies an IP address for the static ARP entry.

mac-address: Specifies a MAC address for the static ARP entry, in the format of H-H-H.

vlan-id: Specifies the ID of a VLAN to which the static ARP entry belongs. The value range is 1 to 4094.

interface-type interface-number: Specifies an interface by its type and number.

vsi-interface *vsi-interface-id*: Specifies a VSI interface by its number. The VSI interface must already exist.

tunnel *number*: Specifies a tunnel interface by its number. The tunnel interface must already exist.

vsi *vsi-name*: Specifies a VSI by its name, a case-sensitive string of 1 to 31 characters.

vpn-instance *vpn-instance-name*: Specifies a VPN instance to which the static ARP entry belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. The VPN instance must already exist. To specify a static ARP entry on the public network, do not specify this option.

Usage guidelines

A static ARP entry is manually configured and maintained. It does not age out and cannot be overwritten by any dynamic ARP entry.

Static ARP entries can be short or long.

A resolved short static ARP entry becomes unresolved upon certain events, for example, when the resolved output interface goes down, or the corresponding VLAN or VLAN interface is deleted.

Long static ARP entries are effective or ineffective. Ineffective long static ARP entries cannot be used for packet forwarding. A long static ARP entry is ineffective when any of the following conditions exists:

- The corresponding VLAN interface or output interface is down.
- The IP address in the entry conflicts with a local IP address.
- No local interface has an IP address in the same subnet as the IP address in the ARP entry.

If you specify the *vlan-id interface-type interface-number* argument, follow these restrictions and guidelines:

- The interface can be an Ethernet interface or an aggregate interface.
- The VLAN and VLAN interface must already exist. The specified Ethernet interface must belong to the specified VLAN.
- The IP address of the VLAN interface and the IP address specified by the *ip-address* argument must be on the same network.
- A long static ARP entry in a VLAN is deleted if the VLAN or VLAN interface is deleted.

On a VXLAN IP gateway that forwards traffic among VXLANs through VXLAN tunnels, a VSI interface can act as the gateway for multiple VXLANs. The VSI interface (input interface) might be connected to multiple VXLAN tunnel interfaces (output interfaces). In this case, you must specify the **vsi-interface** *vsi-interface-id* **tunnel** *number* **vsi** *vsi-name* parameters to identify a VSI interface-VSI-VXLAN tunnel interface binding. For more information about VSI interfaces, VSI, and VXLAN tunnel interfaces, see *VXLAN Configuration Guide*.

Examples

Configure a long static ARP entry that contains IP address 202.38.10.2, MAC address f474-8801-0000, and output interface GigabitEthernet 1/0/1 in VLAN 10.

```
<Switch> system-view
[Switch] arp static 202.38.10.2 f474-8801-0000 10 gigabitethernet 1/0/1
```

Configure a long static ARP entry that contains IP address 1.1.1.1, MAC address f474-8801-0000, input interface VSI-interface 1, output interface Tunnel 1, and the VSI **a**.

```
<Switch> system-view
[Switch] arp static 1.1.1.1 f474-8801-0000 vsi-interface 1 tunnel 1 vsi a
```

Related commands

display arp

reset arp

1.1.9. arp timer aging

Use **arp timer aging** to set the aging timer for dynamic ARP entries.

Use **undo arp timer aging** to restore the default.

Syntax

arp timer aging *aging-minutes*

undo arp timer aging

Default

The aging timer for dynamic ARP entries is 20 minutes.

Views

System view

Predefined user roles

network-admin

Parameters

aging-minutes: Specifies the aging timer in minutes. The value range for this argument is 1 to 1440.

Usage guidelines

Each dynamic ARP entry in the ARP table has a limited lifetime, called an aging timer. The aging timer of a dynamic ARP entry is reset each time the dynamic ARP entry is updated. Dynamic ARP entries that are not updated before their aging timers expire are deleted from the ARP table.

Set the aging timer for dynamic ARP entries as needed. For example, when you configure proxy ARP, set a short aging time so that invalid dynamic ARP entries can be deleted in a timely manner.

Examples

Set the aging timer for dynamic ARP entries to 10 minutes.

```
<Switch> system-view
[Switch] arp timer aging 10
```

Related commands

display arp timer aging

1.1.10. display arp

Use **display arp** to display ARP entries.

Syntax

display arp [[**all** | **dynamic** | **multiport** | **static**] [**slot** *slot-number*] | **vlan** *vlan-id* | **interface** *interface-type interface-number*] [**count** | **verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

all: Displays all ARP entries.

dynamic: Displays dynamic ARP entries.

multiport: Displays multiport ARP entries.

static: Displays static ARP entries.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays ARP entries for the master device.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID. The VLAN ID is in the range of 1 to 4094.

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays ARP entries for all interfaces.

count: Displays the number of ARP entries.

verbose: Displays detailed information about ARP entries.

Usage guidelines

This command displays information about ARP entries, including the IP address, MAC address, VLAN ID, output interface, entry type, and aging timer.

Examples

Display all ARP entries.

```
<Switch> display arp all
  Type: S-Static   D-Dynamic   O-Openflow   R-Rule   M-Multiport  I-Invalid
IP Address       MAC Address     VID     Interface/Link ID      Aging Type
1.1.1.1          02e0-f102-0023  1       GE1/0/1                N/A   S
1.1.1.2          f474-8800-0001  12      GE1/0/2                960   D
1.1.1.3          00e0-fe50-6503  12      Tunnel1                960   D
1.1.1.4          000d-88f7-9f7d  12      0x1                    960   D
```

Display detailed information about all ARP entries.

```
<Switch> display arp all verbose
IP address          : 1.1.1.1                 MAC address    : 02e0-f102-0023
Type                : Static                  Aging          : --
Interface           : GE1/0/1                 VLAN           : 1
VPN instance        : --
Link ID             : --
VXLAN ID            : --
VSI name            : --
VSI interface       : --
Nickname            : 0x0000

IP address          : 1.1.1.2                 MAC address    : 0015-e944-adc5
Type                : Static                  Aging          : 960 sec
Interface           : GE1/0/2                 VLAN           : 12
VPN instance        : --
```

```
Link ID             : --
VXLAN ID            : --
VSI name            : --
VSI interface       : --
Nickname            : 0x0000
```

Display the number of all ARP entries.

```
<Switch> display arp all count
 Total number of entries : 4
```

Table 1-1 Command output

Field	Description
IP Address	IP address in an ARP entry.
MAC Address	MAC address in an ARP entry.
VID	This field is not supported in the current software version. ID of the VLAN or index of the VSI to which the ARP entry belongs. This field displays **N/A** in either of the following situations: • The ARP entry is an unresolved short static ARP entry. • The output interface of the ARP entry does not belong to the VLAN or VSI.
Interface	Output interface in an ARP entry. This field displays **N/A** in either of the following situations: • The ARP entry is an unresolved short static ARP entry. • The ARP entry is a multiport ARP entry and has no output interface information. To obtain the output interface information of the multiport ARP entry, look up the MAC address table according to the MAC address in the ARP entry.
Link ID	This field is not supported in the current software version. Link ID in an ARP entry. This field displays hyphens (**--**) if the ARP entry does not belong to any VSI.
Aging	Aging time for an ARP entry in seconds. For a static ARP entry, this field always displays **N/A**. The static ARP entry never ages out unless you delete it manually. For a dynamic ARP entry, this field displays **N/A** if the aging time is unknown.
Type	ARP entry type: • **D**—Dynamic. • **S**—Static. • **O**—OpenFlow. • **R**—Rule. • **M**—Multiport. • **I**—Invalid.
Nickname	This field is not supported in the current software version. Nickname of the ARP entry. The nickname is a string of four hexadecimal numbers, for example, 012a.
VPN Instance	This field is not supported in the current software version. Name of VPN instance. If no VPN instance is configured for the ARP entry, this field displays **[No Vrf]**.

Field	Description
VXLAN ID	This field is not supported in the current software version. ID of the VXLAN to which the ARP entry belongs. VXLAN ID is also called VNI. If the ARP entry does not belong to any VXLAN, this field displays **N/A**.
VSI Name	This field is not supported in the current software version. Name of the VSI to which the ARP entry belongs. If the ARP entry does not belong to any VSI, this field displays **N/A**.
VSI Interface	This field is not supported in the current software version. Name of the gateway interface of the VSI. If no gateway interface is specified for the VSI, this field displays **N/A**.
Total number of entries	Number of ARP entries.

Related commands

arp static

reset arp

1.1.11. display arp *ip-address*

Use **display arp** *ip-address* to display the ARP entry for an IP address.

Syntax

display arp *ip-address* [**slot** *slot-number*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ip-address: Displays the ARP entry for the specified IP address.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information for the master device.

verbose: Displays the detailed information about the specified ARP entry.

Usage guidelines

The ARP entry information includes the IP address, MAC address, VLAN ID, output interface, entry type, and aging timer.

Examples

Display the ARP entry for the IP address 20.1.1.1.

```
<Switch> display arp 20.1.1.1
  Type: S-Static   D-Dynamic   O-Openflow   R-Rule   M-Multiport  I-Invalid
IP Address       MAC Address     VID     Interface/Link ID      Aging Type
20.1.1.1         f474-8800-0001  N/A     N/A                    N/A   S
```

Related commands

arp static

reset arp

1.1.12. display arp timer aging

Use **display arp timer aging** to display the aging timer of dynamic ARP entries.

Syntax

display arp timer aging

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

This command always displays the aging time in seconds no matter which unit you set in the **arp timer aging** command.

Examples

Display the aging timer of dynamic ARP entries.

```
<Switch> display arp timer aging
Current ARP aging time is 1200 seconds
```

Related commands

arp timer aging

1.1.13. display arp vpn-instance

Use **display arp vpn-instance** to display the ARP entries for a VPN instance.

Syntax

display arp vpn-instance *vpn-instance-name* [**count**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vpn-instance-name: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. The VPN instance name cannot contain any spaces.

count: Displays the number of ARP entries.

Usage guidelines

This command displays information about ARP entries for a VPN instance, including the IP address, MAC address, VLAN ID, output interface, entry type, and aging timer.

Examples

Display ARP entries for VPN instance **test**.

```
<Switch> display arp vpn-instance test
  Type: S-Static   D-Dynamic   O-Openflow   R-Rule   M-Multiport  I-Invalid
IP Address       MAC Address     VID     Interface/Link ID      Aging Type
20.1.1.1         f474-8800-0001  N/A     N/A                    N/A   S
```

Related commands

arp static

reset arp

1.1.14. reset arp

Use **reset arp** to clear ARP entries from the ARP table.

Syntax

reset arp { **all** | **dynamic** | **interface** *interface-type interface-number* | **multiport** | **slot** *slot-number* | **static** }

Views

User view

Predefined user roles

network-admin

Parameters

all: Clears all ARP entries.

dynamic: Clears all dynamic ARP entries.

multiport: Clears all multiport ARP entries.

static: Clears all static ARP entries.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears ARP entries for the master device.

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command clears ARP entries for all interfaces.

Examples

Clear all static ARP entries.

```
<Switch> reset arp static
```

Related commands

arp static

display arp

Contents

A page of this section is **4-x-x**

2. Gratuitous ARP commands 2-1
2.1. Gratuitous ARP commands 2-1
2.1.1. arp ip-conflict log prompt 2-1
2.1.2. arp send-gratuitous-arp 2-1
2.1.3. gratuitous-arp mac-change retransmit 2-2
2.1.4. gratuitous-arp-learning enable 2-3
2.1.5. gratuitous-arp-sending enable 2-4

2. Gratuitous ARP commands

2.1. Gratuitous ARP commands

2.1.1. arp ip-conflict log prompt

Use **arp ip-conflict log prompt** to enable IP conflict notification.

Use **undo arp ip-conflict log prompt** to restore the default.

Syntax

arp ip-conflict log prompt

undo arp ip-conflict log prompt

Default

IP conflict notification is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

By default, the device performs the following operations if it is using the sender IP address of a received ARP packet:

- Sends a gratuitous ARP request.
- Displays an error message after the device receives an ARP reply about the conflict.

You can use this command to enable the device to display error messages before sending a gratuitous ARP reply or request for conflict confirmation.

Examples

Enable IP conflict notification on the device.

```
<Switch> system-view
[Switch] arp ip-conflict log prompt
```

2.1.2. arp send-gratuitous-arp

Use **arp send-gratuitous-arp** to enable periodic sending of gratuitous ARP packets on an interface.

Use **undo arp send-gratuitous-arp** to disable the interface from periodically sending gratuitous ARP packets.

Syntax

arp send-gratuitous-arp [**interval** *interval*]

undo arp send-gratuitous-arp

Default

Periodic sending of gratuitous ARP packets is disabled.

Views

Layer 3 Ethernet interface view

VXLAN VSI interface view

VLAN interface view

Predefined user roles

network-admin

Parameters

interval *interval*: Specifies the sending interval in the range of 200 to 200000 milliseconds. The default value is 2000 milliseconds.

Usage guidelines

This feature takes effect on an interface only when the interface has an IP address and the data link layer state of the interface is up.

This feature can send gratuitous ARP requests only for a VRRP virtual IP address, or the sending interface's primary IP address or manually configured secondary IP address. The primary IP address can be configured manually or automatically, whereas the secondary IP address must be configured manually.

If you change the sending interval for gratuitous ARP packets, the configuration takes effect at the next sending interval.

The sending interval for gratuitous ARP packets might be much longer than the set interval when any of the following conditions exist:

- This feature is enabled on multiple interfaces.
- Each interface is configured with multiple secondary IP addresses.
- A small sending interval is configured in the preceding cases.

Examples

Enable VLAN-interface 2 to send gratuitous ARP packets every 300 milliseconds.

```
<Switch> system-view
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] arp send-gratuitous-arp interval 300
```

2.1.3. gratuitous-arp mac-change retransmit

Use **gratuitous-arp mac-change retransmit** to set the times and the interval for retransmitting a gratuitous ARP packet for the device MAC address change.

Use **undo gratuitous-arp mac-change retransmit** to restore the default.

Syntax

gratuitous-arp mac-change retransmit *times* **interval** *seconds*

undo gratuitous-arp mac-change retransmit

Default

The device sends a gratuitous packet for its MAC address change once only.

Views

System view

Predefined user roles

network-admin

Parameters

times: Specifies the times of retransmitting a gratuitous packet, in the range of 1 to 10.

interval *seconds*: Specifies the interval for retransmitting a gratuitous packet, in the range of 1 to 10 seconds.

Usage guidelines

The device sends a gratuitous ARP packet to inform other devices of its MAC address change. However, the other devices might fail to receive the packet because the device sends the gratuitous ARP packet once only by default. Use this command to configure gratuitous ARP retransmission parameters to ensure that the other devices can receive the packet.

After you execute this command, the device will retransmit a gratuitous ARP packet for its MAC address change at the specified interval for the specified times.

Examples

Set the times to 3 and the interval to 5 for retransmitting a gratuitous ARP packet for the device MAC address change.

```
<Sysname> system-view
[Sysname] gratuitous-arp mac-change retransmit 3 interval 5
```

2.1.4. gratuitous-arp-learning enable

Use **gratuitous-arp-learning enable** to enable learning of gratuitous ARP packets.

Use **undo gratuitous-arp-learning enable** to disable learning of gratuitous ARP packets.

Syntax

gratuitous-arp-learning enable

undo gratuitous-arp-learning enable

Default

Learning of gratuitous ARP packets is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

The learning of gratuitous ARP packets feature allows a device to maintain its ARP table by creating or updating ARP entries based on received gratuitous ARP packets.

When this feature is disabled, the device uses received gratuitous ARP packets to update existing ARP entries only. ARP entries are not created based on the received gratuitous ARP packets, which saves ARP table space.

Examples

Enable learning of gratuitous ARP packets.

```
<Switch> system-view
[Switch] gratuitous-arp-learning enable
```

2.1.5. gratuitous-arp-sending enable

Use **gratuitous-arp-sending enable** to enable sending gratuitous ARP packets upon receiving ARP requests whose sender IP address is on a different subnet.

Use **undo gratuitous-arp-sending enable** to disable sending gratuitous ARP packets upon receiving ARP requests whose sender IP address is on a different subnet.

Syntax

gratuitous-arp-sending enable

undo gratuitous-arp-sending enable

Default

A device does not send gratuitous ARP packets when it receives ARP requests whose sender IP address is on a different subnet.

Views

System view

Predefined user roles

network-admin

Examples

Disable a device from sending gratuitous ARP packets upon receiving ARP requests whose sender IP address is on a different subnet.

```
<Switch> system-view
[Switch] undo gratuitous-arp-sending enable
```

Contents

A page of this section is **4-x-x**

3. Proxy ARP commands ····· 3-1
3.1. Proxy ARP commands ····· 3-1
3.1.1. display local-proxy-arp ····· 3-1
3.1.2. display proxy-arp ····· 3-1
3.1.3. local-proxy-arp enable ····· 3-2
3.1.4. proxy-arp enable ····· 3-3

3. Proxy ARP commands

3.1. Proxy ARP commands

3.1.1. display local-proxy-arp

Use **display local-proxy-arp** to display the local proxy ARP status.

Syntax

display local-proxy-arp [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays the local proxy ARP status for all interfaces.

Usage guidelines

You can use this command to check whether local proxy ARP is enabled or disabled.

Examples

Display the local proxy ARP status for VLAN-interface 2.

```
<Switch> display local-proxy-arp interface vlan-interface 2
Interface Vlan-interface2
 Local Proxy ARP status: enabled
```

Related commands

local-proxy-arp enable

3.1.2. display proxy-arp

Use **display proxy-arp** to display the proxy ARP status.

Syntax

display proxy-arp [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays the proxy ARP status for all interfaces.

Usage guidelines

You can use this command to check whether proxy ARP is enabled or disabled.

Examples

Display the proxy ARP status on VLAN-interface 2.

```
<Switch> display proxy-arp interface vlan-interface 2
Interface Vlan-interface2
 Proxy ARP status: disabled
```

Related commands

proxy-arp enable

3.1.3. local-proxy-arp enable

Use **local-proxy-arp enable** to enable local proxy ARP.

Use **undo local-proxy-arp enable** to disable local proxy ARP.

Syntax

local-proxy-arp enable [**ip-range** *start-ip-address* **to** *end-ip-address*]

undo local-proxy-arp enable

Default

Local proxy ARP is disabled.

Views

Layer 3 Ethernet interface view

VXLAN VSI interface view

VLAN interface view

Predefined user roles

network-admin

Parameters

ip-range *start-ip-address* **to** *end-ip-address*: Specifies the IP address range for which local proxy ARP is enabled. The start IP address must be lower than or equal to the end IP address.

Usage guidelines

Proxy ARP enables a device on a network to answer ARP requests for an IP address not on that network. With proxy ARP, hosts in different broadcast domains can communicate with each other as they do on the same network.

Proxy ARP includes common proxy ARP and local proxy ARP.

Common proxy ARP allows communication between hosts that connect to different Layer 3 interfaces and reside in different broadcast domains.

Local proxy ARP allows communication between hosts that connect to the same Layer 3 interface and reside in different broadcast domains.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Enable local proxy ARP on VLAN-interface 2.

```
<Switch> system-view
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] local-proxy-arp enable
```

Enable local proxy ARP on VLAN-interface 2 for an IP address range.

```
<Switch> system-view
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] local-proxy-arp enable ip-range 1.1.1.1 to 1.1.1.20
```

Related commands

display local-proxy-arp

3.1.4. proxy-arp enable

Use **proxy-arp enable** to enable proxy ARP.

Use **undo proxy-arp enable** to disable proxy ARP.

Syntax

proxy-arp enable

undo proxy-arp enable

Default

Proxy ARP is disabled.

Views

Layer 3 Ethernet interface view

VXLAN VSI interface view

VLAN interface view

Predefined user roles

network-admin

Usage guidelines

Proxy ARP enables a device on a network to answer ARP requests for an IP address not on that network. With proxy ARP, hosts in different broadcast domains can communicate with each other as they do on the same network.

Proxy ARP includes common proxy ARP and local proxy ARP.

Common proxy ARP allows communication between hosts that connect to different Layer 3 interfaces and reside in different broadcast domains.

Local proxy ARP allows communication between hosts that connect to the same Layer 3 interface and reside in different broadcast domains.

Examples

Enable proxy ARP on VLAN-interface 2.

```
<Switch> system-view
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] proxy-arp enable
```

Related commands

display proxy-arp

Contents

A page of this section is **4-x-x**

4. ARP snooping commands ····· 4-1
4.1. ARP snooping commands ····· 4-1
4.1.1. arp snooping enable ····· 4-1
4.1.2. display arp snooping ····· 4-1
4.1.3. reset arp snooping ····· 4-2

4. ARP snooping commands

4.1. ARP snooping commands

4.1.1. arp snooping enable

Use **arp snooping enable** to enable ARP snooping.

Use **undo arp snooping enable** to disable ARP snooping.

Syntax

arp snooping enable

undo arp snooping enable

Default

ARP snooping is disabled.

Views

VLAN view

Predefined user roles

network-admin

Examples

Enable ARP snooping for VLAN 2.

```
<Switch> system-view
[Switch] vlan 2
[Switch-vlan2] arp snooping enable
```

4.1.2. display arp snooping

Use **display arp snooping** to display ARP snooping entries.

Syntax

display arp snooping [**vlan** *vlan-id*] [**slot** *slot-number*] [**count**]

display arp snooping ip *ip-address* [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vlan *vlan-id*: Displays ARP snooping entries for a VLAN. The *vlan-id* argument is in the range of 1 to 4094.

count: Displays the number of the ARP snooping entries.

ip *ip-address*: Displays the ARP snooping entry for the specified IP address.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays ARP snooping entries for the master device.

Examples

Display ARP snooping entries for VLAN 2.

```
<Switch> display arp snooping vlan 2
IP Address    MAC Address    VLAN ID Interface  Aging       Status
3.3.3.3       0003-0003-0003 2       GE1/0/1    20          Valid
3.3.3.4       0004-0004-0004 2       GE1/0/2    5           Invalid
```

Display the number of the ARP snooping entries.

```
<Switch> display arp snooping count
Total entries: 2
```

Table 4-1 Command output

Field	Description
IP Address	IP address in an ARP snooping entry.
MAC Address	MAC address in an ARP snooping entry.
VLAN ID	ID of the VLAN to which the ARP snooping entry belongs.
Interface	Input interface in an ARP snooping entry.
Aging	Aging time for an ARP snooping entry in minutes. If the card learns an ARP snooping entry from another card, the card cannot learn the aging time of the entry, and this field displays **N/A**.
Status	Status of an ARP snooping entry: **Valid**, **Invalid**, **Collision**.
Total entries	Number of ARP snooping entries.

Related commands

reset arp snooping

4.1.3. reset arp snooping

Use **reset arp snooping** to delete ARP snooping entries.

Syntax

reset arp snooping [**ip** *ip-address* | **vlan** *vlan-id*]

Views

User view

Predefined user roles

network-admin

Parameters

ip *ip-address*: Deletes the ARP snooping entry for the specified IP address.

vlan *vlan-id*: Deletes ARP snooping entries for the specified VLAN. The value range for the *vlan-id* argument is 1 to 4094.

Usage guidelines

If you do not specify any option, the command deletes all ARP snooping entries.

Examples

Delete ARP snooping entries for VLAN 2.

```
<Switch> reset arp snooping vlan 2
```

Related commands

display arp snooping

Contents

A page of this section is **4-x-x**

5. IP addressing commands 5-1
5.1. IP addressing commands 5-1
5.1.1. display ip interface 5-1
5.1.2. display ip interface brief 5-3
5.1.3. ip address 5-5
5.1.4. ip address unnumbered 5-6

5. IP addressing commands

5.1. IP addressing commands

5.1.1. display ip interface

Use **display ip interface** to display IP configuration and statistics for Layer 3 interfaces.

Syntax

display ip interface [*interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number: Specifies an interface by its type and number. If you do not specify an interface, this command displays IP configuration and statistics for all Layer 3 interfaces.

Usage guidelines

Use the **display ip interface** command to display IP configuration and statistics for the specified Layer 3 interface. The statistics include the following information:

- The number of unicast packets, bytes, and multicast packets the interface has sent and received.
- The number of TTL-invalid packets and ICMP packets the interface has received.

The packet statistics helps you locate a possible attack on the network.

Examples

Display IP configuration and statistics for VLAN-interface 10.

```
<Switch> display ip interface vlan-interface 10
Vlan-interface10 current state : DOWN
Line protocol current state : DOWN
Internet Address is 1.1.1.1/8 Primary
Broadcast address : 1.255.255.255
The Maximum Transmit Unit : 1500 bytes
input packets : 0, bytes : 0, multicasts : 0
output packets : 0, bytes : 0, multicasts : 0
TTL invalid packet number:         0
ICMP packet input number:          0
  Echo reply:                      0
  Unreachable:                     0
  Source quench:                   0
  Routing redirect:                0
```

```
Echo request:                   0
Router advert:                  0
Router solicit:                 0
Time exceed:                    0
IP header bad:                  0
Timestamp request:              0
Timestamp reply:                0
Information request:            0
Information reply:              0
Netmask request:                0
Netmask reply:                  0
Unknown type:                   0
```

Table 5-1 Command output

Field	Description
current state	Physical link state of the interface: • **Administrative DOWN**—The interface has been shut down by using the **shutdown** command. • **DOWN**—The interface is administratively up, but its physical state is down (possibly because no physical link exists or the link has failed). • **UP**—The interface is both administratively and physically up.
Line protocol current state	Data link layer state of the interface. • **DOWN**—The data link layer protocol is down. • **UP**—The data link layer protocol is up. • **UP (spoofing)**—The data link layer protocol is up, but the link is an on-demand link or does not exist.
Internet Address	IP address of an interface followed by: • **Primary**—A primary IP address. • **Sub**—A secondary IP address. • **DHCP-Allocated**—An IP address obtained through DHCP. • **BOOTP-Allocated**—An IP address obtained through BOOTP. • **Mad**—A MAD IP address. • **IRF-Member**—IP address of the management Ethernet port of an IRF member device.
Broadcast address	Broadcast address of the subnet attached to an interface.
The Maximum Transmit Unit	MTU of the interface, in bytes.
input packets, bytes, multicasts output packets, bytes, multicasts	All received and sent packets and bytes, and received and sent multicast packets on an interface (statistics start at the device startup).
TTL invalid packet number	Number of TTL-invalid packets received on the interface (statistics start at the device startup).
ICMP packet input number: Echo reply:	Total number of ICMP packets received on the interface (statistics start at the device startup): • Echo reply packets.

Field	Description
Unreachable: Source quench: Routing redirect: Echo request: Router advert: Router solicit: Time exceed: IP header bad: Timestamp request: Timestamp reply: Information request: Information reply: Netmask request: Netmask reply: Unknown type:	• Unreachable packets. • Source quench packets. • Routing redirect packets. • Echo request packets. • Router advertisement packets. • Router solicitation packets. • Time exceeded packets. • IP header bad packets. • Timestamp request packets. • Timestamp reply packets. • Information request packets. • Information reply packets. • Netmask request packets. • Netmask reply packets. • Unknown type packets.

Related commands

display ip interface brief

ip address

5.1.2. display ip interface brief

Use **display ip interface brief** to display brief IP configuration for Layer 3 interfaces.

Syntax

display ip interface [*interface-type* [*interface-number*]] **brief** [**description**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type: Specifies an interface type. If you do not specify an interface type, this command displays brief IP configuration for all Layer 3 interfaces.

interface-number: Specifies an interface number. If you do not specify an interface number, this command displays brief IP configuration for all Layer 3 interfaces of the specified type.

description: Displays complete interface descriptions. If you do not specify this keyword, the command displays a maximum of 13 characters for each interface description. If the description is longer than 13 characters, the first 10 characters are displayed, followed by an ellipsis (...).

Usage guidelines

Information displayed by the command includes the state of the physical and link layer protocols, IP address, and interface descriptions.

Examples

Display brief IP configuration for VLAN interfaces.

```
<Switch> display ip interface vlan-interface brief
*down: administratively down
(s): spoofing  (l): loopback
Interface            Physical  Protocol  IP address      VPN instance  Description
Vlan10               down      down      6.6.6.1         --            Link to Co...
Vlan2                down      down      7.7.7.1         vpn-first...  --
<Switch> display ip interface vlan-interface brief description
*down: administratively down
(s): spoofing  (l): loopback
Interface            Physical  Protocol  IP address      VPN instance  Description
Vlan10               down      down      6.6.6.1         --            Link to CoreR
                                                                       Outer
Vlan2                down      down      7.7.7.1         vpn-first-in  --
                                                         stance
```

Table 5-2 Command output

Field	Description
*down: administratively down	The interface is administratively shut down by using the **shutdown** command.
(s) : spoofing	Spoofing attribute of the interface. The link protocol state of the interface is up, but the link is temporarily established on demand or does not exist.
Interface	Interface name.
Physical	Physical state of the interface: • ***down**—The interface is administratively shut down by using the **shutdown** command. • **down**—The interface is administratively up but its physical state is down, possibly because of a connection or link failure. • **up**—Both the administrative and physical states of the interface are up.
Protocol	Link layer protocol state of the interface: • **down**—The protocol state of the interface is down. • **down(l)**—The protocol state of the interface is down (loopback). • **up**—The protocol state of the interface is up. • **up(l)**—The protocol state of the interface is up (loopback). • **up(s)**—The protocol state of the interface is up (spoofing).
IP address	IP address of the interface. If no IP address is configured, this field displays hyphens (**--**).
VPN instance	Name of the VPN instance to which the interface belongs. This field displays a maximum of 12 characters. If the VPN instance name is longer than 12 characters, the first 9 characters are displayed, followed by an ellipsis (...). If the interface does not belong to any VPN instance, this field displays hyphens (**--**).
Description	Description of the interface. This field displays a maximum of 13 characters. If the description is longer than 13 characters, the first 10 characters are displayed, followed by an ellipsis (...). If no

Field	Description
	description is configured, this field displays hyphens (**--**).

Related commands

display ip interface

ip address

5.1.3. ip address

Use **ip address** to assign an IP address to the interface.

Use **undo ip address** to remove the IP address from the interface.

Syntax

ip address *ip-address* { *mask-length* | *mask* } [**sub**]

undo ip address *ip-address* { *mask-length* | *mask* } [**sub**]

Default

No IP address is assigned to an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the IP address of the interface, in dotted decimal notation.

mask-length: Specifies the subnet mask length in the range of 1 to 31. For a loopback interface, the value range is 1 to 32.

mask: Specifies the subnet mask in dotted decimal notation.

sub: Assigns a secondary IP address to the interface.

Usage guidelines

Use the command to assign a primary or secondary IP address to an interface.

An interface can have only one primary IP address. A newly configured primary IP address overwrites the previous address. If the interface connects to multiple subnets, configure primary and secondary IP addresses on the interface so the subnets can communicate with each other through the interface.

You cannot assign secondary IP addresses to an interface that obtains an IP address through BOOTP, PPP address negotiation, IP unnumbered, or DHCP.

If you do not specify any parameters, the **undo ip address** command removes all IP addresses from the interface. The **undo ip address** *ip-address* { *mask* | *mask-length* } command removes the primary IP address. The **undo ip address** *ip-address* { *mask* | *mask-length* } **sub** command removes a secondary IP address.

The primary and secondary IP addresses assigned to the interface can be located on the same network segment. Different interfaces on your device must reside on different network segments.

Examples

Assign VLAN-interface 10 a primary IP address 129.12.0.1 and a secondary IP address 202.38.160.1, with subnet masks both 255.255.255.0.

```
<Switch> system-view
[Switch] interface vlan-interface 10
[Switch-Vlan-interface10] ip address 129.12.0.1 255.255.255.0
[Switch-Vlan-interface10] ip address 202.38.160.1 255.255.255.0 sub
```

Related commands

display ip interface

display ip interface brief

5.1.4. ip address unnumbered

Use **ip address unnumbered** to configure the current interface as IP unnumbered to borrow an IP address from the specified interface.

Use **undo ip address unnumbered** to restore the default.

Syntax

ip address unnumbered interface *interface-type interface-number*

undo ip address unnumbered

Default

The interface does not borrow IP addresses from other interfaces.

Views

Interface view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies an interface from which the current interface can borrow an IP address.

Usage guidelines

Typically, you assign an IP address to an interface either manually or through DHCP. If the IP addresses are not enough, or the interface is used only occasionally, you can configure an interface to borrow an IP address from other interfaces. This is called IP unnumbered, and the interface borrowing the IP address is called IP unnumbered interface.

Loopback interfaces cannot borrow IP addresses of other interfaces, but other interfaces can borrow IP addresses of loopback interfaces.

Multiple interfaces can use the same unnumbered IP address. If an interface has multiple manually configured IP addresses, only the primary IP address manually configured can be borrowed.

You cannot enable a dynamic routing protocol on the interface that has no IP address configured. To enable the interface to communicate with other devices, you must configure a static route to the peer device on the interface.

Examples

Configure Ten-GigabitEthernet1/0/49 to borrow the IP address of LoopBack1.

```
<Sysname> system-view
[Sysname] interface Ten-GigabitEthernet1/0/49
[Switch-Ten-GigabitEthernet1/0/49] ip address unnumbered interface LoopBack1
```

Display interface configuration for Ten-GigabitEthernet1/0/49. It shows the borrowed IP address.

```
<Sysname> display interface Ten-GigabitEthernet 1/0/49
  <...snip...>
  Internet address: 172.16.1.1/32 (unnumbered)
  <...snip...>
```

Contents

A page of this section is **4-x-x**

6. DHCP commands 6-1
6.1. Common DHCP commands 6-1
6.1.1. dhcp dscp 6-1
6.1.2. dhcp enable 6-1
6.1.3. dhcp select 6-2
6.2. DHCP server commands 6-3
6.2.1. address range 6-3
6.2.2. bims-server 6-4
6.2.3. bootfile-name 6-4
6.2.4. dhcp relay mac-forward enable 6-5
6.2.5. dhcp server apply ip-pool 6-6
6.2.6. dhcp server forbidden-ip 6-7
6.2.7. dhcp server ip-pool 6-8
6.2.8. dhcp server ping packets 6-8
6.2.9. dhcp server ping timeout 6-9
6.2.10. dhcp server relay information enable 6-10
6.2.11. display dhcp server conflict 6-10
6.2.12. display dhcp server expired 6-11
6.2.13. display dhcp server free-ip 6-12
6.2.14. display dhcp server ip-in-use 6-13
6.2.15. display dhcp server pool 6-14
6.2.16. display dhcp server statistics 6-16
6.2.17. dns-list 6-18
6.2.18. domain-name 6-19
6.2.19. expired 6-19
6.2.20. forbidden-ip 6-20
6.2.21. gateway-list 6-21
6.2.22. nbns-list 6-22
6.2.23. netbios-type 6-23
6.2.24. network 6-24
6.2.25. next-server 6-25
6.2.26. option 6-25
6.2.27. reset dhcp server conflict 6-27
6.2.28. reset dhcp server expired 6-27
6.2.29. reset dhcp server ip-in-use 6-28
6.2.30. reset dhcp server statistics 6-28
6.2.31. static-bind 6-29
6.2.32. tftp-server domain-name 6-30
6.2.33. tftp-server ip-address 6-30
6.2.34. voice-config 6-31
6.3. DHCP relay agent commands 6-32
6.3.1. dhcp relay client-information record 6-32
6.3.2. dhcp relay client-information refresh enable 6-33
6.3.3. dhcp relay information circuit-id 6-34
6.3.4. dhcp relay information enable 6-36
6.3.5. dhcp relay information remote-id 6-36
6.3.6. dhcp relay information strategy 6-37
6.3.7. dhcp relay release ip 6-38
6.3.8. dhcp relay request-from-tunnel discard 6-39
6.3.9. dhcp relay server-address 6-40
6.3.10. display dhcp relay client-information 6-41

6.3.11. display dhcp relay information ····· 6-42
6.3.12. display dhcp relay server-address ····· 6-44
6.3.13. display dhcp relay statistics ····· 6-45
6.3.14. reset dhcp relay client-information ····· 6-46
6.3.15. reset dhcp relay statistics ····· 6-46
6.4. DHCP client commands ····· 6-47
6.4.1. dhcp client dad enable ····· 6-47
6.4.2. dhcp client dscp ····· 6-48
6.4.3. display dhcp client ····· 6-48
6.4.4. ip address dhcp-alloc ····· 6-51
6.5. DHCP snooping commands ····· 6-51
6.5.1. dhcp snooping binding record ····· 6-51
6.5.2. dhcp snooping enable ····· 6-52
6.5.3. dhcp snooping information circuit-id ····· 6-53
6.5.4. dhcp snooping information enable ····· 6-54
6.5.5. dhcp snooping information remote-id ····· 6-55
6.5.6. dhcp snooping information strategy ····· 6-56
6.5.7. dhcp snooping trust ····· 6-57
6.5.8. dhcp snooping trust tunnel ····· 6-58
6.5.9. display dhcp snooping binding ····· 6-58
6.5.10. display dhcp snooping information ····· 6-60
6.5.11. display dhcp snooping packet statistics ····· 6-61
6.5.12. display dhcp snooping trust ····· 6-62
6.5.13. reset dhcp snooping binding ····· 6-62
6.5.14. reset dhcp snooping packet statistics ····· 6-63
6.6. BOOTP client commands ····· 6-63
6.6.1. display bootp client ····· 6-63
6.6.2. ip address bootp-alloc ····· 6-64

6. DHCP commands

6.1. Common DHCP commands

6.1.1. dhcp dscp

Use **dhcp dscp** to set the DSCP value for DHCP packets sent by the DHCP server or the DHCP relay agent.

Use **undo dhcp dscp** to restore the default.

Syntax

dhcp dscp *dscp-value*

undo dhcp dscp

Default

The DSCP value is 56 in DHCP packets sent by the DHCP server or the DHCP relay agent.

Views

System view

Predefined user roles

network-admin

Parameters

dscp-value: Specifies the DSCP value for DHCP packets, in the range of 0 to 63.

Usage guidelines

The DSCP value of a packet specifies the priority level of the packet and affects the transmission priority of the packet. A bigger DSCP value represents a higher priority.

Examples

Set the DSCP value to 30 for DHCP packets sent by the DHCP server or the DHCP relay agent.

```
<Switch> system-view
[Switch] dhcp dscp 30
```

6.1.2. dhcp enable

Use **dhcp enable** to enable DHCP.

Use **undo dhcp enable** to disable DHCP.

Syntax

dhcp enable

undo dhcp enable

Default

DHCP is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

DHCP related configuration takes effect only after you enable DHCP.

Enable DHCP before you configure the DHCP server or relay agent.

Examples

Enable DHCP.

```
<Switch> system-view
[Switch] dhcp enable
```

6.1.3. dhcp select

Use **dhcp select** to enable the DHCP server or DHCP relay agent on an interface.

Use **undo dhcp select** to disable the DHCP server or DHCP relay agent on an interface. The interface will discard incoming DHCP packets.

Syntax

dhcp select { **relay** | **server** }

undo dhcp select { **relay** | **server** }

Default

The interface operates in the DHCP server mode and responds to DHCP requests with configuration parameters.

Views

Interface view

Predefined user roles

network-admin

Parameters

relay: Enables the DHCP relay agent on the interface.

server: Enables the DHCP server on the interface.

Usage guidelines

Before enabling a DHCP server to operate as a DHCP relay agent, use the **reset dhcp server ip-in-use** command to clear address bindings and authorized ARP entries. These authorized ARP entries might conflict with ARP entries that are created after the DHCP relay agent is enabled.

When DHCP server proxy is enabled on the DHCP relay agent, the proxy forwards packets between the DHCP clients and DHCP server.

- When receiving DHCP requests from DHCP clients, the proxy forwards them to the DHCP server.
- When receiving DHCP responses from the DHCP server, the proxy modifies the DHCP server's IP address in these responses as its own IP address.

Examples

Enable the DHCP relay agent on VLAN-interface 2.

```
<Switch> system-view
[Switch] interface vlan-interface 2
```

```
[Switch-Vlan-interface2] dhcp select relay
```

Related commands

dhcp relay server-address

reset dhcp server ip-in-use

6.2. DHCP server commands

6.2.1. address range

Use **address range** to configure an IP address range in a DHCP address pool for dynamic allocation.

Use **undo address range** to restore the default.

Syntax

address range *start-ip-address end-ip-address*

undo address range

Default

No IP address range exists.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

start-ip-address: Specifies the start IP address.

end-ip-address: Specifies the end IP address.

Usage guidelines

If no IP address range is specified, all IP addresses in the subnet specified by the **network** command in address pool view are assignable. If an IP address range is specified, only the IP addresses in the IP address range are assignable.

After you use the **address range** command, you cannot use the **network secondary** command to specify a secondary subnet in the address pool.

If you execute this command multiple times, the most recent configuration takes effect.

The address range specified by the **address range** command must be within the subnet specified by the **network** command. The addresses outside of the subnet cannot be assigned.

Examples

Specify an address range of 192.168.8.1 through 192.168.8.150 in address pool 1.

```
<Switch> system-view
[Switch] dhcp server ip-pool 1
[Switch-dhcp-pool-1] address range 192.168.8.1 192.168.8.150
```

Related commands

display dhcp server pool

network

6.2.2. bims-server

Use **bims-server** to specify the IP address, port number, and shared key of the BIMS server in a DHCP address pool.

Use **undo bims-server** to restore the default.

Syntax

bims-server ip *ip-address* [**port** *port-number*] **sharekey** { **cipher** | **simple** } *string*

undo bims-server

Default

No BIMS server information is specified.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

ip *ip-address*: Specifies the IP address of the BIMS server.

port *port-number*: Specifies the port number of the BIMS server, in the range of 1 to 65534.

cipher: Specifies a key in encrypted form.

simple: Specifies a key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key string. Its plaintext form is a case-sensitive string of 1 to 16 characters. Its encrypted form is a case-sensitive string of 1 to 53 characters. The DHCP client uses the shared key to encrypt packets sent to the BIMS server.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify BIMS server IP address 1.1.1.1, port number 80, and shared key **aabbcc** in address pool 0.

```
<Switch> system-view
[Switch] dhcp server ip-pool 0
[Switch-dhcp-pool-0] bims-server ip 1.1.1.1 port 80 sharekey simple aabbcc
```

Related commands

display dhcp server pool

6.2.3. bootfile-name

Use **bootfile-name** to specify a configuration file name or URL.

Use **undo bootfile-name** to restore the default.

Syntax

bootfile-name *bootfile-name*

undo bootfile-name

Default

No configuration file name is specified.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

bootfile-name: Specifies the configuration file name, a case-sensitive string of 1 to 63 characters.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

To specify a configuration file on a TFTP server, use the *bootfile-name* argument.

Examples

Specify configuration file name **boot.cfg** in DHCP address pool 0.

```
<Switch> system-view
[Switch] dhcp server ip-pool 0
[Switch-dhcp-pool-0] bootfile-name boot.cfg
```

Related commands

display dhcp server pool

next-server

tftp-server domain-name

tftp-server ip-address

6.2.4. dhcp relay mac-forward enable

Use **dhcp relay mac-forward enable** to configure the DHCP relay agent to perform a MAC address table lookup for a DHCP reply if it does not have the request forwarding information for the reply.

Use **undo dhcp relay mac-forward enable** to restore the default.

Syntax

dhcp relay mac-forward enable [**broadcast**]

undo dhcp relay mac-forward enable

Default

The DHCP relay agent discards a DHCP reply if the agent does not have the request forwarding information for the reply.

Views

System view

Predefined user roles

network-admin

Parameters

broadcast: Enables the DHCP relay agent to broadcast DHCP replies. If you do not specify this keyword, the DHCP relay agent unicasts DHCP replies.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure the DHCP relay agent to perform a MAC address table lookup for a DHCP reply if it does not have the request forwarding information for the reply.

```
<Sysname> system-view
[Sysname] dhcp relay mac-forward enable
```

6.2.5. dhcp server apply ip-pool

Use **dhcp server apply ip-pool** to apply an address pool to an interface.

Use **undo dhcp server apply ip-pool** to restore the default.

Syntax

dhcp server apply ip-pool *pool-name*

undo dhcp server apply ip-pool

Default

No address pool is applied to an interface

Views

Interface view

Predefined user roles

network-admin

Parameters

pool-name: Specifies the name of a DHCP address pool, a case-insensitive string of 1 to 63 characters.

Usage guidelines

Upon receiving a DHCP request from the interface, the DHCP server searches for a static binding for the client from all address pools. If no static binding is found, the server assigns configuration parameters from the address pool applied on the interface to the client. If the address pool has no assignable IP address or does not exist, the DHCP client cannot obtain an IP address.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Apply DHCP address pool 0 to VLAN-interface 2.

```
<Switch> system-view
```

```
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] dhcp server apply ip-pool 0
```

Related commands

dhcp server ip-pool

6.2.6. dhcp server forbidden-ip

Use **dhcp server forbidden-ip** to exclude IP addresses from dynamic allocation globally.

Use **undo dhcp server forbidden-ip** to remove the configuration.

Syntax

dhcp server forbidden-ip *start-ip-address* [*end-ip-address*]

undo dhcp server forbidden-ip *start-ip-address* [*end-ip-address*]

Default

No IP addresses are excluded from dynamic allocation globally.

Views

System view

Predefined user roles

network-admin

Parameters

start-ip-address: Specifies the start IP address.

end-ip-address: Specifies the end IP address, which cannot be lower than the *start-ip-address*. If you do not specify this argument, only the *start-ip-address* is excluded from dynamic allocation.

Usage guidelines

The IP addresses of some devices such as the gateway and FTP server cannot be assigned to clients. Use this command to exclude such addresses from dynamic allocation.

If the excluded IP address is in a static DHCP binding, the address can still be assigned to the client.

The address or address range specified in the **undo dhcp server forbidden-ip** command must be the same as that specified in the **dhcp server forbidden-ip** command. To remove an IP address from the specified address range, you must remove the entire address range.

You can execute this command multiple times to exclude multiple IP address ranges from dynamic allocation.

Examples

Exclude the IP addresses of 10.110.1.1 through 10.110.1.63 from dynamic allocation globally.

```
<Switch> system-view
[Switch] dhcp server forbidden-ip 10.110.1.1 10.110.1.63
```

Related commands

forbidden-ip

static-bind

6.2.7. dhcp server ip-pool

Use **dhcp server ip-pool** to create a DHCP address pool and enter its view, or enter the view of an existing DHCP address pool.

Use **undo dhcp server ip-pool** to delete the specified DHCP address pool.

Syntax

dhcp server ip-pool *pool-name*

undo dhcp server ip-pool *pool-name*

Default

No DHCP address pools exist.

Views

System view

Predefined user roles

network-admin

Parameters

pool-name: Specifies a DHCP address pool name, a case-insensitive string of 1 to 63 characters. The pool name uniquely identifies an address pool.

Usage guidelines

A DHCP address pool is used to store the configuration parameters to be assigned to DHCP clients.

Examples

Create a DHCP address pool named **pool1**.

```
<Switch> system-view
[Switch] dhcp server ip-pool pool1
[Switch-dhcp-pool-pool1]
```

Related commands

dhcp server apply ip-pool

display dhcp server pool

6.2.8. dhcp server ping packets

Use **dhcp server ping packets** to set the maximum number of ping packets.

Use **undo dhcp server ping packets** to restore the default.

Syntax

dhcp server ping packets *number*

undo dhcp server ping packets

Default

The maximum number of ping packets is 1.

Views

System view

Predefined user roles

network-admin

Parameters

number: Sets the maximum number of ping packets, in the range of 0 to 10. To disable the address conflict detection, set the value to 0.

Usage guidelines

To avoid IP address conflicts, the DHCP server pings an IP address before assigning it to a DHCP client.

If a ping attempt succeeds, the server determines that the IP address is in use and picks a new IP address. If all the ping attempts fail, the server assigns the IP address to the requesting DHCP client.

Examples

Set the maximum number of ping packets to 10.

```
<Switch> system-view
[Switch] dhcp server ping packets 10
```

Related commands

dhcp server ping timeout

display dhcp server conflict

reset dhcp server conflict

6.2.9. dhcp server ping timeout

Use **dhcp server ping timeout** to set the ping response timeout time on the DHCP server.

Use **undo dhcp server ping timeout** to restore the default.

Syntax

dhcp server ping timeout *milliseconds*

undo dhcp server ping timeout

Default

The ping response timeout time is 500 milliseconds.

Views

System view

Predefined user roles

network-admin

Parameters

milliseconds: Specifies the timeout time in the range of 0 to 10000 milliseconds. To disable the ping operation for address conflict detection, set the value to 0 milliseconds.

Usage guidelines

To avoid IP address conflicts, the DHCP server pings an IP address before assigning it to a DHCP client.

If a ping attempt succeeds, the server determines that the IP address is in use and picks a new IP address. If all the ping attempts fail, the server assigns the IP address to the requesting DHCP client.

Examples

Set the response timeout time to 1000 milliseconds.

```
<Switch> system-view
[Switch] dhcp server ping timeout 1000
```

Related commands

dhcp server ping packets

display dhcp server conflict

reset dhcp server conflict

6.2.10. dhcp server relay information enable

Use **dhcp server relay information enable** to enable the DHCP server to handle Option 82.

Use **undo dhcp server relay information enable** to configure the DHCP server to ignore Option 82.

Syntax

dhcp server relay information enable

undo dhcp server relay information enable

Default

The DHCP server handles Option 82.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Upon receiving a DHCP request that contains Option 82, the server copies the original Option 82 into the response. If the server is configured to ignore Option 82, the response will not contain Option 82.

Examples

Configure the DHCP server to ignore Option 82.

```
<Switch> system-view
[Switch] undo dhcp server relay information enable
```

6.2.11. display dhcp server conflict

Use **display dhcp server conflict** to display information about IP address conflicts.

Syntax

display dhcp server conflict [**ip** *ip-address*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ip *ip-address*: Displays conflict information about the specified IP address. If you do not specify this option, this command displays information about all IP address conflicts.

Usage guidelines

The DHCP server generates IP address conflict information in the following situations:

- Before assigning an IP address to a DHCP client, the DHCP server pings the IP address and discovers that another host is using the address.
- The DHCP client sends a DECLINE packet to the DHCP server to inform the server of an IP address conflict.
- The DHCP server discovers that the only assignable address in the address pool is its own IP address.

Examples

Display information about all IP address conflicts.

```
<Switch> display dhcp server conflict
IP address          Detect time
4.4.4.1             Apr 25 16:57:20 2007
4.4.4.2             Apr 25 17:00:10 2007
```

Table 6-1 Command output

Field	Description
IP address	Conflicted IP address.
Detect time	Time when the conflict was discovered.

Related commands

reset dhcp server conflict

6.2.12. display dhcp server expired

Use **display dhcp server expired** to display the lease expiration information.

Syntax

display dhcp server expired [**ip** *ip-address* | **pool** *pool-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ip *ip-address*: Displays lease expiration information about the specified IP address. If you do not specify an IP address, this command displays lease expiration information about all IP addresses.

pool *pool-name*: Displays lease expiration information about the specified address pool. The pool name is a case-insensitive string of 1 to 63 characters. If you do not specify an address pool, this command displays lease expiration information about all address pools.

Usage guidelines

DHCP assigns these expired IP addresses to DHCP clients when all available addresses have been assigned.

Examples

Display all lease expiration information.

```
<Switch> display dhcp server expired
IP address       Client-identifier/Hardware address    Lease expiration
4.4.4.6          3030-3066-2e65-3230-302e-3130-3234    Apr 25 17:10:47 2007
                 -2d45-7468-6572-6e65-7430-2f31
```

Table 6-2 Command output

Field	Description
IP address	Expired IP address.
Client-identifier/Hardware address	Client ID or MAC address.
Lease expiration	Time when the lease expired.

Related commands

reset dhcp server expired

6.2.13. display dhcp server free-ip

Use **display dhcp server free-ip** to display information about assignable IP addresses.

Syntax

display dhcp server free-ip [**pool** *pool-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

pool *pool-name*: Displays assignable IP addresses in the specified address pool. The pool name is a case-insensitive string of 1 to 63 characters. If you do not specify an address pool, this command displays all assignable IP addresses for all address pools.

Examples

Display assignable IP addresses in all address pools.

```
<Switch> display dhcp server free-ip
Pool name: 1
  Network: 10.0.0.0 mask 255.0.0.0
    IP ranges from 10.0.0.10 to 10.0.0.100
    IP ranges from 10.0.0.105 to 10.0.0.255
  Secondary networks:
    10.1.0.0 mask 255.255.0.0
      IP ranges from 10.1.0.0 to 10.1.0.255
```

```
    10.2.0.0 mask 255.255.0.0
      IP Ranges from 10.2.0.0 to 10.2.0.255

Pool name: 2
  Network: 20.1.1.0 mask 255.255.255.0
    IP ranges from 20.1.1.0 to 20.1.1.255
```

Table 6-3 Command output

Field	Description
Pool name	Name of the address pool.
Network	Assignable network.
IP ranges	Assignable IP address range.
Secondary networks	Assignable secondary networks.

Related commands

address range

dhcp server ip-pool

network

6.2.14. display dhcp server ip-in-use

Use **display dhcp server ip-in-use** to display binding information about assigned IP addresses.

Syntax

display dhcp server ip-in-use [**ip** *ip-address* | **pool** *pool-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ip *ip-address*: Displays binding information about the specified assigned IP address. If you do not specify an IP address, this command displays binding information about all assigned IP addresses.

pool *pool-name*: Displays binding information about assigned IP addresses in the specified address pool. The pool name is a case-insensitive string of 1 to 63 characters. If you do not specify an address pool, this command displays binding information about assigned IP addresses in all address pools.

Usage guidelines

The binding information can be used by other security modules only when the DHCP server is configured on the gateway of DHCP clients.

If the lease deadline exceeds the year 2100, the lease expiration time is displayed as **After 2100**.

Examples

Display binding information about all assigned DHCP addresses.

```
<Switch> display dhcp server ip-in-use
IP address       Client identifier/    Lease expiration      Type
                 Hardware address
10.1.1.1         4444-4444-4444        Not used              Static(F)
10.1.1.2         3030-3030-2e30-3030-  May 1 14:02:49 2015   Auto(C)
                 662e-3030-3033-2d45-
                 7468-6572-6e65-74
10.1.1.3         1111-1111-1111        After 2100            Static(C)
```

Table 6-4 Command output

Field	Description
IP address	IP address assigned.
Client identifier/Hardware address	Client ID or hardware address.
Lease expiration	Lease expiration time: • **Exact time (May 1 14:02:49 2015 in this example)**—Time when the lease will expire. • **Not used**—The IP address of the static binding has not been assigned to the specific client. • **Unlimited**—Infinite lease expiration time. • **After 2100**—The lease will expire after 2100.
Type	Binding types: • **Static(F)**—A free static binding whose IP address has not been assigned. • **Static(O)**—An offered static binding whose IP address has been selected and sent by the DHCP server in a DHCP-OFFER packet to the client. **Static(C)**—A committed static binding whose IP address has been assigned to the DHCP client. • **Auto(O)**—An offered dynamic binding whose IP address has been dynamically selected by the DHCP server and sent in a DHCP-OFFER packet to the DHCP client. • **Auto(C)**—A committed dynamic binding whose IP address has been dynamically assigned to the DHCP client.

Related commands

reset dhcp server ip-in-use

6.2.15. display dhcp server pool

Use **display dhcp server pool** to display information about a DHCP address pool.

Syntax

display dhcp server pool [*pool-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

pool-name: Displays information about the specified address pool. The pool name is a case-insensitive string of 1 to 63 characters. If you do not specify the *pool-name* argument, this command displays information about all address pools.

Examples

Display information about all DHCP address pools.

```
<Switch> display dhcp server pool
Pool name: 0
  Network 20.1.1.0 mask 255.255.255.0
  class a range 20.1.1.50 20.1.1.60
  bootfile-name abc.cfg
  dns-list 20.1.1.66 20.1.1.67 20.1.1.68
  domain-name www.aabbcc.com
  bims-server ip 192.168.0.51 sharekey cipher $c$3$K13OmQPi791YvQoF2Gs1E+65LOU=
  option 2 ip-address 1.1.1.1
  expired 1 2 3 0

Pool name: 1
  Network 20.1.2.0 mask 255.255.255.0
  secondary networks:
    20.1.3.0 mask 255.255.255.0
    20.1.4.0 mask 255.255.255.0
  bims-server ip 192.168.0.51 port 50 sharekey cipher $c$3$K13OmQPi791YvQoF2Gs1E+65LOU=
  forbidden-ip 20.1.1.22 20.1.1.36 20.1.1.37
  forbidden-ip 20.1.1.22 20.1.1.23 20.1.1.24
  gateway-list 20.1.1.1 20.1.1.2 20.1.1.4
  nbns-list 20.1.1.5 20.1.1.6 20.1.1.7
  netbios-type m-node
  option 2 ip-address 1.1.1.1
  expired 1 0 0 0

Pool name: 2
  Network 20.1.3.0 mask 255.255.255.0
  address range 20.1.3.1 to 20.1.3.15
  class departmentA range 20.1.3.20 to 20.1.3.29
  class departmentB range 20.1.3.30 to 20.1.3.40
  next-server 20.1.3.33
  tftp-server domain-name www.dian.org.cn
  tftp-server ip-address 192.168.0.120
  voice-config ncp-ip 20.1.3.2
  voice-config as-ip 20.1.3.5
  voice-config voice-vlan 3 enable
  voice-config fail-over 20.1.3.6 123*
```

```
  option 2 ip-address 20.1.3.10
  expired 1 0 0 0

Pool name: 3
  static bindings:
    ip-address 10.10.1.2 mask 255.0.0.0
      hardware-address 00e0-00fc-0001 ethernet
    ip-address 10.10.1.3 mask 255.0.0.0
      client-identifier aaaa-bbbb
  expired unlimited
```

Table 6-5 Command output

Field	Description
Pool name	Name of an address pool.
Network	Assignable network.
secondary networks	Assignable secondary networks.
address range	Assignable address range.
class *class-name* range	DHCP user class and its address range.
static bindings	Static IP-to-MAC/client ID bindings.
option	Customized DHCP option.
expired	Lease duration: 1 2 3 4 in this example refers to 1 day 2 hours 3 minutes 4 seconds.
bootfile-name	Boot file name
dns-list	DNS server IP address.
domain-name	Domain name suffix.
bims-server	BIMS server information.
forbidden-ip	IP addresses excluded from dynamic allocation.
gateway-list	Gateway addresses.
nbns-list	WINS server addresses.
netbios-type	NetBIOS node type.
next-server	Next server IP address.
tftp-server domain-name	TFTP server name.
tftp-server ip-address	TFTP server address.
voice-config ncp-ip	Primary network calling processor address.
voice-config as-ip	Backup network calling processor address.
voice-config voice-vlan	Voice VLAN.
voice-config fail-over	Failover route.

6.2.16. display dhcp server statistics

Use **display dhcp server statistics** to display the DHCP server statistics.

Syntax

display dhcp server statistics [**pool** *pool-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

pool *pool-name*: Specifies an address pool by its name, a case-insensitive string of 1 to 63 characters. If you do not specify this option, this command displays information about all address pools.

Examples

Display the DHCP server statistics.

```
<Switch> display dhcp server statistics
    Pool number:                    1
    Pool utilization:               0.39%
    Bindings:
      Automatic:                    1
      Manual:                       0
      Expired:                      0
    Conflict:                       1
    Messages received:              10
      DHCPDISCOVER:                 5
      DHCPREQUEST:                  3
      DHCPDECLINE:                  0
      DHCPRELEASE:                  2
      DHCPINFORM:                   0
      BOOTPREQUEST:                 0
    Messages sent:                  6
      DHCPOFFER:                    3
      DHCPACK:                      3
      DHCPNAK:                      0
      BOOTPREPLY:                   0
    Bad Messages:                   0
```

Table 6-6 Command output

Field	Description
Pool number	Total number of address pools. This field is not displayed when you display statistics for a specific address pool.
Pool utilization	Pool usage rate: • If you display statistics for all address pools, this field displays the usage rate of all address pools. • If you display statistics for an address pool, this field displays the pool usage rate of the specified address pool.

Field	Description
Bindings	Bindings include the following types: • **Automatic**—Number of dynamic bindings. • **Manual**—Number of static bindings. • **Expired**—Number of expired bindings.
Conflict	Total number of conflict addresses. This field is not displayed if you display statistics for a specific address pool.
Messages received	DHCP packets received from clients: • DHCPDISCOVER. • DHCPREQUEST. • DHCPDECLINE. • DHCPRELEASE. • DHCPINFORM. • BOOTPREQUEST. This field is not displayed if you display statistics for a specific address pool.
Messages sent	DHCP packets sent to clients: • DHCPOFFER. • DHCPACK. • DHCPNAK. • BOOTPREPLY. This field is not displayed if statistics about a specific address pool are displayed.
Bad Messages	Number of bad messages. This field is not displayed if you display statistics for a specific address pool.

Related commands

reset dhcp server statistics

6.2.17. dns-list

Use **dns-list** to specify DNS server addresses in a DHCP address pool.

Use **undo dns-list** to remove DNS server addresses from a DHCP address pool.

Syntax

dns-list *ip-address*&<1-8>

undo dns-list [*ip-address*&<1-8>]

Default

No DNS server address is specified.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

ip-address&<1-8>: Specifies a space-separated list of up to eight DNS servers.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

If you do not specify any parameters, the **undo dns-list** command deletes all DNS server addresses in the DHCP address pool.

Examples

Specify DNS server address 10.1.1.254 in DHCP address pool 0.

```
<Switch> system-view
[Switch] dhcp server ip-pool 0
[Switch-dhcp-pool-0] dns-list 10.1.1.254
```

Related commands

display dhcp server pool

6.2.18. domain-name

Use **domain-name** to specify a domain name in a DHCP address pool.

Use **undo domain-name** to restore the default.

Syntax

domain-name *domain-name*

undo domain-name

Default

No domain name is specified.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

domain-name: Specifies the domain name, a case-sensitive string of 1 to 50 characters.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify domain name **company.com** in DHCP address pool 0.

```
<Switch> system-view
[Switch] dhcp server ip-pool 0
[Switch-dhcp-pool-0] domain-name company.com
```

Related commands

display dhcp server pool

6.2.19. expired

Use **expired** to set the lease duration in a DHCP address pool.

Use **undo expired** to restore the default lease duration for a DHCP address pool.

Syntax

expired { **day** *day* [**hour** *hour* [**minute** *minute* [**second** *second*]]] | **unlimited** }

undo expired

Default

The lease duration of a dynamic DHCP address pool is one day.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

day *day*: Specifies the number of days, in the range of 0 to 365.

hour *hour*: Specifies the number of hours, in the range of 0 to 23. The default is 0.

minute *minute*: Specifies the number of minutes, in the range of 0 to 59. The default is 0.

second *second*: Specifies the number of seconds, in the range of 0 to 59. The default is 0.

unlimited: Specifies the unlimited lease duration, which is actually 136 years.

Usage guidelines

The DHCP server assigns an IP address together with the lease duration to the DHCP client. Before the lease expires, the DHCP client must extend the lease duration.

- If the lease extension operation succeeds, the DHCP client can continue to use the IP address.
- If the lease extension operation does not succeed, both of the following events occur:
  - The DHCP client cannot use the IP address after the lease duration expires.
  - The DHCP server will label the IP address as an expired address.

Examples

Set the lease duration to 1 day, 2 hours, 3 minutes, and 4 seconds in DHCP address pool 0.

```
<Switch> system-view
[Switch] dhcp server ip-pool 0
[Switch-dhcp-pool-0] expired day 1 hour 2 minute 3 second 4
```

Related commands

display dhcp server expired

display dhcp server pool

reset dhcp server expired

6.2.20. forbidden-ip

Use **forbidden-ip** to exclude IP addresses from dynamic allocation in an address pool.

Use **undo forbidden-ip** to remove the configuration.

Syntax

forbidden-ip *ip-address*&<1-8>

undo forbidden-ip [*ip-address*&<1-8>]

Default

No IP addresses are excluded from dynamic allocation in an address pool.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

ip-address&<1-8>: Specifies a space-separated list of up to eight excluded IP addresses.

Usage guidelines

The excluded IP addresses in an address pool are still assignable in other address pools.

You can exclude a maximum of 4096 IP addresses in an address pool by executing this command multiple times.

If you do not specify any parameters, the **undo forbidden-ip** command removes all excluded IP addresses.

Examples

Exclude IP addresses 192.168.1.3 and 192.168.1.10 from dynamic allocation in DHCP address pool 0.

```
<Switch> system-view
[Switch] dhcp server ip-pool 0
[Switch-dhcp-pool-0] forbidden-ip 192.168.1.3 192.168.1.10
```

Related commands

dhcp server forbidden-ip

display dhcp server pool

6.2.21. gateway-list

Use **gateway-list** to specify gateway addresses in a DHCP address pool or a DHCP secondary subnet.

Use **undo gateway-list** to remove the specified gateway addresses from a DHCP address pool or a DHCP secondary subnet.

Syntax

gateway-list *ip-address*&<1-64>

undo gateway-list [*ip-address*&<1-64>]

Default

No gateway address is configured in a DHCP address pool or a DHCP secondary subnet.

Views

DHCP address pool view

DHCP secondary subnet view

Predefined user roles

network-admin

Parameters

ip-address&<1-64>: Specifies a space-separated list of up to 64 gateway addresses. Gateway addresses must reside on the same subnet as the assignable IP addresses.

Usage guidelines

The DHCP server assigns gateway addresses to clients on a secondary subnet in the following ways:

- If gateways are specified in both address pool view and secondary subnet view, DHCP assigns those specified in the secondary subnet view.
- If gateways are specified in address pool view but not in secondary subnet view, DHCP assigns those specified in address pool view.

If you do not specify any parameters, the **undo gateway-list** command deletes all gateway addresses.

Examples

Specify gateway address 10.1.1.1 in DHCP address pool 0.

```
<Switch> system-view
[Switch] dhcp server ip-pool 0
[Switch-dhcp-pool-0] gateway-list 10.1.1.1
```

Related commands

display dhcp server pool

6.2.22. nbns-list

Use **nbns-list** to specify WINS server addresses in a DHCP address pool.

Use **undo nbns-list** to remove the specified WINS server addresses.

Syntax

nbns-list *ip-address*&<1-8>

undo nbns-list [*ip-address*&<1-8>]

Default

No WINS server address is specified.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

ip-address&<1-8>: Specifies a space-separated list of up to eight WINS server IP addresses.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

If you do not specify any parameters, the **undo nbns-list** command deletes all WINS server addresses.

Examples

Specify WINS server address 10.1.1.1 in DHCP address pool 0.

```
<Switch> system-view
[Switch] dhcp server ip-pool 0
[Switch-dhcp-pool-0] nbns-list 10.1.1.1
```

Related commands

display dhcp server pool

netbios-type

6.2.23. netbios-type

Use **netbios-type** to specify the NetBIOS node type in a DHCP address pool.

Use **undo netbios-type** to restore the default.

Syntax

netbios-type { **b-node** | **h-node** | **m-node** | **p-node** }

undo netbios-type

Default

No NetBIOS node type is specified.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

b-node: Specifies the broadcast node. A b-node client sends the destination name in a broadcast message to get the name-to-IP mapping from a server.

h-node: Specifies the hybrid node. An h-node client unicasts the destination name to a WINS server. If it does not receive a response, the h-node client broadcasts the destination name to get the mapping from a server.

m-node: Specifies the mixed node. An m-node client broadcasts the destination name. If it does not receive a response, the m-node client unicasts the destination name to the WINS server to get the mapping.

p-node: Specifies the peer-to-peer node. A p-node client sends the destination name in a unicast message to get the mapping from the WINS server.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify the NetBIOS node type as p-node in DHCP address pool 0.

```
<Switch> system-view
[Switch] dhcp server ip-pool 0
[Switch-dhcp-pool-0] netbios-type p-node
```

Related commands

display dhcp server pool

nbns-list

6.2.24. network

Use **network** to specify the subnet for dynamic allocation in a DHCP address pool.

Use **undo network** to remove the specified subnet.

Syntax

network *network-address* [*mask-length* | **mask** *mask*] [**secondary**]

undo network *network-address* [*mask-length* | **mask** *mask*] [**secondary**]

Default

No subnet is specified in a DHCP address pool.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

network-address: Specifies the subnet for dynamic allocation. If no mask length or mask is specified, the natural mask will be used.

mask-length: Specifies the mask length in the range of 1 to 30.

mask *mask*: Specifies the mask in dotted decimal format.

secondary: Specifies the subnet as a secondary subnet. If you do not specify this keyword, this command specifies the primary subnet. If the addresses in the primary subnet are used up, the DHCP server can select addresses from a secondary subnet for clients.

Usage guidelines

You can use the **secondary** keyword to specify a secondary subnet and enter its view. In secondary subnet view, you can specify gateways by using the **gateway-list** command for DHCP clients in the secondary subnet.

You can specify only one primary subnet for a DHCP address pool. If you execute the **network** command multiple times, the most recent configuration takes effect.

You can specify up to 32 secondary subnets for a DHCP address pool.

The primary subnet and secondary subnets in a DHCP address pool must not have the same network address and mask.

If you have used the **address range** or **class** command in an address pool, you cannot specify a secondary subnet in the same address pool.

Modifying or removing the **network** configuration deletes the assigned addresses from the current address pool.

Examples

Specify primary subnet 192.168.8.0/24 and secondary subnet 192.168.10.0/24 in DHCP address pool 0.

```
<Switch> system-view
[Switch] dhcp server ip-pool 0
[Switch-dhcp-pool-0] network 192.168.8.0 mask 255.255.255.0
[Switch-dhcp-pool-0] network 192.168.10.0 mask 255.255.255.0 secondary
[Switch-dhcp-pool-0-secondary]
```

Related commands

display dhcp server pool

gateway-list

6.2.25. next-server

Use **next-server** to specify the IP address of a server in a DHCP address pool.

Use **undo next-server** to restore the default.

Syntax

next-server *ip-address*

undo next-server

Default

No server's IP address is specified in a DHCP address pool.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the IP address of a server.

Usage guidelines

Upon startup, the DHCP client obtains an IP address and the specified server IP address. Then it contacts the specified server, such as a TFTP server, to get other boot information.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify a server's IP address 10.1.1.254 in DHCP address pool 0.

```
<Switch> system-view
[Switch] dhcp server ip-pool 0
[Switch-dhcp-pool-0] next-server 10.1.1.254
```

Related commands

display dhcp server pool

6.2.26. option

Use **option** to customize a DHCP option.

Use **undo option** to remove a customized DHCP option.

Syntax

option *code* { **ascii** *ascii-string* | **hex** *hex-string* | **ip-address** *ip-address*&<1-8> }

undo option *code*

Default

No DHCP option is customized.

Views

DHCP address pool view

DHCP option group view

Predefined user roles

network-admin

Parameters

code: Specifies the number of the customized option, in the range of 2 to 254, excluding 50 through 54, 56, 58, 59, 61, and 82.

ascii *ascii-string*: Specifies a case-sensitive ASCII string of 1 to 255 characters as the option content.

hex *hex-string*: Specifies a hexadecimal number as the option content. The length of the hexadecimal number must be an even number in the range of 2 to 256.

ip-address *ip-address*&<1-8>: Specifies a space-separated list of up to eight IP addresses as the option content.

Usage guidelines

The DHCP server fills the customized option with the specified ASCII string, hexadecimal number, or IP addresses, and sends it in a response to the client.

You can customize options for the following purposes:

- Add newly released options.
- Add options for which the vendor defines the contents, for example, Option 43.
- Add options for which the CLI does not provide a dedicated configuration command. For example, you can use the **option 4 ip-address 1.1.1.1** command to define the time server address 1.1.1.1 for DHCP clients.
- Add all option values if the actual requirement exceeds the limit for a dedicated option configuration command. For example, the **dns-list** command can specify up to eight DNS servers. To specify more than eight DNS server, you must use the **option 6** command to define all DNS servers.

DHCP options specified by dedicated commands take precedence over those specified by the **option** commands. For example, if a DNS server address is specified by both the **dns-list** command and the **option 6** command, the server uses the address specified by the **dns-list** command.

DHCP options specified in DHCP option groups take precedence over those specified in DHCP address pools.

If you execute this command multiple times with the same *code* specified, the most recent configuration takes effect.

Examples

Configure Option 7 to specify log server address 2.2.2.2 in DHCP address pool 0.

```
<Switch> system-view
[Switch] dhcp server ip-pool 0
[Switch-dhcp-pool-0] option 7 ip-address 2.2.2.2
```

Related commands

display dhcp server pool

6.2.27. reset dhcp server conflict

Use **reset dhcp server conflict** to clear IP address conflict information.

Syntax

reset dhcp server conflict [**ip** *ip-address*]

Views

User view

Predefined user roles

network-admin

Parameters

ip *ip-address*: Clears conflict information about the specified IP address. If you do not specify this option, this command clears all address conflict information.

Usage guidelines

Address conflicts occur when dynamically assigned IP addresses have been statically configured for other hosts. After you modify the address pool configuration, the conflicted addresses might become assignable. To assign these addresses, use the **reset dhcp server conflict** command to clear the conflict information first.

Examples

Clear all IP address conflict information.

```
<Switch> reset dhcp server conflict
```

Related commands

display dhcp server conflict

6.2.28. reset dhcp server expired

Use **reset dhcp server expired** to clear binding information about expired IP addresses.

Syntax

reset dhcp server expired [**ip** *ip-address* | **pool** *pool-name*]

Views

User view

Predefined user roles

network-admin

Parameters

ip *ip-address*: Clears binding information about the specified expired IP address. If you do not specify an IP address, this command clears binding information about all expired IP addresses.

pool *pool-name*: Clears binding information about the expired IP addresses in the specified address pool. The pool name is a case-insensitive string of 1 to 63 characters. If you do not specify an address pool, this command clears binding information about expired IP addresses in all address pools.

Examples

Clear binding information about all expired IP addresses.

```
<Switch> reset dhcp server expired
```

Related commands

display dhcp server expired

6.2.29. reset dhcp server ip-in-use

Use **reset dhcp server ip-in-use** to clear binding information about assigned IP addresses.

Syntax

reset dhcp server ip-in-use [**ip** *ip-address* | **pool** *pool-name*]

Views

User view

Predefined user roles

network-admin

Parameters

ip *ip-address*: Clears binding information about the specified assigned IP address. If you do not specify an IP address, this command clears binding information about all assigned IP addresses.

pool *pool-name*: Clears binding information about assigned IP addresses in the specified address pool. The pool name is a case-insensitive string of 1 to 63 characters. If you do not specify an address pool, this command clears binding information about assigned IP addresses in all address pools.

Usage guidelines

If you use this command to clear information about an assigned static binding, the static binding becomes a free static binding.

Examples

Clear binding information about IP address 10.110.1.1.

```
<Switch> reset dhcp server ip-in-use ip 10.110.1.1
```

Related commands

display dhcp server ip-in-use

6.2.30. reset dhcp server statistics

Use **reset dhcp server statistics** to clear DHCP server statistics.

Syntax

reset dhcp server statistics

Views

User view

Predefined user roles

network-admin

Examples

Clear DHCP server statistics.

```
<Switch> reset dhcp server statistics
```

Related commands

display dhcp server statistics

6.2.31. static-bind

Use **static-bind** to statically bind a client ID or MAC address to an IP address.

Use **undo static-bind** to remove a static binding.

Syntax

static-bind ip-address *ip-address* [*mask-length* | **mask** *mask*] { **client-identifier** *client-identifier* | **hardware-address** *hardware-address* [**ethernet** | **token-ring**] }

undo static-bind ip-address *ip-address*

Default

No static binding is specified in a DHCP address pool.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

ip-address *ip-address*: Specifies the IP address of the static binding. The natural mask is used if no mask length or mask is specified.

mask-length: Specifies the mask length in the range of 1 to 30.

mask *mask*: Specifies the mask, in dotted decimal format.

client-identifier *client-identifier*: Specifies the client ID of the static binding, a string of 4 to 254 characters. The string can contain only hexadecimal numbers and hyphen (-), in the format of H-H-H…. The last H can be a two-digit or four-digit hexadecimal number while the other Hs must be all four-digit hexadecimal numbers. For example, aabb-cccc-dd is correct, and aabb-c-dddd and aabb-cc-dddd are not correct.

hardware-address *hardware-address*: Specifies the client hardware address of the static binding, a string of 4 to 39 characters. The string can contain only hexadecimal numbers and hyphen (-), in the format of H-H-H…. The last H can be a two-digit or four-digit hexadecimal number while the other Hs must be all four-digit hexadecimal numbers. For example, aabb-cccc-dd is correct, and aabb-c-dddd and aabb-cc-dddd are not correct.

ethernet: Specifies the client hardware address type as Ethernet. The default type is Ethernet.

token-ring: Specifies the client hardware address type as token ring.

Usage guidelines

The IP address of a static binding must not be an interface address of the DHCP server. Otherwise, an IP address conflict occurs, and the bound client cannot obtain the IP address.

You can specify multiple static bindings in an address pool. The total number of static bindings in all address pools cannot exceed 8192.

An IP address can be bound to only one DHCP client. To modify the binding for a DHCP client, first execute the **undo** form of the command to delete the existing binding and then create a new binding.

Examples

Bind IP address 10.1.1.1/24 to client ID **00aa-aabb** in DHCP address pool 0.

```
<Switch> system-view
[Switch] dhcp server ip-pool 0
[Switch-dhcp-pool-0] static-bind ip-address 10.1.1.1 mask 255.255.255.0
client-identifier 00aa-aabb
```

Related commands

display dhcp server pool

6.2.32. tftp-server domain-name

Use **tftp-server domain-name** to specify a TFTP server name in a DHCP address pool.

Use **undo tftp-server domain-name** to restore the default.

Syntax

tftp-server domain-name *domain-name*

undo tftp-server domain-name

Default

No TFTP server name is specified.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

domain-name: Specifies the TFTP server name, a case-sensitive string of 1 to 63 characters.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify TFTP server name **aaa** in DHCP address pool 0.

```
<Switch> system-view
[Switch] dhcp server ip-pool 0
[Switch-dhcp-pool-0] tftp-server domain-name aaa
```

Related commands

display dhcp server pool

tftp-server ip-address

6.2.33. tftp-server ip-address

Use **tftp-server ip-address** to specify a TFTP server address in a DHCP address pool.

Use **undo tftp-server ip-address** to restore the default.

Syntax

tftp-server ip-address *ip-address*

undo tftp-server ip-address

Default

No TFTP server address is specified.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the IP address of a TFTP server.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify TFTP server address 10.1.1.1 in DHCP address pool 0.

```
<Switch> system-view
[Switch] dhcp server ip-pool 0
[Switch-dhcp-pool-0] tftp-server ip-address 10.1.1.1
```

Related commands

display dhcp server pool

tftp-server domain-name

6.2.34. voice-config

Use **voice-config** to configure the content for Option 184 in a DHCP address pool.

Use **undo voice-config** to remove the Option 184 content from a DHCP address pool.

Syntax

voice-config { **as-ip** *ip-address* | **fail-over** *ip-address dialer-string* | **ncp-ip** *ip-address* | **voice-vlan** *vlan-id* { **disable** | **enable** } }

undo voice-config [**as-ip** | **fail-over** | **ncp-ip** | **voice-vlan**]

Default

No Option 184 content is configured in a DHCP address pool.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

as-ip *ip-address*: Specifies the IP address of the backup network calling processor.

fail-over *ip-address dialer-string*: Specifies the failover IP address and dialer string. The *dialer-string* is a string of 1 to 39 characters. Valid characters are digits and asterisk (*).

ncp-ip *ip-address*: Specifies the IP address of the primary network calling processor.

voice-vlan *vlan-id*: Specifies the voice VLAN ID in the range of 2 to 4094.

- **disable**: Disables the specified VLAN. DHCP clients will not take this VLAN as their voice VLAN.
- **enable**: Enables the specified VLAN. DHCP clients will take this VLAN as their voice VLAN.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure Option 184 in DHCP address pool 0. The primary and backup network calling processors are at 10.1.1.1 and 10.2.2.2, respectively. The voice VLAN 3 is enabled. The failover IP address is 10.3.3.3. The dialer string is 99*.

```
<Switch> system-view
[Switch] dhcp server ip-pool 0
[Switch-dhcp-pool-0] voice-config ncp-ip 10.1.1.1
[Switch-dhcp-pool-0] voice-config as-ip 10.2.2.2
[Switch-dhcp-pool-0] voice-config voice-vlan 3 enable
[Switch-dhcp-pool-0] voice-config fail-over 10.3.3.3 99*
```

Related commands

display dhcp server pool

6.3. DHCP relay agent commands

6.3.1. dhcp relay client-information record

Use **dhcp relay client-information record** to enable recording client information in relay entries.

Use **undo dhcp relay client-information record** to disable the feature.

Syntax

dhcp relay client-information record

undo dhcp relay client-information record

Default

The DHCP relay agent does not record client information in relay entries.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Client information is recorded only when the DHCP relay agent is configured on the gateway of DHCP clients. A relay entry contains information about a client such as the client's IP and MAC addresses.

Disabling the recording of client information deletes all recorded relay entries.

Examples

Enable the recording of relay entries on the relay agent.

```
<Switch> system-view
[Switch] dhcp relay client-information record
```

Related commands

dhcp relay client-information refresh enable

6.3.2. dhcp relay client-information refresh enable

Use **dhcp relay client-information refresh enable** to enable the DHCP relay agent to periodically refresh dynamic relay entries.

Use **undo dhcp relay client-information refresh enable** to disable the DHCP relay agent to periodically refresh dynamic relay entries.

Syntax

dhcp relay client-information refresh enable

undo dhcp relay client-information refresh enable

Default

The DHCP relay agent periodically refreshes relay entries.

Views

System view

Predefined user roles

network-admin

Usage guidelines

A DHCP client unicasts a DHCP-RELEASE message to the DHCP server to release its IP address. The DHCP relay agent conveys the message to the DHCP server and does not remove the IP-to-MAC entry of the client.

With this feature, the DHCP relay agent uses a client's IP address to periodically send a DHCP-REQUEST message to the DHCP server.

- If the server returns a DHCP-ACK message or does not return any message within an interval, the DHCP relay agent performs the following operations:
  - Removes the relay entry.
  - Sends a DHCP-RELEASE message to the DHCP server to release the IP address.
- If the server returns a DHCP-NAK message, the relay agent keeps the entry.

With this feature disabled, the DHCP relay agent does not remove relay entries automatically. After a DHCP client releases its IP address, you must use the **reset dhcp relay client-information** on the relay agent to remove the corresponding relay entry.

Examples

Disable periodic refresh of relay entries.

```
<Switch> system-view
[Switch] undo dhcp relay client-information refresh enable
```

Related commands

dhcp relay client-information record

dhcp relay client-information refresh

reset dhcp relay client-information

6.3.3. dhcp relay information circuit-id

Use **dhcp relay information circuit-id** to configure the padding mode and padding format for the Circuit ID sub-option of Option 82.

Use **undo dhcp relay information circuit-id** to restore the default.

Syntax

dhcp relay information circuit-id { **bas** | **string** *circuit-id* | **vxlan-port** | { **normal** | **verbose** [**node-identifier** { **mac** | **sysname** | **user-defined** *node-identifier* }] [**interface**] } [**format** { **ascii** | **hex** }] }

undo dhcp relay information circuit-id

Default

The padding mode is **normal** and the padding format is **hex**.

Views

Interface view

Predefined user roles

network-admin

Parameters

bas: Specifies the bas mode that uses the interface and VLAN information to pad the Circuit ID sub-option.

string *circuit-id*: Specifies the string mode that uses a case-sensitive string of 3 to 63 characters as the content of the Circuit ID sub-option.

vxlan-port: Specifies the mode that uses the VXLAN ID and port number to pad the Circuit ID sub-option.

normal: Specifies the normal mode, in which the padding content consists of the VLAN ID and port number.

verbose: Specifies the verbose mode. The padding content includes the node identifier, interface information, and VLAN ID. The default node identifier is the MAC address of the access node. The default interface information consists of the Ethernet type (fixed to **eth**), chassis number, slot number, sub-slot number, and interface number.

node-identifier { **mac** | **sysname** | **user-defined** *node-identifier* }: Specifies the access node identifier.

- **mac**: Uses the MAC address of the access node as the node identifier.
- **sysname**: Uses the device name as the node identifier. You can set the device name by using the **sysname** command in system view. The padding format for the device name is always ASCII regardless of the specified padding format.

NOTE:

If **sysname** is specified as the node identifier, do not include any spaces when you set the device name. Otherwise, the DHCP relay agent fails to add or replace Option 82.

- **user-defined** *node-identifier:* Uses a case-sensitive string of 1 to 50 characters as the node identifier. The padding format for the specified character string is always ASCII regardless of the specified padding format.

interface: Uses the interface name as the interface information. The padding format for the interface name is always ASCII regardless of the specified padding format.

format: Specifies the padding format for the Circuit ID sub-option.

ascii: Specifies the ASCII padding format.

hex: Specifies the hex padding format.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

The padding format for the string mode, the normal mode, or the verbose mode varies by command configuration. Table 6-7 shows how the padding format is determined for different modes.

Table 6-7 Padding format for different modes

Keyword (mode)	If no padding format is set	If the padding format is ascii	If the padding format is hex
string *circuit-id*	The padding format is ASCII, and is not configurable.	N/A	N/A
normal	Hex.	ASCII.	Hex.
verbose	Hex for the VLAN ID. ASCII for the node identifier, Ethernet type, chassis number, slot number, sub-slot number, and interface number.	ASCII.	ASCII for the node identifier and Ethernet type. Hex for the chassis number, slot number, sub-slot number, interface number, and VLAN ID.

Examples

Specify the content mode as verbose, node identifier as the device name, and the padding format as ASCII for the Circuit ID sub-option.

```
<Switch> system-view
[Switch] interface vlan-interface 10
[Switch-Vlan-interface10] dhcp relay information enable
[Switch-Vlan-interface10] dhcp relay information strategy replace
[Switch-Vlan-interface10] dhcp relay information circuit-id verbose node-identifier
sysname format ascii
```

Related commands

dhcp relay information enable

dhcp relay information strategy

display dhcp relay information

6.3.4. dhcp relay information enable

Use **dhcp relay information enable** to enable the DHCP relay agent to support Option 82.

Use **undo dhcp relay information enable** to disable Option 82 support.

Syntax

dhcp relay information enable

undo dhcp relay information enable

Default

The DHCP relay agent does not support Option 82.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

This command enables the DHCP relay agent to add Option 82 to DHCP requests that do not contain Option 82 before forwarding the requests to the DHCP server. The content of Option 82 is determined by the **dhcp relay information circuit-id** and **dhcp relay information remote-id** commands. If the DHCP requests contain Option 82, the relay agent handles the requests according to the strategy configured with the **dhcp relay information strategy** command.

If this feature is disabled, the relay agent forwards requests that contain or do not contain Option 82 to the DHCP server.

Examples

Enable Option 82 support on the relay agent.

```
<Switch> system-view
[Switch] interface vlan-interface 10
[Switch-Vlan-interface10] dhcp relay information enable
```

Related commands

dhcp relay information circuit-id

dhcp relay information remote-id

dhcp relay information strategy

display dhcp relay information

6.3.5. dhcp relay information remote-id

Use **dhcp relay information remote-id** to configure the padding mode and padding format for the Remote ID sub-option of Option 82.

Use **undo dhcp relay information remote-id** to restore the default.

Syntax

dhcp relay information remote-id { **normal** [**format** { **ascii** | **hex** }] | **string** *remote-id* | **sysname** }

undo dhcp relay information remote-id

Default

The padding mode is **normal** and the padding format is **hex**.

Views

Interface view

Predefined user roles

network-admin

Parameters

normal: Specifies the normal mode in which the padding content is the MAC address of the receiving interface.

format: Specifies the padding format for the Remote ID sub-option. The default padding format is hex.

ascii: Specifies the ASCII padding format.

hex: Specifies the hex padding format.

string *remote-id*: Specifies the string mode that uses a case-sensitive string of 1 to 63 characters as the content of the Remote ID sub-option.

sysname: Specifies the sysname mode that uses the device name as the content of the Remote ID sub-option. You can set the device name by using the **sysname** command.

Usage guidelines

The padding format for the specified character string (**string**) or the device name (**sysname**) is always ASCII. The padding format for the **normal** mode is determined by the command.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify the padding content for the Remote ID sub-option of Option 82 as **device001**.

```
<Switch> system-view
[Switch] interface vlan-interface 10
[Switch-Vlan-interface10] dhcp relay information enable
[Switch-Vlan-interface10] dhcp relay information strategy replace
[Switch-Vlan-interface10] dhcp relay information remote-id string device001
```

Related commands

dhcp relay information enable

dhcp relay information strategy

display dhcp relay information

6.3.6. dhcp relay information strategy

Use **dhcp relay information strategy** to configure the strategy for the DHCP relay agent to handle messages containing Option 82.

Use **undo dhcp relay information strategy** to restore the default handling strategy.

Syntax

dhcp relay information strategy { **drop** | **keep** | **replace** }

undo dhcp relay information strategy

Default

The handling strategy for messages that contain Option 82 is **replace**.

Views

Interface view

Predefined user roles

network-admin

Parameters

drop: Drops DHCP messages that contain Option 82 messages.

keep: Keeps the original Option 82 intact and forwards the DHCP messages.

replace: Replaces the original Option 82 with the configured Option 82 before forwarding the DHCP messages.

Usage guidelines

This command takes effect only on DHCP requests that contain Option 82.

For DHCP requests that do not contain Option 82, the DHCP relay agent always adds Option 82 to the requests before forwarding the requests to the DHCP server.

If the handling strategy is **replace**, configure a padding mode and padding format for Option 82. If the handling strategy is **keep** or **drop**, you do not need to configure any padding mode or padding format. The settings do not take effect even if you configure them.

Examples

Specify the handling strategy for Option 82 as **keep**.

```
<Switch> system-view
[Switch] interface vlan-interface 10
[Switch-Vlan-interface10] dhcp relay information enable
[Switch-Vlan-interface10] dhcp relay information strategy keep
```

Related commands

dhcp relay information enable

display dhcp relay information

6.3.7. dhcp relay release ip

Use **dhcp relay release ip** to release a client IP address.

Syntax

dhcp relay release ip *ip-address* [**vpn-instance** *vpn-instance-name*]

Views

System view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the IP address to be released.

vpn-instance *vpn-instance-name*: Specifies the VPN instance to which the specified IP address belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command releases the IP address on the public network.

Usage guidelines

After you execute this command, the relay agent sends a DHCP-RELEASE packet to the DHCP server and removes the relay entry of the IP address. Upon receiving the packet, the server removes binding information about the specified IP address to release the IP address.

Examples

Release IP address 1.1.1.1.

```
<Switch> system-view
[Switch] dhcp relay release ip 1.1.1.1
```

6.3.8. dhcp relay request-from-tunnel discard

Use **dhcp relay request-from-tunnel discard** to configure the DHCP relay agent to discard the DHCP requests that are delivered from VXLAN tunnels.

Use **undo dhcp relay request-from-tunnel discard** to restore the default.

Syntax

dhcp relay request-from-tunnel discard

undo dhcp relay request-from-tunnel discard

Default

The DHCP relay agent can forward the DHCP requests that are delivered from VXLAN tunnels.

Views

VXLAN VSI interface view

Predefined user roles

network-admin

Usage guidelines

In a VXLAN network, the DHCP relay agent feature can be configured on the VSI interface of a VTEP.

When the DHCP relay agent receives a DHCP request from an AC mapped to the VSI interface, the relay agent forwards this request to the DHCP servers and broadcasts this request to other VTEPs. If those VTEPs also function as the DHCP relay agents, each will forward the DHCP request to the DHCP servers they are connecting to. To prevent a DHCP server from receiving the same DHCP request from different VTEPs, you can configure this command on the VSI interface of the VTEPs that are not directly connecting to DHCP clients.

Examples

Configure the DHCP relay agent to discard the DHCP requests that are delivered from VXLAN tunnels.

```
<Switch> system-view
[Switch] interface vsi-interface 1
[Switch-Vsi-interface1] dhcp relay request-from-tunnel discard
```

6.3.9. dhcp relay server-address

Use **dhcp relay server-address** to specify DHCP servers on the DHCP relay agent.

Use **undo dhcp relay server-address** to remove DHCP servers.

Syntax

dhcp relay server-address *ip-address* [**class** *class-name*] [**public** | **vpn-instance** *vpn-instance-name*]

undo dhcp relay server-address [*ip-address* [**public** | **vpn-instance** *vpn-instance-name*]]

Default

No DHCP server is specified on the DHCP relay agent.

Views

Interface view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the IP address of a DHCP server. The DHCP relay agent forwards DHCP packets received from DHCP clients to this DHCP server.

class *class-name*: Specifies a DHCP user class to match DHCP request packets. The class name is a case-sensitive string of 1 to 63 characters. If you do not specify this option, no DHCP user class is used to match DHCP requests.

public: Specifies that the DHCP server is on the public network.

vpn-instance *vpn-instance-name*: Specifies the VPN instance to which the specified IP address belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays the relay entry for the specified IP address on the public network. If there is a specified DHCP server in the same VPN as the VLAN interface for which you want to set the **dhcp relay server-address** setting, the **vpn-instance** setting is not required.

Usage guidelines

The specified IP address of the DHCP server must not reside on the same subnet as the IP address of the DHCP relay agent interface. Otherwise, the DHCP clients might fail to obtain IP addresses.

You can specify a maximum of eight DHCP servers on an interface.

After receiving a DHCP request, the DHCP relay agent forwards the packets as follows:

- If the request matches a user class rule, the DHCP relay agent forwards the packet to DHCP servers that are configured with the user class.
- If the request does not match any user class rule, the DHCP relay agent forwards the request to DHCP servers with no user classes configured.

If you execute this command with the same user class but different values for the *ip-address* argument, you specify the same user class for different DHCP servers. If you execute the command with different user classes for the same *ip-address*, the most recent configuration takes effect.

If you do not specify an IP address, the **undo dhcp relay server-address** command removes all DHCP servers on the interface.

If the DHCP server selecting algorithm is **master-backup**, make sure both the master and backup servers have the same user class configured or have no user classes configured. Otherwise, DHCP clients cannot obtain IP addresses correctly.

Examples

Specify DHCP server address 1.1.1.1 on VLAN-interface 10.

```
<Switch> system-view
[Switch] interface vlan-interface 10
[Switch-Vlan-interface10] dhcp relay server-address 1.1.1.1
```

Related commands

dhcp select relay

display dhcp relay interface

6.3.10. display dhcp relay client-information

Use **display dhcp relay client-information** to display relay entries on the relay agent.

Syntax

display dhcp relay client-information [**interface** *interface-type interface-number* | **ip** *ip-address* [**vpn-instance** *vpn-instance-name*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Displays relay entries on the specified interface. If you do not specify an interface, this command displays relay entries on all interfaces.

ip *ip-address*: Displays the relay entry for the specified IP address. If you do not specify an IP address, this command displays relay entries for all IP addresses.

vpn-instance *vpn-instance-name*: Specifies the VPN instance to which the specified IP address belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays the relay entry for the specified IP address on the public network.

Usage guidelines

The DHCP relay agent records relay entries only after you configure the **dhcp relay client-information record** command.

Examples

Display all relay entries on the relay agent.

```
<Switch> display dhcp relay client-information
Total number of client-information items: 2
Total number of dynamic items: 1
Total number of temporary items: 1
IP address       MAC address      Type        Interface           VPN name
10.1.1.5         00e0-0000-0000   Temporary   Vlan2               N/A
```

Table 6-8 Command output

Field	Description
Total number of client-information items	Total number of relay entries.
Total number of dynamic items	Total number of dynamic relay entries.
Total number of temporary items	Total number of temporary relay entries.
IP address	IP address of the DHCP client.
MAC address	MAC address of the DHCP client.
Type	Relay entry type: • **Dynamic**—The relay agent creates a dynamic relay entry upon receiving an ACK response from the DHCP server. • **Temporary**—The relay agent creates a temporary relay entry upon receiving a REQUEST packet from a DHCP client.
Interface	Layer 3 interface connected to the DHCP client. **N/A** is displayed for relay entries without interface information.
VPN name	Name of the VPN instance to which the DHCP client belongs. If the DHCP client does not belong to any VPN, this field displays **N/A**.

Related commands

dhcp relay client-information record

reset dhcp relay client-information

6.3.11. display dhcp relay information

Use **display dhcp relay information** to display Option 82 configuration information for the DHCP relay agent.

Syntax

display dhcp relay information [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Displays Option 82 configuration information for the specified interface. If you do not specify an interface, this command displays Option 82 configuration information about all interfaces.

Examples

Display Option 82 configuration information for all interfaces.

```
<Switch> display dhcp relay information
Interface: Vlan-interface100
   Status: Enable
   Strategy: Replace
   Circuit ID Pattern: Verbose
   Remote ID Pattern: Sysname
   Circuit ID format-type: Undefined
   Remote ID format-type: ASCII
   Node identifier: aabbcc
Interface: Vlan-interface200
   Status: Enable
   Strategy: Replace
   Circuit ID Pattern: User Defined
   Remote ID Pattern: User Defined
   Circuit ID format-type: ASCII
   Remote ID format-type: ASCII
   User defined:
   Circuit ID: vlan100
   Remote ID: device001
```

Table 6-9 Command output

Field	Description
Interface	Interface name.
Status	Option 82 states: • **Enable**—DHCP relay agent support for Option 82 is enabled. • **Disable**—DHCP relay agent support for Option 82 is disabled.
Strategy	Handling strategy for request messages containing Option 82, **Drop**, **Keep**, or **Replace**.
Circuit ID Pattern	Padding content mode of the Circuit ID sub-option, **Verbose**, **Normal**, or **User Defined**.
Remote ID Pattern	Padding content mode of the Remote ID sub-option, **Sysname**, **Normal**, or **User Defined**.
Circuit ID format-type	Padding format of the Circuit ID sub-option, **ASCII**, **Hex**, or **Undefined**.
Remote ID format-type	Padding format of the Remote ID sub-option, **ASCII**, **Hex**, or **Undefined**.
Node identifier	Access node identifier.
User defined	Content of the user-defined sub-options.
Circuit ID	User-defined content of the Circuit ID sub-option.
Remote ID	User-defined content of the Remote ID sub-option.

6.3.12. display dhcp relay server-address

Use **display dhcp relay server-address** to display DHCP server addresses configured on an interface.

Syntax

display dhcp relay server-address [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Displays DHCP server addresses on the specified interface. If you do not specify an interface, this command displays DHCP server addresses on all interfaces.

Examples

Display DHCP server addresses on all interfaces.

```
<Switch> display dhcp relay server-address
Interface name      Server IP address   Public/VRF name      Class name
Vlan2               2.2.2.2             Y/--                 --
Vlan2               2.2.2.3             Y/--                 abc
```

Table 6-10 Command output

Field	Description
Interface name	Interface name.
Server IP address	DHCP server IP address.
Public/VRF name	Location of the DHCP server, which is determined by the configuration of the **dhcp relay server-address** command. • If neither the **public** keyword nor the **vpn-instance** *vpn-instance-name* option is specified, this field displays **--/--**. • If the **public** keyword is specified, this field displays **Y/--**. • If the **vpn-instance** *vpn-instance-name* option is specified, the VPN instance name is displayed after the slash (/), for example, **--/abc**.
Class name	Name of a DHCP user class to match DHCP requests. This field displays hyphens (**--**) if the **class** *class-name* option is not specified in the **dhcp relay server-address** command.

Related commands

dhcp relay server-address

6.3.13. display dhcp relay statistics

Use **display dhcp relay statistics** to display DHCP packet statistics on the DHCP relay agent.

Syntax

display dhcp relay statistics [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Displays DHCP packet statistics on the specified interface. If you do not specify an interface, this command displays all DHCP packet statistics on the DHCP relay agent.

Examples

Display all DHCP packet statistics on the DHCP relay agent.

```
<Switch> display dhcp relay statistics
DHCP packets dropped:                   0
DHCP packets received from clients:     0
   DHCPDISCOVER:                        0
   DHCPREQUEST:                         0
   DHCPINFORM:                          0
   DHCPRELEASE:                         0
   DHCPDECLINE:                         0
   BOOTPREQUEST:                        0
DHCP packets received from servers:     0
   DHCPOFFER:                           0
   DHCPACK:                             0
   DHCPNAK:                             0
   BOOTPREPLY:                          0
DHCP packets relayed to servers:        0
   DHCPDISCOVER:                        0
   DHCPREQUEST:                         0
   DHCPINFORM:                          0
   DHCPRELEASE:                         0
   DHCPDECLINE:                         0
   BOOTPREQUEST:                        0
DHCP packets relayed to clients:        0
   DHCPOFFER:                           0
   DHCPACK:                             0
   DHCPNAK:                             0
   BOOTPREPLY:                          0
DHCP packets sent to servers:           0
```

```
    DHCPDISCOVER:                    0
    DHCPREQUEST:                     0
    DHCPINFORM:                      0
    DHCPRELEASE:                     0
    DHCPDECLINE:                     0
    BOOTPREQUEST:                    0
DHCP packets sent to clients:        0
    DHCPOFFER:                       0
    DHCPACK:                         0
    DHCPNAK:                         0
    BOOTPREPLY:                      0
```

Related commands

reset dhcp relay statistics

6.3.14. reset dhcp relay client-information

Use **reset dhcp relay client-information** to clear relay entries on the DHCP relay agent.

Syntax

reset dhcp relay client-information [**interface** *interface-type interface-number* | **ip** *ip-address* [**vpn-instance** *vpn-instance-name*]]

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Clears relay entries on the specified interface. If you do not specify an interface, this command clears relay entries on all interfaces.

ip *ip-address*: Clears the relay entry for the specified IP address. If you do not specify an IP address, this command clears relay entries for all IP addresses.

vpn-instance *vpn-instance-name*: Specifies the VPN instance to which the specified IP address belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command clears the relay entry for the specified IP address on the public network.

Examples

Clear all relay entries on the DHCP relay agent.

```
<Switch> reset dhcp relay client-information
```

Related commands

display dhcp relay client-information

6.3.15. reset dhcp relay statistics

Use **reset dhcp relay statistics** to clear relay agent statistics.

Syntax

reset dhcp relay statistics [**interface** *interface-type interface-number*]

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command clears all DHCP relay agent statistics.

Examples

Clear all DHCP relay agent statistics.

```
<Switch> reset dhcp relay statistics
```

Related commands

display dhcp relay statistics

6.4. DHCP client commands

6.4.1. dhcp client dad enable

Use **dhcp client dad enable** to enable duplicate address detection.

Use **undo dhcp client dad enable** to disable duplicate address detection.

Syntax

dhcp client dad enable

undo dhcp client dad enable

Default

Duplicate address detection is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

DHCP client detects IP address conflict through ARP packets. An attacker can act as the IP address owner to send an ARP reply. This makes the client unable to use the IP address assigned by the server. As a best practice, disable duplicate address detection when ARP attacks exist on the network.

Examples

Disable the duplicate address.

```
<Switch> system-view
[Switch] undo dhcp client dad enable
```

6.4.2. dhcp client dscp

Use **dhcp client dscp** to set the DSCP value for DHCP packets sent by the DHCP client.

Use **undo dhcp client dscp** to restore the default.

Syntax

dhcp client dscp *dscp-value*

undo dhcp client dscp

Default

The DSCP value is 56 in DHCP packets sent by the DHCP client.

Views

System view

Predefined user roles

network-admin

Parameters

dscp-value: Sets the DSCP value for DHCP packets, in the range of 0 to 63.

Usage guidelines

The DSCP value of a packet specifies the priority level of the packet and affects the transmission priority of the packet. A bigger DSCP value represents a higher priority.

Examples

Set the DSCP value to 30 for DHCP packets sent by the DHCP client.

```
<Switch> system-view
[Switch] dhcp client dscp 30
```

6.4.3. display dhcp client

Use **display dhcp client** to display DHCP client information.

Syntax

display dhcp client [**verbose**] [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

verbose: Displays detailed DHCP client information. If you do not specify this keyword, the command displays brief DHCP client information.

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays DHCP client information on all interfaces.

Examples

Display brief DHCP client information on all interfaces.

```
<Switch> display dhcp client
Vlan-interface10 DHCP client information:
 Current state: BOUND
 Allocated IP: 40.1.1.20 255.255.255.0
 Allocated lease: 259200 seconds, T1: 129600 seconds, T2: 226800 seconds
 DHCP server: 40.1.1.2
```

Display detailed DHCP client information on all interfaces.

```
<Switch> display dhcp client verbose
Vlan-interface10 DHCP client information:
 Current state: BOUND
 Allocated IP: 40.1.1.20 255.255.255.0
 Allocated lease: 259200 seconds, T1: 129600 seconds, T2: 226800 seconds
 Lease from May 21 19:00:29 2012   to   May 31 19:00:29 2012
 DHCP server: 40.1.1.2
 Transaction ID: 0x1c09322d
 Default router: 40.1.1.2
 Classless static routes:
   Destination: 1.1.0.1, Mask: 255.0.0.0, NextHop: 192.168.40.16
   Destination: 10.198.122.63, Mask: 255.255.255.255, NextHop: 192.168.40.16
 DNS servers: 44.1.1.11 44.1.1.12
 Domain name: ddd.com
 Boot servers: 200.200.200.200  1.1.1.1
 ACS parameter:
   URL: http://192.168.1.1:7547/acs
   Username: bims
   Password: ******
 Client ID type: acsii(type value=00)
 Client ID value: 000c.29d3.8659-Vlan10
 Client ID (with type) hex: 0030-3030-632e-3239-
                            6433-2e38-3635-392d-
                            4574-6830-2f30-2f32
 T1 will timeout in 1 day 11 hours 58 minutes 52 seconds.
```

Table 6-11 Command output

Field	Description
DHCP client information	Information about the interface that acts as the DHCP client.
Current state	Current state of the DHCP client: • **HALT**—The client stops applying for an IP address. • **INIT**—The initialization state. • **SELECTING**—The client has sent out a DHCP-DISCOVER message in search for a DHCP server and is waiting for the response from DHCP servers. • **REQUESTING**—The client has sent out a

Field	Description
	DHCP-REQUEST message requesting for an IP address and is waiting for the response from DHCP servers. • **BOUND**—The client has received the DHCP-ACK message from a DHCP server and obtained an IP address successfully. • **RENEWING**—The T1 timer expires. • **REBOUNDING**—The T2 timer expires.
Allocated IP	IP address allocated by the DHCP server.
Allocated lease	Allocated lease time.
T1	1/2 lease time (in seconds) of the DHCP client IP address.
T2	7/8 lease time (in seconds) of the DHCP client IP address.
Lease from….to….	Start and end time of the lease.
DHCP server	DHCP server IP address that assigned the IP address.
Transaction ID	Transaction ID, a random number chosen by the client to identify an IP address allocation.
Default router	Gateway address assigned to the client.
Classless static routes	Classless static routes assigned to the client.
Static routes	Classful static routes assigned to the client.
DNS servers	DNS server address assigned to the client.
Domain name	Domain name suffix assigned to the client.
Boot servers	PXE server addresses (up to 16 addresses) specified for the DHCP client, which are obtained through Option 43.
ACS parameter	Parameters about the ACS.
URL	URL of the ACS.
Username	Username for logging in to the ACS.
Password	Password for logging in to the ACS. If a password is configured, this field displays ******. If no password is configured, this field is not displayed.
Client ID type	DHCP client ID type: • If an ASCII string is used as the client ID value, the type value is 00. • If the MAC address of a specific interface is used as the client ID value, the type value is 01. • If a hexadecimal number is used as the client ID value, the type value is the first two characters in the string.
Client ID value	Value of the DHCP client ID.
Client ID (with type) hex	DHCP client ID with the type field, a hexadecimal number.
T1 will timeout in 1 day 11 hours 58 minutes 52 seconds.	How long the T1 (1/2 lease time) timer will timeout.

Related commands

ip address dhcp-alloc

6.4.4. ip address dhcp-alloc

Use **ip address dhcp-alloc** to configure an interface to use DHCP for IP address acquisition.

Use **undo ip address dhcp-alloc** to cancel an interface from using DHCP.

Syntax

ip address dhcp-alloc

undo ip address dhcp-alloc

Default

An interface does not use DHCP for IP address acquisition.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

When you execute the **undo ip address dhcp-alloc** command, the interface sends a DHCP-RELEASE message to release the IP address obtained through DHCP. If the interface is down, the message cannot be sent out. This situation can occur when a subinterface obtained an IP address through DHCP, and the **shutdown** command is executed on its primary interface. The subinterface will fail to send a DHCP-RELEASE message.

Examples

Configure VLAN-interface 10 to use DHCP for IP address acquisition.

```
<Switch> system-view
[Switch] interface vlan-interface 10
[Switch-Vlan-interface10] ip address dhcp-alloc
```

6.5. DHCP snooping commands

DHCP snooping works between the DHCP client and the DHCP server or between the DHCP client and the relay agent. DHCP snooping does not work between the DHCP server and the DHCP relay agent.

6.5.1. dhcp snooping binding record

Use **dhcp snooping binding record** to enable recording of client information in DHCP snooping entries.

Use **undo dhcp snooping binding record** to disable recording of client information in DHCP snooping entries.

Syntax

dhcp snooping binding record

undo dhcp snooping binding record

Default

DHCP snooping does not record client information.

Views

Layer 2 Ethernet interface/Layer 2 aggregate interface view

VSI view

VLAN view

Predefined user roles

network-admin

Usage guidelines

This command enables DHCP snooping on the port directly connecting to the clients to record client information in DHCP snooping entries.

If you configure this command in a VSI view, this command takes effect on the ACs that are mapped to the VSI and the VXLAN tunnel interfaces that are assigned to the VSI.

Examples

Enable the recording of client information in DHCP snooping entries on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] dhcp snooping binding record
```

6.5.2. dhcp snooping enable

Use **dhcp snooping enable** to enable DHCP snooping globally.

Use **undo dhcp snooping enable** to disable DHCP snooping globally.

Syntax

dhcp snooping enable

undo dhcp snooping enable

Default

DHCP snooping is disabled globally.

Views

System view

Predefined user roles

network-admin

Usage guidelines

After you enable DHCP snooping globally on the device, trusted ports forward responses from DHCP servers and untrusted ports discard responses. This mechanism ensures that DHCP clients obtain IP addresses from authorized DHCP servers.

When DHCP snooping is disabled globally, all ports on the device can forward responses from DHCP servers.

Examples

Enable DHCP snooping globally.

```
<Switch> system-view
```

```
[Switch] dhcp snooping enable
```

6.5.3. dhcp snooping information circuit-id

Use **dhcp snooping information circuit-id** to configure the padding mode and padding format for the Circuit ID sub-option.

Use **undo dhcp snooping information circuit-id** to restore the default.

Syntax

dhcp snooping information circuit-id { [**vlan** *vlan-id*] **string** *circuit-id* | { **normal** | **verbose** [**node-identifier** { **mac** | **sysname** | **user-defined** *node-identifier* }] } [**format** { **ascii** | **hex** }] }

undo dhcp snooping information circuit-id [**vlan** *vlan-id*]

Default

The padding mode is normal and the padding format is hex.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

vlan *vlan-id*: Pads the Circuit ID sub-option for packets received from the specified VLAN. If you do not specify a VLAN, the device pads the Circuit ID sub-option for packets received from the default VLAN.

string *circuit-id*: Specifies the string mode, in which the padding content for the Circuit ID sub-option is a case-sensitive string of 3 to 63 characters.

normal: Specifies the normal mode. The padding content includes the VLAN ID and interface number.

verbose: Specifies the verbose mode. The padding content includes the node identifier, interface information, and VLAN ID. The default node identifier is the MAC address of the access node. The default interface information consists of the Ethernet type (fixed to **eth**), chassis number, slot number, sub-slot number, and interface number.

node-identifier { **mac** | **sysname** | **user-defined** *node-identifier* }: Specifies the access node identifier.

- **mac**: Uses the MAC address of the access node as the node identifier.
- **sysname**: Uses the device name as the node identifier. You can set the device name by using the **sysname** command in system view. The padding format for the device name is always ASCII regardless of the specified padding format.

> **NOTE:**
> If **sysname** is specified as the node identifier, do not include any spaces when you set the device name. Otherwise, the DHCP snooping device fails to add or replace Option 82.

- **user-defined** *node-identifier*: Uses a case-sensitive string of 1 to 50 characters as the node identifier. The padding format for the specified character string is always ASCII regardless of the specified padding format.

format: Specifies the padding format for the Circuit ID sub-option.

ascii: Specifies the ASCII padding format.

hex: Specifies the hex padding format.

Usage guidelines

The Circuit ID sub-option cannot carry information about interface splitting or subinterfaces. For more information about interface splitting and subinterfaces, see *Interface Configuration Guide*.

If you execute this command multiple times, the most recent configuration takes effect.

The padding format for the string mode, the normal mode, or the verbose mode varies by command configuration. Table 6-12 shows how the padding format is determined for different modes.

Table 6-12 Padding format for different modes

Keyword (mode)	If no padding format is set	If the padding format is ascii	If the padding format is hex
string *circuit-id*	The padding format is always ASCII, and is not configurable.	N/A	N/A
normal	Hex.	ASCII.	Hex.
verbose	Hex for the VLAN ID. ASCII for the node identifier, Ethernet type, chassis number, slot number, sub-slot number, and interface number.	ASCII.	ASCII for the node identifier and Ethernet type. Hex for the chassis number, slot number, sub-slot number, interface number, and VLAN ID.

Examples

Configure verbose as the padding mode, device name as the node identifier, and ASCII as the padding format for the Circuit ID sub-option.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] dhcp snooping information enable
[Switch-GigabitEthernet1/0/1] dhcp snooping information strategy replace
[Switch-GigabitEthernet1/0/1] dhcp snooping information circuit-id verbose
node-identifier sysname format ascii
```

Related commands

dhcp snooping information enable

dhcp snooping information strategy

display dhcp snooping information

6.5.4. dhcp snooping information enable

Use **dhcp snooping information enable** to enable DHCP snooping to support Option 82.

Use **undo dhcp snooping information enable** to disable this feature.

Syntax

dhcp snooping information enable

undo dhcp snooping information enable

Default

DHCP snooping does not support Option 82.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

This command enables DHCP snooping to add Option 82 into DHCP requests that do not contain Option 82 before forwarding the requests to the DHCP server. The content of Option 82 is determined by the **dhcp snooping information circuit-id** and **dhcp snooping information remote-id** commands. If the received DHCP request packets contain Option 82, DHCP snooping handles the packets according to the strategy configured by the **dhcp snooping information strategy** command.

Examples

Enable DHCP snooping to support Option 82.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] dhcp snooping information enable
```

Related commands

dhcp snooping information circuit-id

dhcp snooping information remote-id

dhcp snooping information strategy

6.5.5. dhcp snooping information remote-id

Use **dhcp snooping information remote-id** to configure the padding mode and padding format for the Remote ID sub-option.

Use **undo dhcp snooping information remote-id** to restore the default.

Syntax

dhcp snooping information remote-id { **normal** [**format** { **ascii** | **hex** }] | [**vlan** *vlan-id*] { **string** *remote-id* | **sysname** } }

undo dhcp snooping information remote-id [**vlan** *vlan-id*]

Default

The padding mode is normal and the padding format is hex.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

vlan *vlan-id*: Pads the Remote ID sub-option for packets received from the specified VLAN. If you do not specify a VLAN, the device pads the Remote ID sub-option for packets received from the default VLAN.

string *remote-id*: Specifies the string mode that uses a case-sensitive string of 1 to 63 characters as the content of the Remote ID sub-option.

sysname: Specifies the sysname mode that uses the device name as the Remote ID sub-option. You can configure the device name by using the **sysname** command in system view.

normal: Specifies the normal mode. The padding content is the MAC address of the receiving interface.

format: Specifies the padding format for the Remote ID sub-option. The default padding format is hex.

ascii: Specifies the ASCII padding format.

hex: Specifies the hex padding format.

Usage guidelines

DHCP snooping uses ASCII to pad the specified string or device name for the Remote ID sub-option. The padding format for the normal padding mode is determined by the command configuration.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Pad the Remote ID sub-option with a character string of **device001**.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] dhcp snooping information enable
[Switch-GigabitEthernet1/0/1] dhcp snooping information strategy replace
[Switch-GigabitEthernet1/0/1] dhcp snooping information remote-id string device001
```

Related commands

dhcp snooping information enable

dhcp snooping information strategy

display dhcp snooping information

6.5.6. dhcp snooping information strategy

Use **dhcp snooping information strategy** to configure the handling strategy for Option 82 in request messages.

Use **undo dhcp snooping information strategy** to restore the default.

Syntax

dhcp snooping information strategy { **drop** | **keep** | **replace** }

undo dhcp snooping information strategy

Default

The handling strategy for Option 82 in request messages is **replace**.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

drop: Drops DHCP messages that contain Option 82.

keep: Keeps the original Option 82 intact and forwards the DHCP messages.

replace: Replaces the original Option 82 with the configured Option 82 before forwarding the DHCP messages.

Usage guidelines

This command takes effect only on DHCP requests that contain Option 82. For DHCP requests that do not contain Option 82, the DHCP snooping device always adds Option 82 into the requests before forwarding them to the DHCP server.

If the handling strategy is **replace**, configure a padding mode and a padding format for Option 82. If the handling strategy is **keep** or **drop**, you do not need to configure a padding mode or padding format for Option 82.

Examples

Specify the handling strategy for Option 82 in request messages as **keep**.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] dhcp snooping information enable
[Switch-GigabitEthernet1/0/1] dhcp snooping information strategy keep
```

Related commands

dhcp snooping information circuit-id

dhcp snooping information remote-id

6.5.7. dhcp snooping trust

Use **dhcp snooping trust** to configure a port as a trusted port.

Use **undo dhcp snooping trust** to restore the default state of a port.

Syntax

dhcp snooping trust

undo dhcp snooping trust

Default

After you enable DHCP snooping, all ports are untrusted.

Views

Layer 2 Ethernet interface/Layer 2 aggregate interface view

Layer 3 Ethernet interface view

Ethernet service instance view

Predefined user roles

network-admin

Usage guidelines

Specify the ports facing the DHCP server as trusted ports and specify the other ports as untrusted ports so DHCP clients can obtain valid IP addresses.

Examples

Specify Layer 2 Ethernet interface GigabitEthernet 1/0/1 as a trusted port.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] dhcp snooping trust
```

Related commands

display dhcp snooping trust

6.5.8. dhcp snooping trust tunnel

Use **dhcp snooping trust tunnel** to configure VXLAN tunnel interfaces assigned to a VSI as trusted interfaces.

Use **undo dhcp snooping trust tunnel** to restore the default.

Syntax

dhcp snooping trust tunnel

undo dhcp snooping trust tunnel

Default

After you enable DHCP snooping, all tunnel interfaces are untrusted.

Views

VSI view

Predefined user roles

network-admin

Examples

Configure the tunnel interfaces as trusted in the VSI **a**.

```
<Switch> system-view
[Switch] vsi a
[Switch-vsi-a] dhcp snooping trust tunnel
```

6.5.9. display dhcp snooping binding

Use **display dhcp snooping binding** to display DHCP snooping entries.

Syntax

display dhcp snooping binding [**ip** *ip-address* [**vlan** *vlan-id*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ip *ip-address*: Displays the DHCP snooping entry for the specified IP address.

vlan *vlan-id*: Specifies the VLAN ID where the IP address resides.

Usage guidelines

If you do not specify any parameters, this command displays all DHCP snooping entries.

Examples

Display summary information about all DHCP snooping entries.

```
<Switch> display dhcp snooping binding
 2 DHCP snooping entries found
 IP address      MAC address    Lease         VLAN  SVLAN Interface
 =============== ============== ============ ===== ===== =================
 1.1.1.7         0000-0101-0107 16907533     2     3     GE1/0/1
 1.1.1.11        0000-0101-010b 16907537     2     3     GE1/0/3
```

Display detailed information about all DHCP snooping entries.

```
<Switch> display dhcp snooping binding verbose
 IP address: 1.1.1.7
 MAC address: 0000-0101-0107
 Lease: 16907553 seconds
 VLAN: 2
 SVLAN: 3
 Interface: GigabitEthernet1/0/1
 Parameter request list: 03 06 21

 IP address: 1.1.1.104
 MAC address: 0000-0101-010b
 Lease: 16907537 seconds
 VLAN: 2
 SVLAN: 3
 Interface: GigabitEthernet1/0/3
 Parameter request list: 37 0B 01 0F 03 06 2C 2E 2F 1F 21 F9 2B
```

Table 6-13 Command output

Field	Description
DHCP snooping entries found	Number of DHCP snooping entries.
IP address	IP address assigned to the DHCP client.
MAC address	MAC address of the DHCP client.
Lease	Remaining lease duration in seconds.
VLAN	When both DHCP snooping and QinQ are enabled or the DHCP packet contains two VLAN tags, this field identifies the outer VLAN tag. Otherwise, it identifies the VLAN where the port connecting the DHCP client resides.
SVLAN	When both DHCP snooping and QinQ are enabled or the DHCP packet contains two VLAN tags, this field identifies the inner VLAN tag. Otherwise, it displays **N/A**.

Field	Description
Interface	Port connected to the DHCP client.
Parameter request list	Parameters that the DHCP client requests, in hexadecimal notation.

Related commands

dhcp snooping enable

reset dhcp snooping binding

6.5.10. display dhcp snooping information

Use **display dhcp snooping information** to display Option 82 configuration on the DHCP snooping device.

Syntax

display dhcp snooping information { **all** | **interface** *interface-type interface-number* }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

all: Displays Option 82 configuration on all Layer 2 Ethernet interfaces.

interface *interface-type interface-number*: Specifies an interface by its type and number.

Examples

Display Option 82 configuration on all interfaces.

```
<Switch> display dhcp snooping information all
Interface: Bridge-Aggregation1
   Status: Disable
   Strategy: Drop
   Circuit ID:
     Padding format: User Defined
       User defined: abcd
     Format: ASCII
   Remote ID:
     Padding format: Normal
     Format: ASCII
   VLAN 10:
     Circuit ID: abcd
     Remote ID: company
```

Table 6-14 Command output

Field	Description
Interface	Interface name.
Status	Option 82 status, **Enable** or **Disable**.
Strategy	Handling strategy for DHCP requests that contain Option 82, **Drop**, **Keep**, or **Replace**.
Circuit ID	Content of the Circuit ID sub-option.
Padding format	Padding format of Option 82: • For Circuit ID sub-option, the padding format can be **Normal**, **User Defined**, **Verbose (sysname)**, **Verbose (MAC)**, or **Verbose (user defined)**. • For Remote ID sub-option, the padding format can be **Normal**, **Sysname**, or **User Defined**.
Node identifier	Access node identifier.
User defined	Content of the user-defined sub-option.
Format	Code type of Option 82 sub-option: • For Circuit ID sub-option, the code type can be **ASCII**, **Default**, or **Hex**. • For Remote ID sub-option, the code type can be **ASCII** or **Hex**.
Remote ID	Content of the Remote ID sub-option.
VLAN	Pads Circuit ID sub-option and Remote ID sub-option in the DHCP packets received in the specified VLAN.

6.5.11. display dhcp snooping packet statistics

Use **display dhcp snooping packet statistics** to display DHCP packet statistics for DHCP snooping.

Syntax

display dhcp snooping packet statistics [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays DHCP packet statistics for the master device.

Examples

Display DHCP packet statistics for DHCP snooping.

```
<Switch> display dhcp snooping packet statistics
 DHCP packets received                  : 100
 DHCP packets sent                      : 200
 Invalid DHCP packets dropped           : 0
```

Related commands

reset dhcp snooping packet statistics

6.5.12. display dhcp snooping trust

Use **display dhcp snooping trust** to display information about trusted ports.

Syntax

display dhcp snooping trust

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display information about trusted ports.

```
<Switch> display dhcp snooping trust
 DHCP snooping is enabled.
 Interface                                Trusted          VLAN
 ========================                 =============    =======
 GigabitEthernet1/0/1                     Trusted
 GigabitEthernet1/0/2                     -                100
 GigabitEthernet1/0/3                     -                100, 200
```

Table 6-15 Command output

Field	Description
Interface	Interface name.
Trusted	For a DHCP snooping trusted port configured in system view, this field displays **Trusted**. For a trusted port configured in VLAN view, this field displays a hyphen (**-**).
VLAN	VLANs in which the port is configured as trusted. If a trusted port is configured after DHCP snooping is enabled globally, this field is empty.

Related commands

dhcp snooping trust

6.5.13. reset dhcp snooping binding

Use **reset dhcp snooping binding** to clear DHCP snooping entries.

Syntax

reset dhcp snooping binding { **all** | **ip** *ip-address* [**vlan** *vlan-id*] }

Views

User view

Predefined user roles

network-admin

Parameters

all: Clears all DHCP snooping entries.

ip *ip-address*: Clears the DHCP snooping entry for the specified IP address.

vlan *vlan-id*: Clears DHCP snooping entries for the specified VLAN. If you do not specify a VLAN, this command clears DHCP snooping entries for the default VLAN.

Examples

Clear all DHCP snooping entries.

```
<Switch> reset dhcp snooping binding all
```

Related commands

display dhcp snooping binding

6.5.14. reset dhcp snooping packet statistics

Use **reset dhcp snooping packet statistics** to clear DHCP packet statistics for DHCP snooping.

Syntax

reset dhcp snooping packet statistics [**slot** *slot-number*]

Views

User view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears DHCP packet statistics for the master device.

Examples

Clear DHCP packet statistics for DHCP snooping.

```
<Switch> reset dhcp snooping packet statistics
```

Related commands

display dhcp snooping packet statistics

6.6. BOOTP client commands

6.6.1. display bootp client

Use **display bootp client** to display information about a BOOTP client.

Syntax

display bootp client [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays BOOTP client information on all interfaces.

Examples

Display BOOTP client information on VLAN-interface 10.

```
<Switch> display bootp client interface vlan-interface 10
Vlan-interface10 BOOTP client information:
Allocated IP: 169.254.0.2 255.255.0.0
Transaction ID: 0x3d8a7431
MAC Address: f474-880a-c3ef
```

Table 6-16 Command output

Field	Description
BOOTP client information	Information about the interface that acts as a BOOTP client.
Allocated IP	BOOTP client's IP address allocated by the BOOTP server.
Transaction ID	Value of the **XID** field in a BOOTP message. The BOOTP client chooses a random number for the **XID** field when sending a BOOTP request to the BOOTP server. It is used to match a response message from the BOOTP server. If the values of the **XID** field are different in the BOOTP response and request, the BOOTP client drops the BOOTP response.
Mac Address	MAC address of a BOOTP client.

Related commands

ip address bootp-alloc

6.6.2. ip address bootp-alloc

Use **ip address bootp-alloc** to configure an interface to use BOOTP for IP address acquisition.

Use **undo ip address bootp-alloc** to cancel an interface from using BOOTP.

Syntax

ip address bootp-alloc

undo ip address bootp-alloc

Default

An interface does not use BOOTP for IP address acquisition.

Views

Interface view

Predefined user roles

network-admin

Examples

Configure VLAN-interface 10 to use BOOTP for IP address acquisition.

```
<Switch> system-view
[Switch] interface vlan-interface 10
[Switch-Vlan-interface10] ip address bootp-alloc
```

Related commands

display bootp client

Contents

A page of this section is **4-x-x**

7. DNS commands 7-1
7.1. DNS commands 7-1
7.1.1. display dns domain 7-1
7.1.2. display dns host 7-2
7.1.3. display dns server 7-3
7.1.4. dns domain 7-4
7.1.5. dns dscp 7-5
7.1.6. dns proxy enable 7-5
7.1.7. dns server 7-6
7.1.8. ip host 7-6
7.1.9. reset dns host 7-7

7. DNS commands

7.1. DNS commands

7.1.1. display dns domain

Use **display dns domain** to display the domain name suffixes.

Syntax

display dns domain [**dynamic**] [**vpn-instance** *vpn-instance-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

dynamic: Displays the domain name suffixes dynamically obtained through DHCP or other protocols. If you do not specify this keyword, the command displays the statically configured and dynamically obtained domain name suffixes.

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays domain name suffixes for the public network.

Examples

Display the statically configured and dynamically obtained domain name suffixes for the public network.

```
<Switch> display dns domain
Type:
  D: Dynamic    S: Static

No.     Type    Domain suffix
1       S       com
2       D       net
```

Table 7-1 Command output

Field	Description
No.	Sequence number.
Type	Domain name suffix type: • **S**—A statically configured domain name suffix. • **D**—A domain name suffix dynamically obtained through DHCP or other protocols.
Domain suffix	Domain name suffixes.

Related commands

dns domain

7.1.2. display dns host

Use **display dns host** to display information about domain name-to-IP address mappings.

Syntax

display dns host [**ip**] [**vpn-instance** *vpn-instance-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ip: Specifies type A queries. A type A query resolves a domain name to the mapped IPv4 address.

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays domain name-to-IP address mappings for the public network.

Usage guidelines

If you do not specify the **ip** keyword, this command displays domain name-to-IP address mappings of all query types.

Examples

Display domain name-to-IP address mappings of all query types.

```
<Switch> display dns host
Type:
  D: Dynamic    S: Static

Total number: 3
No.  Host name          Type  TTL        Query type   IP addresses
1    sample.com         D     3132       A            192.168.10.1
                                                      192.168.10.2
                                                      192.168.10.3
2    zig.sample.com     S     -          A            192.168.1.1
3    sample.net         S     -          AAAA         FE80::4904:4448
```

Table 7-2 Command output

Field	Description
No.	Sequence number.
Host name	Domain name.
Type	Domain name-to-IP address mapping type: • **S**—A static mapping configured by the **ip host** command. • **D**—A mapping dynamically obtained through dynamic domain name resolution.

Field	Description
TTL	Time in seconds that a mapping can be stored in the cache. For a static mapping, a hyphen (-) is displayed.
Query type	Query type: A and AAAA.
IP addresses	Replied IP address: • For a type A query, the replied IP address is an IPv4 address. • For a type AAAA query, the replied IP address is an IPv6 address.

Related commands

ip host

reset dns host

7.1.3. display dns server

Use **display dns server** to display IPv4 DNS server information.

Syntax

display dns server [**dynamic**] [**vpn-instance** *vpn-instance-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

dynamic: Displays IPv4 DNS server information dynamically obtained through DHCP or other protocols. If you do not specify this keyword, the command displays statically configured and dynamically obtained IPv4 DNS server information.

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays IPv4 DNS server information for the public network.

Examples

Display IPv4 DNS server information for the public network.

```
<Switch> display dns server
Type:
  D: Dynamic    S: Static

No. Type  IP address
1   S     202.114.0.124
2   S     169.254.65.125
```

Table 7-3 Command output

Field	Description
No.	Sequence number.

Field	Description
Type	DNS server type: • **S**—A manually configured DNS server. • **D**—DNS server information dynamically obtained through DHCP or other protocols.
IP address	IPv4 address of the DNS server.

Related commands

dns server

7.1.4. dns domain

Use **dns domain** to configure a domain name suffix.

Use **undo dns domain** to delete the specified domain name suffix.

Syntax

dns domain *domain-name* [**vpn-instance** *vpn-instance-name*]

undo dns domain *domain-name* [**vpn-instance** *vpn-instance-name*]

Default

No domain name suffix is configured. Only the provided domain name is resolved.

Views

System view

Predefined user roles

network-admin

Parameters

domain-name: Specifies a domain name suffix. It is a dot-separated, case-insensitive string that can include letters, digits, hyphens (-), underscores (_), and dots (.), for example, aabbcc.com. The domain name suffix can include a maximum of 253 characters, and each separated string includes no more than 63 characters.

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. To configure a domain name suffix for the public network, do not specify this option.

Usage guidelines

For domain name resolution, the resolver automatically uses the suffix list to supply the missing part of an incomplete name entered by a user.

A domain name suffix applies to both IPv4 DNS.

The system allows a maximum of 16 domain name suffixes for the public network or each VPN instance. You can specify domain name suffixes for both public network and VPN instances.

Examples

Configure domain name suffix **com** for the public network.

```
<Switch> system-view
[Switch] dns domain com
```

Related commands

display dns domain

7.1.5. dns dscp

Use **dns dscp** to set the DSCP value for DNS packets sent by a DNS client or DNS proxy.

Use **undo dns dscp** to restore the default.

Syntax

dns dscp *dscp-value*

undo dns dscp

Default

The DSCP value is 0 in DNS packets sent by a DNS client or DNS proxy.

Views

System view

Predefined user roles

network-admin

Parameters

dscp-value: Specifies the DSCP value in the range of 0 to 63.

Usage guidelines

The DSCP value of a packet specifies the priority level of the packet and affects the transmission priority of the packet. A bigger DSCP value represents a higher priority.

Examples

Set the DSCP value to 30 for outgoing DNS packets.

```
<Switch> system-view
[Switch] dns dscp 30
```

7.1.6. dns proxy enable

Use **dns proxy enable** to enable DNS proxy.

Use **undo dns proxy enable** to disable DNS proxy.

Syntax

dns proxy enable

undo dns proxy enable

Default

DNS proxy is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This configuration applies to both IPv4 DNS.

Examples

Enable DNS proxy.

```
<Switch> system-view
[Switch] dns proxy enable
```

7.1.7. dns server

Use **dns server** to specify the IPv4 address of a DNS server.

Use **undo dns server** to remove the IPv4 address of a DNS server.

Syntax

dns server *ip-address* [**vpn-instance** *vpn-instance-name*]

undo dns server [*ip-address*] [**vpn-instance** *vpn-instance-name*]

Default

No DNS server IPv4 address is specified.

Views

System view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the IPv4 address of a DNS server.

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. To specify a DNS server IPv4 address for the public network, do not use this option.

Usage guidelines

The device sends a DNS query request to the DNS servers in the order their IPv4 addresses are specified.

The system allows a maximum of six DNS server IPv4 addresses for the public network or each VPN instance. You can specify DNS server IPv4 addresses for both public network and VPN instances.

If you do not specify an IPv4 address, the **undo dns server** command removes all DNS server IPv4 addresses for the public network or the specified VPN instance.

Examples

Specify DNS server IPv4 address 172.16.1.1.

```
<Switch> system-view
[Switch] dns server 172.16.1.1
```

Related commands

display dns server

7.1.8. ip host

Use **ip host** to create a host name-to-IPv4 address mapping.

Use **undo ip host** to remove a host name-to-IPv4 address mapping.

Syntax

ip host *host-name ip-address* [**vpn-instance** *vpn-instance-name*]

undo ip host *host-name ip-address* [**vpn-instance** *vpn-instance-name*]

Default

No host name-to-IPv4 address mappings exist.

Views

System view

Predefined user roles

network-admin

Parameters

host-name: Specifies a host name, a case-insensitive string of 1 to 253 characters. Valid characters are letters, digits, hyphens (-), underscores (_), and dots (.).

ip-address: Specifies the IPv4 address of the host.

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. To create a host name-to-IP address mapping for the public network, do not specify this option.

Usage guidelines

The system allows a maximum of 1024 host name-to-IPv4 address mappings for the public network or each VPN instance. You can configure host name-to-IPv4 address mappings for both public network and VPN instances.

For the public network or a VPN instance, each host name maps to only one IPv4 address. If you execute this command multiple times, the most recent configuration takes effect.

Do not use the **ping** command parameter **ip**, **-a**, **-c**, **-f**, **-h**, **-i**, **-m**, **-n**, **-p**, **-q**, **-r**, **-s**, **-t**, **-tos**, **-v**, or **-vpn-instance** as the host name. For more information about the **ping** command parameters, see *Network Management and Monitoring Command Reference*.

Examples

Map IPv4 address 10.110.0.1 to host name **aaa** for the public network.

```
<Switch> system-view
[Switch] ip host aaa 10.110.0.1
```

Related commands

display dns host

7.1.9. reset dns host

Use **reset dns host** to clear dynamic DNS entries.

Syntax

reset dns host [**ip**] [**vpn-instance** *vpn-instance-name*]

Views

User view

Predefined user roles

network-admin

Parameters

ip: Specifies type A queries. A type A query resolves a domain name to the mapped IPv4 address.

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command clears dynamic DNS entries for the public network.

Usage guidelines

If you do not specify the **ip** keyword, the **reset dns host** command clears dynamic DNS entries of all query types.

Examples

Clear dynamic DNS entries of all query types for the public network.

```
<Switch> reset dns host
```

Related commands

display dns host

Contents

A page of this section is **4-x-x**

8. Basic IP forwarding commands 8-1
8.1. Basic IP forwarding commands 8-1
8.1.1. display fib 8-1

8. Basic IP forwarding commands

8.1. Basic IP forwarding commands

8.1.1. display fib

Use **display fib** to display FIB entries.

Syntax

display fib [**vpn-instance** *vpn-instance-name*] [*ip-address* [*mask* | *mask-length*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. To display the FIB entries for the public network, do not specify any VPN.

ip-address: Displays the FIB entry that matches the specified destination IP address.

mask: Specifies the mask for the IP address.

mask-length: Specifies the mask length for the IP address. The value range is 0 to 32.

Usage guidelines

If you specify an IP address without a mask or mask length, this command displays the longest matching FIB entry.

If you specify an IP address and a mask or mask length, this command displays the exactly matching FIB entry.

Examples

Display all FIB entries of the public network.

```
<Switch> display fib

Destination count: 5 FIB entry count: 5

Flag:
  U:Usable   G:Gateway   H:Host   B:Blackhole   D:Dynamic   S:Static
  R:Relay     F:FRR

Destination/Mask   Nexthop         Flag     OutInterface/Token       Label
0.0.0.0/32         127.0.0.1       UH       InLoop0                  Null
1.1.1.0/24         192.168.126.1   USGR     M-GE0/0/0                Null
127.0.0.0/8        127.0.0.1       U        InLoop0                  Null
127.0.0.0/32       127.0.0.1       UH       InLoop0                  Null
```

```
127.0.0.1/32       127.0.0.1       UH       InLoop0                 Null
```

Display the FIB entries for VPN **vpn1**.

```
<Switch> display fib vpn-instance vpn1
Destination count: 6 FIB entry count: 6

Flag:
  U:Usable    G:Gateway    H:Host    B:Blackhole    D:Dynamic    S:Static
  R:Relay     F:FRR

Destination/Mask    Nexthop         Flag     OutInterface/Token      Label
0.0.0.0/32          127.0.0.1       UH       InLoop0                  Null
20.20.20.0/24       20.20.20.25     U        M-GE0/0/0                Null
20.20.20.0/32       20.20.20.25     UBH      M-GE0/0/0                Null
20.20.20.25/32      127.0.0.1       UH       InLoop0                  Null
20.20.20.25/32      20.20.20.25     H        M-GE0/0/0                Null
20.20.20.255/32     20.20.20.25     UBH      M-GE0/0/0                Null
```

Display the FIB entries matching the destination IP address 10.2.1.1.

```
<Switch> display fib 10.2.1.1

Destination count: 1 FIB entry count: 1

Flag:
  U:Usable    G:Gateway    H:Host    B:Blackhole    D:Dynamic    S:Static
  R:Relay     F:FRR

Destination/Mask    Nexthop         Flag     OutInterface/Token       Label
10.2.1.1/32         127.0.0.1       UH       InLoop0                  Null
```

Table 8-1 Command output

Field	Description
Destination count	Total number of destination addresses.
FIB entry count	Total number of FIB entries.
Destination/Mask	Destination address and the mask length.
Nexthop	Next hop address.
Flag	Flags of routes: • **U**—Usable route. • **G**—Gateway route. • **H**—Host route. • **B**—Blackhole route. • **D**—Dynamic route. • **S**—Static route. • **R**—Relay route. • **F**—Fast reroute.
OutInterface/Token	Output interface/LSP index number.
Label	Inner label.

Contents

A page of this section is **4-x-x**

9. IP performance optimization commands 9-1
9.1. IP performance optimization commands 9-1
9.1.1. display icmp statistics 9-1
9.1.2. display ip statistics 9-2
9.1.3. display rawip 9-3
9.1.4. display rawip verbose 9-4
9.1.5. display tcp 9-7
9.1.6. display tcp statistics 9-7
9.1.7. display tcp verbose 9-9
9.1.8. display udp 9-13
9.1.9. display udp statistics 9-14
9.1.10. display udp verbose 9-14
9.1.11. ip forward-broadcast 9-17
9.1.12. ip icmp error-interval 9-18
9.1.13. ip mtu 9-19
9.1.14. ip redirects enable 9-19
9.1.15. ip ttl-expires enable 9-20
9.1.16. ip unreachables enable 9-21
9.1.17. reset ip statistics 9-22
9.1.18. reset tcp statistics 9-22
9.1.19. reset udp statistics 9-23
9.1.20. tcp path-mtu-discovery 9-23
9.1.21. tcp timer fin-timeout 9-24
9.1.22. tcp timer syn-timeout 9-24
9.1.23. tcp window 9-25

9. IP performance optimization commands

9.1. IP performance optimization commands

9.1.1. display icmp statistics

Use **display icmp statistics** to display ICMP statistics.

Syntax

display icmp statistics [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays ICMP statistics for all member devices.

Usage guidelines

ICMP statistics include information about received and sent ICMP packets.

Examples

Display ICMP statistics.

```
<Switch> display icmp statistics
  Input: bad formats   0                  bad checksum            0
         echo          175                destination unreachable 0
         source quench 0                  redirects               0
         echo replies  201                parameter problem       0
         timestamp     0                  information requests    0
         mask requests 0                  mask replies            0
         time exceeded 0                  invalid type            0
         router advert 0                  router solicit          0
         broadcast/multicast echo requests ignored           0
         broadcast/multicast timestamp requests ignored      0
 Output: echo          0                  destination unreachable 0
         source quench 0                  redirects               0
         echo replies  175                parameter problem       0
         timestamp     0                  information replies     0
         mask requests 0                  mask replies            0
         time exceeded 0                  bad address             0
         packet error  1442               router advert           3
```

9.1.2. display ip statistics

Use **display ip statistics** to display IP packet statistics.

Syntax

display ip statistics [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays IP packet statistics for all member devices.

Usage guidelines

IP statistics include information about received and sent packets, fragments, and reassembly.

Examples

Display IP packet statistics.

```
<Switch> display ip statistics
  Input:    sum            7120            local             112
            bad protocol   0               bad format        0
            bad checksum   0               bad options       0
  Output:   forwarding     0               local             27
            dropped        0               no route          2
            compress fails 0
  Fragment:input           0               output            0
            dropped        0
            fragmented     0               couldn't fragment 0
  Reassembling:sum         0               timeouts          0
```

Table 9-1 Command output

Field	Description
Input	Statistics about received packets: • **sum**—Total number of packets received. • **local**—Total number of packets destined for the device. • **bad protocol**—Total number of unknown protocol packets. • **bad format**—Total number of packets with incorrect format. • **bad checksum**—Total number of packets with incorrect checksum. • **bad options**—Total number of packets with incorrect option.
Output	Statistics about sent packets: • **forwarding**—Total number of packets forwarded. • **local**—Total number of packets locally sent. • **dropped**—Total number of packets discarded. • **no route**—Total number of packets for which no route is

Field	Description
	available. • **compress fails**—Total number of packets failed to be compressed.
Fragment	Statistics about fragments: • **input**—Total number of fragments received. • **output**—Total number of fragments sent. • **dropped**—Total number of fragments dropped. • **fragmented**—Total number of packets successfully fragmented. • **couldn't fragment**—Total number of packets failed to be fragmented.
Reassembling	Statistics about reassembly: • **sum**—Total number of packets reassembled. • **timeouts**—Total number of reassembly timeouts.

Related commands

display ip interface

reset ip statistics

9.1.3. display rawip

Use **display rawip** to display brief information about RawIP connections.

Syntax

display rawip [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays brief information about RawIP connections for all member devices.

Usage guidelines

Brief RawIP connection information includes local and peer addresses, protocol, and PCB.

Examples

Display brief information about RawIP connections.

```
<Switch> display rawip
 Local Addr       Foreign Addr     Protocol  Slot  Cpu PCB
 0.0.0.0          0.0.0.0          1         1     0   0x0000000000000009
 0.0.0.0          0.0.0.0          1         1     0   0x0000000000000008
 0.0.0.0          0.0.0.0          1         5     0   0x0000000000000002
```

Table 9-2 Command output

Field	Description
Local Addr	Local IP address.
Foreign Addr	Peer IP address.
Protocol	Protocol number.
PCB	Protocol control block.

9.1.4. display rawip verbose

Use **display rawip verbose** to display detailed information about RawIP connections.

Syntax

display rawip verbose [**slot** *slot-number* [**pcb** *pcb-index*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

pcb *pcb-index*: Displays detailed RawIP connection information for the specified PCB. The *pcb-index* argument specifies the index of the PCB. The index is a hexadecimal value in the range of 1 to ffffffffffffffff.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays detailed information about RawIP connections for all member devices.

Usage guidelines

The detailed information includes socket creator, state, option, type, protocol number, and the source and destination IP addresses of RawIP connections.

Examples

Display detailed information about RawIP connections.

```
<Switch> display rawip verbose
Total RawIP socket number: 1

 Location: slot: 6 cpu: 0
 Creator: ping[320]
 State: N/A
 Options: N/A
 Error: 0
 Receiving buffer(cc/hiwat/lowat/drop/state): 0 / 9216 / 1 / 0 / N/A
 Sending buffer(cc/hiwat/lowat/state): 0 / 9216 / 512 / N/A
 Type: 3
 Protocol: 1
 Connection info: src = 0.0.0.0, dst = 0.0.0.0
```

```
Inpcb flags: N/A
Inpcb extflag: INP_EXTRCVICMPERR INP_EXTFILTER
Inpcb vflag: INP_IPV4
TTL: 255(minimum TTL: 0)
Send VRF: 0xffff
Receive VRF: 0xffff
```

Table 9-3 Command output

Field	Description
Total RawIP socket number	Total number of RawIP sockets.
Creator	Name of the operation that created the socket. The number in brackets is the process number of the creator.
State	State of the socket.
Options	Socket options.
Error	Error code.

Receiving buffer (cc/hiwat/lowat/drop/state)	Displays receive buffer information in the following order:
	• **cc**—Used space.
	• **hiwat**—Maximum space.
	• **lowat**—Minimum space.
	• **drop**—Number of dropped packets.
	• **state**—Buffer state:
	  ○ **CANTSENDMORE**—Unable to send data to the peer.
	  ○ **CANTRCVMORE**—Unable to receive data from the peer.
	  ○ **RCVATMARK**—Receiving tag.
	  ○ **N/A**—None of the above states.

Sending buffer (cc/hiwat/lowat/state)	Displays send buffer information in the following order:
	• **cc**—Used space.
	• **hiwat**—Maximum space.
	• **lowat**—Minimum space.
	• **state**—Buffer state:
	  ○ **CANTSENDMORE**—Unable to send data to the peer.
	  ○ **CANTRCVMORE**—Unable to receive data from the peer.
	  ○ **RCVATMARK**—Receiving tag.
	  ○ **N/A**—None of the above states.

Type	Socket type: • **1—SOCK_STREAM**. This socket uses TCP to provide reliable transmission of byte streams. • **2—SOCK_DGRAM**. This socket uses UDP to provide datagram transmission. • **3—SOCK_RAW**. This socket allows an application to change the next upper-layer protocol header. • **N/A**—None of the above types.
Protocol	Number of the protocol using the socket.
Connection info	Source IP address and destination IP address.

Field	Description
Inpcb flags	Flags in the Internet PCB: • **INP_RECVOPTS**—Receives IP options. • **INP_RECVRETOPTS**—Receives replied IP options. • **INP_RECVDSTADDR**—Receives destination IP address. • **INP_HDRINCL**—Provides the entire IP header. • **INP_REUSEADDR**—Reuses the IP address. • **INP_REUSEPORT**—Reuses the port number. • **INP_ANONPORT**—Port number not specified. • I**NP_RECVIF**—Records the input interface of the packet. • **INP_RECVTTL**—Receives TTL of the packet. Only UDP and RawIP support this flag. • **INP_DONTFRAG**—Sets the **Don't Fragment** flag. • **INP_ROUTER_ALERT**—Receives packets with the router alert option. Only RawIP supports this flag. • **INP_PROTOCOL_PACKET**—Identifies a protocol packet. • **INP_RCVVLANID**—Receives the VLAN ID of the packet. Only UDP and RawIP support this flag. • **INP_RCVMACADDR**—Receives the MAC address of the frame. • **INP_RECVTOS**—Receives TOS of the packet. Only UDP and RawIP support this flag. • **INP_USEICMPSRC**—Uses the specified IP address as the source IP address for outgoing ICMP packets. • **INP_SYNCPCB**—Waits until Internet PCB is synchronized. • **N/A**—None of the above flags.
Inpcb extflag	Extension flags in the Internet PCB: • **INP_EXTRCVPVCIDX**—Records the PVC index of the received packet. • **INP_RCVPWID**—Records the PW ID of the received packet. • **INP_EXTRCVICMPERR**—Receives an ICMP error packet. • **INP_EXTFILTER**—Filters the contents in the received packet. • **N/A**—None of the above flags.
Inpcb vflag	IP version flags in the Internet PCB: • **INP_IPV4**—IPv4 protocol. • **INP_TIMEWAIT**—In **TIMEWAIT** state. • **INP_ONESBCAST**—Sends broadcast packets. • **INP_DROPPED**—Protocol dropped flag. • **INP_SOCKREF**—Strong socket reference. • **INP_DONTBLOCK**—Do not block synchronization of the Internet PCB. • **N/A**—None of the above flags.
TTL	TTL value in the Internet PCB.
Send VRF	VRF from which packets are sent.

Field	Description
Receive VRF	VRF from which packets are received.

9.1.5. display tcp

Use **display tcp** to display brief information about TCP connections.

Syntax

display tcp [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays brief information about TCP connections for all member devices.

Usage guidelines

Brief TCP connection information includes local IP address, local port number, peer IP address, peer port number, and TCP connection state.

Examples

Display brief information about TCP connections.

```
<Switch> display tcp
 *: TCP connection with authentication
 Local Addr:port       Foreign Addr:port     State       Slot  Cpu PCB
*0.0.0.0:21            0.0.0.0:0             LISTEN      1     0   0x000000000000c387
 192.168.20.200:23     192.168.20.14:1284    ESTABLISHED 1     0   0x0000000000000009
 192.168.20.200:23     192.168.20.14:1283    ESTABLISHED 1     0   0x0000000000000002
```

Table 9-4 Command output

Field	Description
*	Indicates that the TCP connection uses authentication.
Local Addr:port	Local IP address and port number.
Foreign Addr:port	Peer IP address and port number.
State	TCP connection state.
PCB	PCB index.

9.1.6. display tcp statistics

Use **display tcp statistics** to display TCP traffic statistics.

Syntax

display tcp statistics [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays TCP traffic statistics for all member devices.

Usage guidelines

TCP traffic statistics include information about received and sent TCP packets and Syncache/syncookie.

Examples

Display TCP traffic statistics.

```
<Switch> display tcp statistics
Received packets:
    Total: 4150
    packets in sequence: 1366 (134675 bytes)
    window probe packets: 0, window update packets: 0
    checksum error: 0, offset error: 0, short error: 0
    packets dropped for lack of memory: 0
    packets dropped due to PAWS: 0
    duplicate packets: 12 (36 bytes), partially duplicate packets: 0 (0 bytes)
    out-of-order packets: 0 (0 bytes)
    packets with data after window: 0 (0 bytes)
    packets after close: 0
    ACK packets: 3531 (795048 bytes)
    duplicate ACK packets: 33, ACK packets for unsent data: 0

Sent packets:
    Total: 4058
    urgent packets: 0
    control packets: 50
    window probe packets: 3, window update packets: 11
    data packets: 3862 (795012 bytes), data packets retransmitted: 0 (0 bytes)
    ACK-only packets: 150 (52 delayed)
    unnecessary packet retransmissions: 0

Syncache/syncookie related statistics:
    entries added to syncache: 12
    syncache entries retransmitted: 0
    duplicate SYN packets: 0
    reply failures: 0
    successfully build new socket: 12
```

```
    bucket overflows: 0
    zone failures: 0
    syncache entries removed due to RST: 0
    syncache entries removed due to timed out: 0
    ACK checked by syncache or syncookie failures: 0
    syncache entries aborted: 0
    syncache entries removed due to bad ACK: 0
    syncache entries removed due to ICMP unreachable: 0
    SYN cookies sent: 0
    SYN cookies received: 0

SACK related statistics:
    SACK recoveries: 1
    SACK retransmitted segments: 0 (0 bytes)
    SACK blocks (options) received: 0
    SACK blocks (options) sent: 0
    SACK scoreboard overflows: 0

Other statistics:
    retransmitted timeout: 0, connections dropped in retransmitted timeout: 0
    persist timeout: 0
    keepalive timeout: 21, keepalive probe: 0
    keepalive timeout, so connections disconnected: 0
    fin_wait_2 timeout, so connections disconnected: 0
    initiated connections: 29, accepted connections: 12, established connections:
23
    closed connections: 50051 (dropped: 0, initiated dropped: 0)
    bad connection attempt: 0
    ignored RSTs in the window: 0
    listen queue overflows: 0
    RTT updates: 3518(attempt segment: 3537)
    correct ACK header predictions: 0
    correct data packet header predictions: 568
    resends due to MTU discovery: 0
    packets dropped due to MD5 authentication failure: 0
    packets that passed MD5 authentication: 0
    sent Keychain-encrypted packets: 0
    packets that passed Keychain authentication: 0
    packets dropped due to Keychain authentication failure: 0
```

Related commands

reset tcp statistics

9.1.7. display tcp verbose

Use **display tcp verbose** to display detailed information about TCP connections.

Syntax

display tcp verbose [**slot** *slot-number* [**pcb** *pcb-index*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

pcb *pcb-index*: Displays detailed TCP connection information for the specified PCB. The index is a hexadecimal value in the range of 1 to ffffffffffffffff.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays detailed information about TCP connections for all member devices.

Usage guidelines

The detailed TCP connection information includes socket creator, state, option, type, protocol number, source IP address and port number, destination IP address and port number, and connection state.

Examples

Display detailed information about TCP connections.

```
<Switch> display tcp verbose
TCP inpcb number: 1(tcpcb number: 1)

 Location: slot: 6 cpu: 0
 NSR standby: N/A
 Creator: bgpd[199]
 State: ISCONNECTED
 Options: N/A
 Error: 0
 Receiving buffer(cc/hiwat/lowat/state): 0 / 65700 / 1 / N/A
 Sending buffer(cc/hiwat/lowat/state): 0 / 65700 / 512 / N/A
 Type: 1
 Protocol: 6
 Connection info: src = 192.168.20.200:179 ,  dst = 192.168.20.14:4181
 Inpcb flags: N/A
 Inpcb extflag: N/A
 Inpcb vflag: INP_IPV4
 TTL: 255(minimum TTL: 0)
 Connection state: ESTABLISHED
 TCP options: TF_REQ_SCALE TF_REQ_TSTMP TF_SACK_PERMIT TF_NSR
 NSR state: READY(M)
 Send VRF: 0x0
 Receive VRF: 0x0
```

Table 9-5 Command output

Field	Description
TCP inpcb number	Number of TCP IP PCBs.
tcpcb number	Number of TCP PCBs. This field is not displayed if the state of the TCP connection is **TIME_WAIT**.
Creator	Name of the operation that created the socket. The number in brackets is the process number of the creator.
State	State of the socket.
Options	Socket options.
Error	Error code.

Receiving buffer (cc/hiwat/lowat/state)	Displays receive buffer information in the following order:
	• **cc**—Used space.
	• **hiwat**—Maximum space.
	• **lowat**—Minimum space.
	• **state**—Buffer state:
	  ○ **CANTSENDMORE**—Unable to send data to the peer.
	  ○ **CANTRCVMORE**—Unable to receive data from the peer.
	  ○ **RCVATMARK**—Receiving tag.
	  ○ **N/A**—None of the above states.

Sending buffer (cc/hiwat/lowat/state)	Displays send buffer information in the following order:
	• **cc**—Used space.
	• **hiwat**—Maximum space.
	• **lowat**—Minimum space.
	• **state**—Buffer state:
	  ○ **CANTSENDMORE**—Unable to send data to the peer.
	  ○ **CANTRCVMORE**—Unable to receive data from the peer.
	  ○ **RCVATMARK**—Receiving tag.
	  ○ **N/A**—None of the above states.

Type	Socket type: • **1**—**SOCK_STREAM**. This socket uses TCP to provide reliable transmission of byte streams. • **2**—**SOCK_DGRAM**. This socket uses UDP to provide datagram transmission. • **3**—**SOCK_RAW**. This socket allows an application to change the next upper-layer protocol header. • **N/A**—None of the above types.
Protocol	Number of the protocol using the socket.
Connection info	Source IP address and port number, and destination IP address and port number.
Inpcb flags	Flags in the Internet PCB: • **INP_RECVOPTS**—Receives IP options. • **INP_RECVRETOPTS**—Receives replied IP options. • **INP_RECVDSTADDR**—Receives destination IP address.

Field	Description
	• **INP_HDRINCL**—Provides the entire IP header. • **INP_REUSEADDR**—Reuses the IP address. • **INP_REUSEPORT**—Reuses the port number. • **INP_ANONPORT**—Port number not specified. • I**NP_RECVIF**—Records the input interface of the packet. • **INP_RECVTTL**—Receives TTL of the packet. Only UDP and RawIP support this flag. • **INP_DONTFRAG**—Sets the **Don't Fragment** flag. • **INP_ROUTER_ALERT**—Receives packets with the router alert option. Only RawIP supports this flag. • **INP_PROTOCOL_PACKET**—Identifies a protocol packet. • **INP_RCVVLANID**—Receives the VLAN ID of the packet. Only UDP and RawIP support this flag. • **INP_RCVMACADDR**—Receives the MAC address of the frame. • **INP_RECVTOS**—Receives TOS of the packet. Only UDP and RawIP support this flag. • **INP_SYNCPCB**—Waits until Internet PCB is synchronized. • **N/A**—None of the above flags.
Inpcb extflag	Extension flags in the Internet PCB: • **INP_EXTRCVPVCIDX**—Records the PVC index of the received packet. • **INP_RCVPWID**—Records the PW ID of the received packet. • **INP_EXTDONTDROP**—Does not drop the received packet. • **N/A**—None of the above flags.
Inpcb vflag	IP version flags in the Internet PCB: • **INP_IPV4**—IPv4 protocol. • **INP_TIMEWAIT**—In **TIMEWAIT** state. • **INP_ONESBCAST**—Sends broadcast packets. • **INP_DROPPED**—Protocol dropped flag. • **INP_SOCKREF**—Strong socket reference. • **INP_DONTBLOCK**—Do not block synchronization of the Internet PCB. • **N/A**—None of the above flags.
TTL	TTL value in the Internet PCB.
TCP options	TCP options: • **TF_MD5SIG**—Enables MD5 signature. • **TF_NODELAY**—Disables the Nagle algorithm that buffers the sent data inside the TCP. • **TF_NOOPT**—No TCP options. • **TF_NOPUSH**—Forces TCP to delay sending any TCP data until a full sized segment is buffered in the TCP buffers. • **TF_BINDFOREIGNADDR**—Binds the peer IP address. • **TF_NSR**—Enables TCP NSR.

Field	Description
	• **TF_REQ_SCALE**—Enables the TCP window scale option. • **TF_REQ_TSTMP**—Enables the time stamp option. • **TF_SACK_PERMIT**—Enables the TCP selective acknowledgement option. • **TF_ENHANCED_AUTH**—Enables the enhanced authentication option.
NSR state	State of the TCP connections. Between the parentheses is the role of the connection: • **M**—Main connection. • **S**—Standby connection.
Send VRF	VRF from which packets are sent.
Receive VRF	VRF from which packets are received.

9.1.8. display udp

Use **display udp** to display brief information about UDP connections.

Syntax

display udp [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays brief information about UDP connections for all member devices.

Usage guidelines

Brief UDP connection information includes local IP address and port number, and peer IP address and port number.

Examples

Display brief information about UDP connections.

```
<Switch> display udp
 Local Addr:port        Foreign Addr:port     Slot  Cpu PCB
 0.0.0.0:69             0.0.0.0:0             1     0   0x0000000000000003
 192.168.20.200:1024    192.168.20.14:69      5     0   0x0000000000000002
```

Table 9-6 Command output

Field	Description
Local Addr:port	Local IP address and port number.
Foreign Addr:port	Peer IP address and port number.

Field	Description
PCB	PCB index.

9.1.9. display udp statistics

Use **display udp statistics** to display UDP traffic statistics.

Syntax

display udp statistics [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays UDP traffic statistics for all member devices.

Usage guidelines

UDP traffic statistics include information about received and sent UDP packets.

Examples

Display UDP traffic statistics.

```
<Switch> display udp statistics
Received packets:
     Total: 240
     checksum error: 0, no checksum: 0
     shorter than header: 0, data length larger than packet: 0
     no socket on port(unicast): 0
     no socket on port(broadcast/multicast): 240
     not delivered, input socket full: 0
Sent packets:
     Total: 0
```

Related commands

reset udp statistics

9.1.10. display udp verbose

Use **display udp verbose** to display detailed information about UDP connections.

Syntax

display udp verbose [**slot** *slot-number* [**pcb** *pcb-index*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

pcb *pcb-index*: Displays detailed UDP connection information for the specified PCB. The index is a hexadecimal value in the range of 1 to ffffffffffffffff.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays detailed information about UDP connections for all member devices.

Usage guidelines

The detailed information includes socket creator, status, option, type, protocol number, source IP address and port number, and destination IP address and port number for UDP connections.

Examples

Display detailed UDP connection information.

```
<Switch> display udp verbose
Total UDP socket number: 1


 Location: slot: 6 cpu: 0
 Creator: sock_test_mips[250]
 State: N/A
 Options: N/A
 Error: 0
 Receiving buffer(cc/hiwat/lowat/drop/state): 0 / 41600 / 1 / 0 / N/A
 Sending buffer(cc/hiwat/lowat/state): 0 / 9216 / 512 / N/A
 Type: 2
 Protocol: 17
 Connection info: src = 0.0.0.0:69, dst = 0.0.0.0:0
 Inpcb flags: N/A
 Inpcb extflag: N/A
 Inpcb vflag: INP_IPV4
 TTL: 255(minimum TTL: 0)
 Send VRF: 0xffff
 Receive VRF: 0xffff
```

Table 9-7 Command output

Field	Description
Total UDP socket number	Total number of UDP sockets.
Creator	Name of the operation that created the socket. The number in brackets is the process number of the creator.
State	Socket state.
Options	Socket option.
Error	Error code.
Receiving buffer(cc/hiwat/lowat/drop/state)	Displays receive buffer information in the following order: • **cc**—Used space.

Field	Description

	• **hiwat**—Maximum space.
	• **lowat**—Minimum space.
	• **drop**—Number of dropped packets.
	• **state**—Buffer state:
	  ○ **CANTSENDMORE**—Unable to send data to the peer.
	  ○ **CANTRCVMORE**—Unable to receive data from the peer.
	  ○ **RCVATMARK**—Receiving tag.
	  ○ **N/A**—None of the above states.

Sending buffer(cc/hiwat/lowat/state)	Displays send buffer information in the following order:
	• **cc**—Used space.
	• **hiwat**—Maximum space.
	• **lowat**—Minimum space.
	• **state**—Buffer state:
	  ○ **CANTSENDMORE**—Unable to send data to the peer.
	  ○ **CANTRCVMORE**—Unable to receive data from the peer.
	  ○ **RCVATMARK**—Receiving tag.
	  ○ **N/A**—None of the above states.

Type	Socket type: • **1**—**SOCK_STREAM**. This socket uses TCP to provide reliable transmission of byte streams. • **2**—**SOCK_DGRAM**. This socket uses UDP to provide datagram transmission. • **3**—**SOCK_RAW**. This socket allows an application to change the next upper-layer protocol header. • **N/A**—None of the above types.
Protocol	Number of the protocol using the socket.
Inpcb flags	Flags in the Internet PCB: • **INP_RECVOPTS**—Receives IP options. • **INP_RECVRETOPTS**—Receives replied IP options. • **INP_RECVDSTADDR**—Receives destination IP address. • **INP_HDRINCL**—Provides the entire IP header. • **INP_REUSEADDR**—Reuses the IP address. • **INP_REUSEPORT**—Reuses the port number. • **INP_ANONPORT**—Port number not specified. • I**NP_RECVIF**—Records the input interface of the packet. • **INP_RECVTTL**—Receives TTL of the packet. Only UDP and RawIP support this flag. • **INP_DONTFRAG**—Sets the **Don't Fragment** flag. • **INP_ROUTER_ALERT**—Receives packets with the router alert option. Only RawIP supports this flag. • **INP_PROTOCOL_PACKET**—Identifies a protocol packet. • **INP_RCVVLANID**—Receives the VLAN ID of the packet. Only UDP and RawIP support this flag. • **INP_RCVMACADDR**—Receives the MAC address

Field	Description
	of the frame. • **INP_RECVTOS**—Receives TOS of the packet. Only UDP and RawIP support this flag. • **INP_SYNCPCB**—Waits until Internet PCB is synchronized. • **N/A**—None of the above flags.
Inpcb extflag	Extension flags in the Internet PCB: • **INP_EXTRCVPVCIDX**—Records the PVC index of the received packet. • **INP_RCVPWID**—Records the PW ID of the received packet. • **N/A**—None of the above flags.
Inpcb vflag	IP version flags in the Internet PCB: • **INP_IPV4**—IPv4 protocol. • **INP_TIMEWAIT**—In **TIMEWAIT** state. • **INP_ONESBCAST**—Sends broadcast packets. • **INP_DROPPED**—Protocol dropped flag. • **INP_SOCKREF**—Strong socket reference. • **INP_DONTBLOCK**—Do not block synchronization of the Internet PCB. • **N/A**—None of the above flags.
TTL	TTL value in the Internet PCB.
Send VRF	VRF from which packets are sent.
Receive VRF	VRF from which packets are received.

9.1.11. ip forward-broadcast

Use **ip forward-broadcast** to enable an interface to forward directed broadcast packets destined for the directly connected network.

Use **undo ip forward-broadcast** to disable an interface from forwarding directed broadcast packets destined for the directly connected network.

Syntax

ip forward-broadcast

undo ip forward-broadcast

Default

An interface cannot forward directed broadcasts destined for the directly connected network.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

A directed broadcast packet is destined for all hosts on a specific network. In the destination IP address of the directed broadcast, the network ID identifies the target network, and the host ID is made up of all ones.

If an interface is allowed to forward directed broadcasts destined for the directly connected network, hackers can exploit this vulnerability to attack the target network. In some scenarios, however, an interface must send such directed broadcast packets to support UDP helper and Wake on LAN.

The command enables the interface to forward directed broadcast packets that are destined for the directly connected network and are received from another subnet to support Wake on LAN. Wake on LAN sends the directed broadcasts to wake up the hosts on the target network.

Examples

Enable VLAN-interface 2 to forward directed broadcast packets destined for the directly connected network.

```
<Switch> system-view
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip forward-broadcast
```

9.1.12. ip icmp error-interval

Use **ip icmp error-interval** to set the bucket size and the interval for tokens to arrive in the bucket for ICMP error messages.

Use **undo ip icmp error-interval** to restore the default.

Syntax

ip icmp error-interval *interval* [*bucketsize*]

undo ip icmp error-interval

Default

The bucket allows a maximum of 10 tokens, and a token is placed in the bucket every 100 milliseconds.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the interval for tokens to arrive in the bucket. The value range is 0 to 2147483647 milliseconds. To disable the ICMP rate limit, set the value to 0.

bucketsize: Specifies the maximum number of tokens allowed in the bucket. The value range is 1 to 200.

Usage guidelines

This command limits the rate at which ICMP error messages are sent. Use this command to avoid sending excessive ICMP error messages within a short period that might cause network congestion. A token bucket algorithm is used with one token representing one ICMP error message.

A token is placed in the bucket at intervals until the maximum number of tokens that the bucket can hold is reached.

A token is removed from the bucket when an ICMP error message is sent. When the bucket is empty, ICMP error messages are not sent until a new token is placed in the bucket.

Examples

Set the bucket size to 40 tokens and the interval for tokens to arrive in the bucket to 200 milliseconds for ICMP error messages.

```
<Switch> system-view
[Switch] ip icmp error-interval 200 40
```

9.1.13. ip mtu

Use **ip mtu** to set the MTU of IPv4 packets sent over an interface.

Use **undo ip mtu** to restore the default.

Syntax

ip mtu *mtu-size*

undo ip mtu

Default

The MTU of IPv4 packets sent over an interface is not set.

Views

Interface view

Predefined user roles

network-admin

Parameters

mtu-size: Specifies the MTU in bytes. The value range for the *mtu-size* argument is 128 to 9216.

Usage guidelines

When a packet exceeds the MTU of the sending interface, the device processes the packet in one of the following ways:

- If the packet disallows fragmentation, the device discards it.
- If the packet allows fragmentation, the device fragments it and forwards the fragments.

Fragmentation and reassembling consume system resources, so set an appropriate MTU to avoid fragmentation.

If an interface supports both the **mtu** and **ip mtu** commands, the device fragments a packet based on the MTU set by the **ip mtu** command.

Examples

Set the MTU of VLAN-interface 100 to 1280 bytes.

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ip mtu 1280
```

9.1.14. ip redirects enable

Use **ip redirects enable** to enable sending ICMP redirect messages.

Use **undo ip redirects enable** to disable sending ICMP redirect messages.

Syntax

ip redirects enable

undo ip redirects enable

Default

Sending ICMP redirect messages is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

ICMP redirect messages simplify host management and enable hosts to gradually optimize their routing tables.

A host that has only one route destined for the default gateway sends all packets to the default gateway. The default gateway sends an ICMP redirect message to inform the host of a correct next hop by following these rules:

- The receiving and sending interfaces are the same.
- The selected route is not created or modified by any ICMP redirect messages.
- The selected route is not destined for 0.0.0.0.
- There is no source route option in the received packet.

Examples

Enable sending ICMP redirect messages.

```
<Switch> system-view
[Switch] ip redirects enable
```

9.1.15. ip ttl-expires enable

Use **ip ttl-expires enable** to enable sending ICMP time exceeded messages.

Use **undo ip ttl-expires enable** to disable sending ICMP time exceeded messages.

Syntax

ip ttl-expires enable

undo ip ttl-expires enable

Default

Sending ICMP time exceeded messages is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

A device sends ICMP time exceeded messages by following these rules:

- The device sends an ICMP TTL exceeded in transit message to the source when the following conditions are met:
  - The received packet is not destined for the device.
  - The TTL field of the packet is 1.

- When the device receives the first fragment of an IP datagram destined for the device itself, it starts a timer. If the timer expires before all the fragments of the datagram are received, the device sends an ICMP fragment reassembly time exceeded message to the source.

A device disabled from sending ICMP time exceeded messages does not send ICMP TTL exceeded in transit messages but can still send ICMP fragment reassembly time exceeded messages.

Examples

Enable sending ICMP time exceeded messages.

```
<Switch> system-view
[Switch] ip ttl-expires enable
```

9.1.16. ip unreachables enable

Use **ip unreachables enable** to enable sending ICMP destination unreachable messages.

Use **undo ip unreachables enable** to disable sending ICMP destination unreachable messages.

Syntax

ip unreachables enable

undo ip unreachables enable

Default

Sending ICMP destination unreachable messages is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

A device sends ICMP destination unreachable messages by following these rules:

- The device sends the source an ICMP network unreachable message when the following conditions are met:
  - The received packet does not match any route.
  - No default route exists in the routing table.
- The device sends the source an ICMP protocol unreachable message when the following conditions are met:
  - The received packet is destined for the device.
  - The transport layer protocol of the packet is not supported by the device.
- The device sends the source an ICMP port unreachable message when the following conditions are met:
  - The received UDP packet is destined for the device.
  - The packet's port number does not match the running process.
- The device sends the source an ICMP source route failed message when the following conditions are met:
  - The source uses Strict Source Routing to send packets.
  - The intermediate device finds that the next hop specified by the source is not directly connected.

- The device sends the source an ICMP fragmentation needed and DF set message when the following conditions are met:
  - The MTU of the sending interface is smaller than the packet.
  - The packet has Don't Fragment set.

Examples

Enable sending ICMP destination unreachable messages.

```
<Switch> system-view
[Switch] ip unreachables enable
```

9.1.17. reset ip statistics

Use **reset ip statistics** to clear IP traffic statistics.

Syntax

reset ip statistics [**slot** *slot-number*]

Views

User view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears IP traffic statistics for all member devices.

Usage guidelines

Use this command to clear history IP traffic statistics before you collect IP traffic statistics for a time period.

Examples

Clear IP traffic statistics.

```
<Switch> reset ip statistics
```

Related commands

display ip interface

display ip statistics

9.1.18. reset tcp statistics

Use **reset tcp statistics** to clear TCP traffic statistics.

Syntax

reset tcp statistics

Views

User view

Predefined user roles

network-admin

Examples

Clear TCP traffic statistics.

```
<Switch> reset tcp statistics
```

Related commands

display tcp statistics

9.1.19. reset udp statistics

Use **reset udp statistics** to clear UDP traffic statistics.

Syntax

reset udp statistics

Views

User view

Predefined user roles

network-admin

Examples

Clear UDP traffic statistics.

```
<Switch> reset udp statistics
```

Related commands

display udp statistics

9.1.20. tcp path-mtu-discovery

Use **tcp path-mtu-discovery** to enable TCP path MTU discovery.

Use **undo tcp path-mtu-discovery** to disable TCP path MTU discovery.

Syntax

tcp path-mtu-discovery [**aging** *age-time* | **no-aging**]

undo tcp path-mtu-discovery

Default

TCP path MTU discovery is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

aging *age-time*: Specifies the aging time for the path MTU, in the range of 10 to 30 minutes. The default aging time is 10 minutes.

no-aging: Does not age out the path MTU.

Usage guidelines

After you enable TCP path MTU discovery, all new TCP connections detect the path MTU. The device uses the path MTU to calculate the MSS to avoid IP fragmentation.

After you disable TCP path MTU discovery, the system stops all path MTU timers. The TCP connections established later do not detect the path MTU, but the TCP connections previously established still can detect the path MTU.

Examples

Enable TCP path MTU discovery and set the path MTU aging time to 20 minutes.

```
<Switch> system-view
[Switch] tcp path-mtu-discovery aging 20
```

9.1.21. tcp timer fin-timeout

Use **tcp timer fin-timeout** to set the TCP FIN wait timer.

Use **undo tcp timer fin-timeout** to restore the default.

Syntax

tcp timer fin-timeout *time-value*

undo tcp timer fin-timeout

Default

The TCP FIN wait timer is 675 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

time-value: Specifies the TCP FIN wait timer in the range of 76 to 3600 seconds.

Usage guidelines

TCP starts the FIN wait timer when the state of a TCP connection changes to FIN_WAIT_2. If no FIN packet is received within the timer interval, the TCP connection is terminated.

If a FIN packet is received, TCP changes the connection state to TIME_WAIT. If a non-FIN packet is received, TCP restarts the timer and tears down the connection when the timer expires.

Examples

Set the TCP FIN wait timer to 800 seconds.

```
<Switch> system-view
[Switch] tcp timer fin-timeout 800
```

9.1.22. tcp timer syn-timeout

Use **tcp timer syn-timeout** to set the TCP SYN wait timer.

Use **undo tcp timer syn-timeout** to restore the default.

Syntax

tcp timer syn-timeout *time-value*

undo tcp timer syn-timeout

Default

The TCP SYN wait timer is 75 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

time-value: Specifies the TCP SYN wait timer in the range of 2 to 600 seconds.

Usage guidelines

TCP starts the SYN wait timer after sending a SYN packet. Within the SYN wait timer if no response is received or the upper limit on TCP connection tries is reached, TCP fails to establish the connection.

Examples

Set the TCP SYN wait timer to 80 seconds.

```
<Switch> system-view
[Switch] tcp timer syn-timeout 80
```

9.1.23. tcp window

Use **tcp window** to set the size of the TCP receive/send buffer.

Use **undo tcp window** to restore the default.

Syntax

tcp window *window-size*

undo tcp window

Default

The size of the TCP receive/send buffer is 63 KB.

Views

System view

Predefined user roles

network-admin

Parameters

window-size: Specifies the size of the TCP receive/send buffer, in the range of 1 to 64 KB.

Examples

Set the size of the TCP receive/send buffer to 3 KB.

```
<Switch> system-view
[Switch] tcp window 3
```

Contents

A page of this section is **4-x-x**

10. UDP helper commands 10-1
10.1. UDP helper commands 10-1
10.1.1. display udp-helper interface 10-1
10.1.2. reset udp-helper statistics 10-2
10.1.3. udp-helper enable 10-2
10.1.4. udp-helper port 10-3
10.1.5. udp-helper server 10-3

10. UDP helper commands

10.1. UDP helper commands

10.1.1. display udp-helper interface

Use **display udp-helper interface** to display information about broadcast to unicast conversion by UDP helper on an interface.

Syntax

display udp-helper interface *interface-type interface-number*

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number: Specifies an interface by its type and number.

Usage guidelines

This command displays information about destination servers and total number of unicast packets converted from UDP broadcast packets by UDP helper.

Examples

Display information about broadcast to unicast conversion by UDP helper on VLAN-interface 100.

```
<Switch> display udp-helper interface vlan-interface 100
Interface                Server VPN instance          Server address Packets sent
Vlan-interface100        N/A                          192.1.1.2      0
Vlan-interface100        N/A                          192.1.1.2      0
```

Table 10-1 Command output

Field	Description
Interface	Interface name.
Server VPN instance	VPN instance to which the destination server belongs.
Server address	Destination server to which UDP packets are forwarded.
Packets sent	Number of unicast packets that are converted from broadcast packets by UDP helper.

Related commands

reset udp-helper statistics

udp-helper server

10.1.2. reset udp-helper statistics

Use **reset udp-helper statistics** to clear statistics about broadcast to unicast conversion by UDP helper.

Syntax

reset udp-helper statistics

Views

User view

Predefined user roles

network-admin

Examples

Clear the statistics about broadcast to unicast conversion by UDP helper.

```
<Switch> reset udp-helper statistics
```

Related commands

display udp-helper interface

10.1.3. udp-helper enable

Use **udp-helper enable** to enable UDP helper.

Use **undo udp-helper enable** to disable UDP helper.

Syntax

udp-helper enable

undo udp-helper enable

Default

UDP helper is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

For UDP helper to take effect on an interface, make sure the following conditions are met:

- UDP helper is enabled.
- A UDP port number is specified by using the **udp-helper port** command.
- Packet conversion for UDP helper is configured on the interface.

Examples

Enable UDP helper.

```
<Switch> system-view
[Switch] udp-helper enable
```

Related commands

udp-helper port

udp-helper server

10.1.4. udp-helper port

Use **udp-helper port** to specify a UDP port number for UDP helper.

Use **undo udp-helper port** to remove UDP port numbers.

Syntax

udp-helper port { *port-number* | **dns** | **netbios-ds** | **netbios-ns** | **tacacs** | **tftp** | **time** }

undo udp-helper port { *port-number* | **dns** | **netbios-ds** | **netbios-ns** | **tacacs** | **tftp** | **time** }

Default

No UDP port numbers are specified for UDP helper.

Views

System view

Predefined user roles

network-admin

Parameters

port-number: Specifies a UDP port number in the range of 1 to 65535 (except 67 and 68).

dns: Specifies the UDP port 53 used by DNS packets.

netbios-ds: Specifies the UDP port 138 used by NetBIOS distribution service packets.

netbios-ns: Specifies the UDP port 137 used by NetBIOS name service packets.

tacacs: Specifies the UDP port 49 used by TACACS packets.

tftp: Specifies the UDP port 69 used by TFTP packets.

time: Specifies the UDP port 37 used by time protocol packets.

Usage guidelines

Upon receiving a UDP broadcast or multicast packet, UDP helper uses the specified UDP ports to match the UDP destination port number of the packet.

To specify a UDP port, you can specify the port number or the protocol keyword. For example, **udp-helper port** 53 and **udp-helper port dns** specify the same UDP port.

You can specify a maximum of 256 UDP ports on a device.

Examples

Specify the UDP port 100 for UDP helper.

```
<Switch> system-view
[Switch] udp-helper port 100
```

10.1.5. udp-helper server

Use **udp-helper server** to specify a destination server for UDP helper to convert broadcast to unicast.

Use **undo udp-helper server** to remove a destination server.

Syntax

udp-helper server *ip-address* [**global** | **vpn-instance** *vpn-instance-name*]

undo udp-helper server [*ip-address* [**global** | **vpn-instance** *vpn-instance-name*]]

Default

No destination server is specified for UDP helper to convert broadcast to unicast.

Views

Interface view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the IP address of a destination server, in dotted decimal notation.

global: Forwards converted unicast packets to the server on the public network.

vpn-instance *vpn-instance-name*: Specifies a VPN instance to which the server belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

Specify destination servers on an interface that receives UDP broadcast packets. If the packets' destination UDP port numbers match the UDP helper ports, UDP helper forwards the broadcasts to the specified servers.

You can specify a maximum of 20 unicast and multicast addresses for UDP helper to convert broadcast packets on an interface.

If you do not specify the *ip-address* argument, the **undo udp-helper server** command removes all destination servers on the interface.

A destination server with the **global** keyword and the same destination server with the **vpn-instance** *vpn-instance-name* option do not overwrite each other. If you specify only the IP address, UDP helper forwards converted unicast packets in the VPN to which the receiving interface belongs. If the interface is not bound to any VPN instance, UDP helper forwards the unicast packets on the public network.

Examples

Specify the destination server 192.1.1.2 for UDP helper to convert broadcast to unicast on VLAN-interface 100.

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] udp-helper server 192.1.1.2
```

Specify the destination server 192.1.1.2 on the public network for UDP helper to convert broadcast to unicast on VLAN-interface 100.

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] udp-helper server 192.1.1.2 global
```

Related commands

display udp-helper interface

Contents

A page of this section is **4-x-x**

11. IPv6 basics commands ····· 11-1
11.1. IPv6 basics commands ····· 11-1
11.1.1. display ipv6 fib ····· 11-1
11.1.2. display ipv6 interface ····· 11-2
11.1.3. display ipv6 neighbors ····· 11-7
11.1.4. display ipv6 neighbors count ····· 11-9
11.1.5. display ipv6 neighbors vpn-instance ····· 11-9
11.1.6. display ipv6 pathmtu ····· 11-10
11.1.7. display ipv6 rawip ····· 11-11
11.1.8. display ipv6 rawip verbose ····· 11-12
11.1.9. display ipv6 statistics ····· 11-15
11.1.10. display ipv6 tcp ····· 11-17
11.1.11. display ipv6 tcp verbose ····· 11-18
11.1.12. display ipv6 udp ····· 11-22
11.1.13. display ipv6 udp verbose ····· 11-22
11.1.14. ipv6 address ····· 11-25
11.1.15. ipv6 address anycast ····· 11-26
11.1.16. ipv6 address auto ····· 11-27
11.1.17. ipv6 address auto link-local ····· 11-27
11.1.18. ipv6 address eui-64 ····· 11-28
11.1.19. ipv6 address link-local ····· 11-29
11.1.20. ipv6 hop-limit ····· 11-30
11.1.21. ipv6 hoplimit-expires enable ····· 11-31
11.1.22. ipv6 icmpv6 error-interval ····· 11-31
11.1.23. ipv6 icmpv6 multicast-echo-reply enable ····· 11-32
11.1.24. ipv6 mtu ····· 11-33
11.1.25. ipv6 nd autoconfig managed-address-flag ····· 11-34
11.1.26. ipv6 nd autoconfig other-flag ····· 11-34
11.1.27. ipv6 nd dad attempts ····· 11-35
11.1.28. ipv6 nd ns retrans-timer ····· 11-36
11.1.29. ipv6 nd nud reachable-time ····· 11-36
11.1.30. ipv6 nd ra halt ····· 11-37
11.1.31. ipv6 nd ra interval ····· 11-38
11.1.32. ipv6 nd ra prefix ····· 11-38
11.1.33. ipv6 nd ra router-lifetime ····· 11-40
11.1.34. ipv6 neighbor ····· 11-40
11.1.35. ipv6 neighbor stale-aging ····· 11-42
11.1.36. ipv6 neighbors max-learning-num ····· 11-42
11.1.37. ipv6 pathmtu ····· 11-43
11.1.38. ipv6 pathmtu age ····· 11-44
11.1.39. ipv6 unreachables enable ····· 11-44
11.1.40. local-proxy-nd enable ····· 11-45
11.1.41. reset ipv6 neighbors ····· 11-46
11.1.42. reset ipv6 pathmtu ····· 11-46
11.1.43. reset ipv6 statistics ····· 11-47

11. IPv6 basics commands

11.1. IPv6 basics commands

11.1.1. display ipv6 fib

Use **display ipv6 fib** to display IPv6 FIB entries.

Syntax

display ipv6 fib [**vpn-instance** *vpn-instance-name*] [*ipv6-address* [*prefix-length*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays IPv6 FIB entries for the public network.

ipv6-address: Displays IPv6 FIB entries for a destination IPv6 address. If you do not specify an IPv6 address, this command displays all IPv6 FIB entries.

prefix-length: Specifies a prefix length for the IPv6 address, in the range of 0 to 128. If you do not specify the prefix length, this command displays the IPv6 FIB entry longest matching the IPv6 address.

Examples

Display all IPv6 FIB entries for the public network.

```
<Switch> display ipv6 fib

Destination count: 1 FIB entry count: 1

Flag:
  U:Usable   G:Gateway   H:Host   B:Blackhole   D:Dynamic   S:Static
  R:Relay     F:FRR

Destination: ::1                                        Prefix length: 128
Nexthop      : ::1                                       Flags: UH
Time stamp : 0x1                                        Label: Null
Interface  : InLoop0                                    Token: Invalid
```

Table 11-1 Command output

Field	Description
Destination count	Total number of destination addresses.

Field	Description
FIB entry count	Total number of IPv6 FIB entries.
Destination	Destination address.
Prefix length	Prefix length of the destination address.
Nexthop	Next hop address.
Flags	Route flag: • **U**—Usable route. • **G**—Gateway route. • **H**—Host route. • **B**—Black hole route. • **D**—Dynamic route. • **S**—Static route. • **R**—Recursive route. • **F**—Fast re-route.
Time stamp	Time when the IPv6 FIB entry was generated.
Label	Inner MPLS label. For IPv6 FIB entries for the public network, this field displays **Null**.
Interface	Outgoing interface.
Token	Label switched path index number.

11.1.2. display ipv6 interface

Use **display ipv6 interface** to display IPv6 interface information.

Syntax

display ipv6 interface [*interface-type* [*interface-number*]] [**brief**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type: Specifies an interface by its type.

interface-number: Specifies an interface by its number.

brief: Displays brief IPv6 interface information, including physical status, link-layer protocols, and IPv6 address. If you do not specify the keyword, this command displays detailed IPv6 interface information, including IPv6 configuration and operating information, and IPv6 packet statistics.

Usage guidelines

If you do not specify an interface, this command displays IPv6 information about all interfaces.

If you specify only the *interface-type* argument, this command displays IPv6 information about the interfaces of the specified type.

If you specify both the *interface-type* and the *interface-number* arguments, this command displays IPv6 information about the specified interface.

Examples

Display IPv6 information about VLAN-interface 2.

```
<Switch> display ipv6 interface vlan-interface 2
Vlan-interface2 current state: UP
Line protocol current state: UP
IPv6 is enabled, link-local address is FE80::1234:56FF:FE65:4322 [TENTATIVE]
  Global unicast address(es):
    10::1234:56FF:FE65:4322, subnet is 10::/64 [TENTATIVE] [AUTOCFG]
      [valid lifetime 4641s/preferred lifetime 4637s]
    20::1234:56ff:fe65:4322, subnet is 20::/64 [TENTATIVE] [EUI-64]
    30::1, subnet is 30::/64 [TENTATIVE] [ANYCAST]
    40::2, subnet is 40::/64 [TENTATIVE] [DHCP]
    50::3, subnet is 50::/64 [TENTATIVE]
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:1
    FF02::1:FF65:4322
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND retransmit interval is 1000 milliseconds
  Hosts use stateless autoconfig for addresses
IPv6 Packet statistics:
  InReceives:                    0
  InTooShorts:                   0
  InTruncatedPkts:               0
  InHopLimitExceeds:             0
  InBadHeaders:                  0
  InBadOptions:                  0
  ReasmReqds:                    0
  ReasmOKs:                      0
  InFragDrops:                   0
  InFragTimeouts:                0
  OutFragFails:                  0
  InUnknownProtos:               0
  InDelivers:                    0
  OutRequests:                   0
  OutForwDatagrams:              0
  InNoRoutes:                    0
  InTooBigErrors:                0
  OutFragOKs:                    0
  OutFragCreates:                0
  InMcastPkts:                   0
  InMcastNotMembers:             0
```

```
OutMcastPkts:                 0
InAddrErrors:                 0
InDiscards:                   0
OutDiscards:                  0
```

Table 11-2 Command output

Field	Description
Vlan-interface2 current state	Physical state of the interface: • **Administratively DOWN**—The interface has been administratively shut down by using the **shutdown** command. • **DOWN**—The interface is administratively up but its physical state is down, possibly because of a connection or link failure. • **UP**—The administrative and physical states of the interface are both up.
Line protocol current state	Link layer state of the interface: • **DOWN**—The link layer protocol state of the interface is down. • **UP**—The link layer protocol state of the interface is up.
IPv6 is enabled	IPv6 is enabled on the interface. This feature is automatically enabled after an IPv6 address is configured for an interface.
link-local address	Link-local address of the interface.
Global unicast address(es)	Global unicast addresses of the interface. IPv6 address states: • **TENTATIVE**—Initial state. DAD is being performed or is to be performed on the address. • **DUPLICATE**—The address is not unique on the link. • **PREFERRED**—The address is preferred and can be used as the source or destination address of a packet. If an address is in this state, the command does not display the address state. • **DEPRECATED**—The address is beyond the preferred lifetime but in the valid lifetime. It is valid, but it cannot be used as the source address for a new connection. Packets destined for the address are processed correctly. If a global unicast address is not manually configured, the following notations indicate how the address is obtained: • **AUTOCFG**—Stateless autoconfigured. • **DHCP**—Assigned by a DHCPv6 server. • **EUI-64**—Manually configured EUI-64 IPv6 address. • **RANDOM**—Random address automatically generated. If the address is a manually configured anycast address, it is noted with **ANYCAST**.
valid lifetime	Specifies how long autoconfigured global unicast addresses using a prefix are valid.
preferred lifetime	Specifies how long autoconfigured global unicast addresses using a prefix are preferred.
Joined group address(es)	Addresses of the multicast groups that the interface has joined.

Field	Description
MTU	MTU of the interface.
ND DAD is enabled, number of DAD attempts	DAD is enabled. • If DAD is enabled, this field displays the number of attempts to send an NS message for DAD (set by using the **`ipv6 nd dad attempts`** command). • If DAD is disabled, this field displays **ND DAD is disabled**. To disable DAD, set the number of attempts to 0.
ND reachable time	Time during which a neighboring device is reachable.
ND retransmit interval	Interval for retransmitting an NS message.
Hosts use stateless autoconfig for addresses	Hosts obtained IPv6 addresses through stateless autoconfiguration.
InReceives	Received IPv6 packets, including error messages.
InTooShorts	Received IPv6 packets that are too short. For example, the received IPv6 packet is less than 40 bytes.
InTruncatedPkts	Received IPv6 packets with a length less than the payload length field specified in the packet header.
InHopLimitExceeds	Received IPv6 packets with a hop count exceeding the hop limit field specified in the packet header.
InBadHeaders	Received IPv6 packets with incorrect basic headers.
InBadOptions	Received IPv6 packets with incorrect extension headers.
ReasmReqds	Received IPv6 fragments.
ReasmOKs	Number of reassembled IPv6 packets.
InFragDrops	Received IPv6 fragments that are discarded because of certain errors.
InFragTimeouts	Received IPv6 fragments that are discarded because the amount of time they stay in the system buffer exceeds the specified interval.
OutFragFails	IPv6 packets that fail to be fragmented on the output interface.
InUnknownProtos	Received IPv6 packets with unknown or unsupported protocol type.
InDelivers	Received IPv6 packets that are delivered to user protocols (such as ICMPv6, TCP, and UDP).
OutRequests	Local IPv6 packets sent by IPv6 user protocols.
OutForwDatagrams	IPv6 packets forwarded by the interface.
InNoRoutes	Received IPv6 packets that are discarded because no matching route can be found.
InTooBigErrors	Received IPv6 packets that fail to be forwarded because they exceeded the Path MTU.
OutFragOKs	Fragmented IPv6 packets on the output interface.
OutFragCreates	Number of IPv6 fragments on the output interface.
InMcastPkts	Received IPv6 multicast packets.

Field	Description
InMcastNotMembers	Received IPv6 multicast packets that are discarded because the interface is not in the multicast group.
OutMcastPkts	IPv6 multicast packets sent by the interface.
InAddrErrors	Received IPv6 packets that are discarded due to invalid destination addresses.
InDiscards	Received IPv6 packets that are discarded due to resource problems rather than packet errors.
OutDiscards	IPv6 packets that fail to be sent due to resource problems rather than packet errors.

Display brief IPv6 information about all interfaces.

```
<Switch> display ipv6 interface brief
*down: administratively down
(s): spoofing
Interface                          Physical Protocol IPv6 Address
Vlan-interface1                    down     down     Unassigned
Vlan-interface2                    up       up       2001::1
Vlan-interface100                  up       up       Unassigned
```

Table 11-3 Command output

Field	Description
*down: administratively down	The interface has been administratively shut down by using the **shutdown** command.
(s): spoofing	Spoofing attribute of the interface. The link protocol state of the interface is up, but the link is temporarily established on demand or does not exist.
Interface	Name of the interface.
Physical	Physical state of the interface: • ***down**—The interface has been administratively shut down by using the **shutdown** command. • **down**—The interface is administratively up but its physical state is down, possibly because of a connection or link failure. • **up**—The administrative and physical states of the interface are both up.
Protocol	Link layer protocol state of the interface: • **down**—The network layer protocol state of the interface is down. • **up**—The network layer protocol state of the interface is up.
IPv6 Address	IPv6 address of the interface. • If multiple global unicast addresses are configured, this field displays the lowest address. • If no global unicast address is configured, this field displays the link-local address. • If no address is configured, this field displays **Unassigned**.

11.1.3. display ipv6 neighbors

Use **display ipv6 neighbors** to display IPv6 neighbor information.

Syntax

display ipv6 neighbors { { *ipv6-address* | **all** | **dynamic** | **static** } [**slot** *slot-number*] | **interface** *interface-type interface-number* | **vlan** *vlan-id* } [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ipv6-address: Specifies the IPv6 address of a neighbor whose information is displayed.

all: Displays information about all neighbors, including neighbors acquired dynamically and configured statically on the public network and all private networks.

dynamic: Displays information about all neighbors acquired dynamically.

static: Displays information about all neighbors configured statically.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays IPv6 neighbor information for all member devices.

interface *interface-type interface-number*: Specifies an interface by its type and number.

vlan *vlan-id*: Displays information about neighbors in the specified VLAN. The value range for VLAN ID is 1 to 4094.

verbose: Displays detailed neighbor information.

Examples

Display all neighbor information.

```
<Switch> display ipv6 neighbors all
Type: S-Static    D-Dynamic    O-Openflow     R-Rule    I-Invalid
IPv6 address                Link layer     VID       Interface/Link ID   State T  Age
1::2                        6864-6839-0202 1         GE1/0/1              STALE D  136
FE80::6A64:68FF:FE39:202  6864-6839-0202 1         GE1/0/1              STALE D  126
```

Display detailed information about all neighbors.

```
<Switch> display ipv6 neighbors all verbose
Type: S-Static    D-Dynamic    O-Openflow     R-Rule    I-Invalid
IPv6 Address: 1::2
Link Layer  : 6864-6839-0202      VID : 1    Interface: GE1/0/1
State       : STALE                 Type: D     Age      : 290
Vpn-instance: [No Vrf]
Nickname    : 0x0
IPv6 Address: FE80::6A64:68FF:FE39:202
Link Layer  : 6864-6839-0202      VID : 1    Interface: GE1/0/1
State       : STALE                 Type: D     Age      : 280
```

```
Vpn-instance: [No Vrf]
Nickname      : 0x0
```

Table 11-4 Command output

Field	Description
IPv6 Address	IPv6 address of a neighbor.
Link Layer	Link layer address (MAC address) of a neighbor.
VID	VLAN or virtual switch instance (VSI) to which the interface connected to a neighbor belongs. This field displays **N/A** if the VLAN ID or VSI index is invalid.

Interface/Link ID	Interface or link connected to a neighbor.
	• If the neighbor entry does not belong to a VSI, this field displays the interface name. If the interface name is not available, the field displays **N/A**.
	• If the neighbor entry belongs to a VSI and the interface is a tunnel interface, the displayed value depends on the address resolution status.
	  ○ If the address is not resolved, this field displays the VSI.
	  ○ If the address is resolved, this field displays the tunnel ID.
	• If the neighbor entry belongs to a VSI but the interface is not a tunnel interface, the displayed value depends on the address resolution status.
	  ○ If the address is not resolved, this field displays the VSI.
	  ○ If the address is resolved, this field displays the link ID. The link ID is a string with a maximum of eight hexadecimal numbers.

State	State of a neighbor: • **INCMP**—The address is being resolved. The link layer address of the neighbor is unknown. • **REACH**—The neighbor is reachable. • **STALE**—Whether the neighbor is reachable is unknown. The device does not verify the reachability any longer unless data is sent to the neighbor. • **DELAY**—Whether the neighbor is reachable is unknown. The device sends an NS message after a delay. • **PROBE**—Whether the neighbor is reachable is unknown. The device sends an NS message to verify the reachability of the neighbor.
Type	Neighbor information type: • **S**—Statically configured. • **D**—Dynamically obtained. • **O**—Learned from the OpenFlow module. • **R**—Learned from the Portal module. • **I**—Invalid.
Age	A hyphen (-) indicates a static entry. For a dynamic entry, this field displays the elapsed time in seconds. If the neighbor is never reachable, this field displays a pound sign (#).
Vpn-instance	Name of a VPN or **[No Vrf]** with no VPN configured.
Nickname	Nickname of a neighbor entry. The name is a string of four hexadecimal numbers.

Related commands

ipv6 neighbor

reset ipv6 neighbors

11.1.4. display ipv6 neighbors count

Use **display ipv6 neighbors count** to display the number of neighbor entries.

Syntax

display ipv6 neighbors { { **all** | **dynamic** | **static** } [**slot** *slot-number*] | **interface** *interface-type interface-number* | **vlan** *vlan-id* } **count**

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

all: Displays the total number of all neighbor entries, including neighbor entries created dynamically and configured statically.

dynamic: Displays the total number of neighbor entries created dynamically.

static: Displays the total number of neighbor entries configured statically.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays the number of neighbor entries for all member devices.

interface *interface-type interface-number*: Specifies an interface by its type and number.

vlan *vlan-id*: Displays the total number of neighbor entries in the specified VLAN. The value range for VLAN ID is 1 to 4094.

Examples

Display the total number of neighbor entries created dynamically.

```
<Switch> display ipv6 neighbors dynamic count
 Total number of dynamic entries: 2
```

11.1.5. display ipv6 neighbors vpn-instance

Use **display ipv6 neighbors vpn-instance** to display neighbor information about a VPN instance.

Syntax

display ipv6 neighbors vpn-instance *vpn-instance-name* [**count**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vpn-instance-name: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. The VPN instance must already exist.

count: Displays the total number of neighbor entries in the specified VPN instance.

Examples

Display neighbor information about the VPN instance **vpn1**.

```
<Switch> display ipv6 neighbors vpn-instance vpn1
Type: S-Static    D-Dynamic    O-Openflow     R-Rule    I-Invalid
IPv6 address                  Link Layer      VID  Interface      State T  Age
FE80::200:5EFF:FE32:B800    0000-5e32-b800  N/A  GE1/0/1        REACH IS -
```

Table 11-5 Command output

Field	Description
IPv6 address	IPv6 address of a neighbor.
Link-layer	Link layer address (MAC address) of a neighbor.
VID	VLAN to which the interface connected to a neighbor belongs.
Interface	Interface connected to a neighbor.
State	Neighbor state: • **INCMP**—The address is being resolved. The link layer address of the neighbor is unknown. • **REACH**—The neighbor is reachable. • **STALE**—Whether the neighbor is reachable is unknown. The device does not verify the reachability any longer unless data is sent to the neighbor. • **DELAY**—Whether the neighbor is reachable is unknown. The device sends an NS message after a delay. • **PROBE**—Whether the neighbor is reachable is unknown. The device sends an NS message to verify the reachability of the neighbor.
T	Neighbor information type: • **S**—Statically configured. • **D**—Dynamically obtained. • **O**—Learned from the OpenFlow module. • **I**—Invalid.
Age	A hyphen (-) indicates a static entry. For a dynamic entry, this field displays the elapsed time in seconds. If the neighbor is never reachable, this field displays a pound sign (#).

11.1.6. display ipv6 pathmtu

Use the **display ipv6 pathmtu** command to display IPv6 Path MTU information.

Syntax

display ipv6 pathmtu [**vpn-instance** *vpn-instance-name*] { *ipv6-address* | { **all** | **dynamic** | **static** } [**count**] }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays IPv6 Path MTU information about the public network.

ipv6-address: Specifies the destination IPv6 address for which the Path MTU information is to be displayed.

all: Displays all Path MTU information for the public network.

dynamic: Displays all dynamic Path MTU information.

static: Displays all static Path MTU information.

count: Displays the total number of Path MTU entries.

Examples

Display all Path MTU information.

```
<Switch> display ipv6 pathmtu all
IPv6 destination address                PathMTU   Age    Type
1:2::3:2                                   1800       -      Static
1:2::4:2                                   1400       10     Dynamic
1:2::5:2                                   1280       10     Dynamic
```

Displays the total number of Path MTU entries.

```
<Switch> display ipv6 pathmtu all count
Total number of entries: 3
```

Table 11-6 Command output

Field	Description
PathMTU	Path MTU value on the network path to an IPv6 address.
Age	Time for a Path MTU to live. For a static Path MTU, this field displays a hyphen (-).
Type	Path MTU type: • **Dynamic**—Dynamically negotiated. • **Static**—Statically configured.
Total number of entries	Total number of Path MTU entries.

Related commands

ipv6 pathmtu

reset ipv6 pathmtu

11.1.7. display ipv6 rawip

Use **display ipv6 rawip** to display brief information about IPv6 RawIP connections.

Syntax

display ipv6 rawip [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays brief information about IPv6 RawIP connections for all member devices.

Examples

Display brief information about IPv6 RawIP connections.

```
<Switch> display ipv6 rawip
Local Addr            Foreign Addr        Protocol Slot    PCB
2001:2002:2003:2      3001:3002:3003:3    58       1       0x0000000000000009
004:2005:2006:20      004:3005:3006:30
07:2008                 07:3008
2002::100             2002::138            58       2       0x0000000000000008
::                      ::                   58       5       0x0000000000000002
```

Table 11-7 Command output

Field	Description
Local Addr	Local IPv6 address.
Foreign Addr	Peer IPv6 address.
Protocol	Protocol number.
PCB	PCB index.

11.1.8. display ipv6 rawip verbose

Use **display ipv6 rawip verbose** to display detailed information about IPv6 RawIP connections.

Syntax

display ipv6 rawip verbose [**slot** *slot-number* [**pcb** *pcb-index*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

pcb *pcb-index*: Displays detailed information about IPv6 RawIP connections of the specified PCB. The value range for the *pcb-index* argument is 1 to 16.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays detailed information about IPv6 RawIP connections for all member devices.

Examples

Display detailed information about an IPv6 RawIP connection.

```
<Switch> display ipv6 rawip verbose
Total RawIP socket number: 1

 Location: slot: 6
 Creator: ping ipv6[320]
 State: N/A
 Options: N/A
 Error: 0
 Receiving buffer(cc/hiwat/lowat/drop/state): 0 / 9216 / 1 / 0 / N/A
 Sending buffer(cc/hiwat/lowat/state): 0 / 9216 / 512 / N/A
 Type: 3
 Protocol: 58
 Connection info: src = ::, dst = ::
 Inpcb flags: N/A
 Inpcb extflag: INP_EXTRCVICMPERR INP_EXTFILTER
 Inpcb vflag: INP_IPV6
 Hop limit: 255 (minimum hop limit: 0)
 Send VRF: 0xffff
 Receive VRF: 0xffff
```

Table 11-8 Command output

Field	Description
Total RawIP socket number	Total number of IPv6 RawIP sockets.
Creator	Task name of the socket. The process number is in the square brackets.
State	Socket state.
Options	Socket options.
Error	Error code.

Receiving buffer (cc/hiwat/lowat/drop/state)	Displays receive buffer information in the following order:
	• **cc**—Used space.
	• **hiwat**—Maximum space.
	• **lowat**—Minimum space.
	• **drop**—Number of dropped packets.
	• **state**—Buffer state:
	  ○ **CANTSENDMORE**—Unable to send data to the peer.
	  ○ **CANTRCVMORE**—Unable to receive data from the peer.
	  ○ **RCVATMARK**—Receiving tag.
	  ○ **N/A**—None of the above states.

Sending buffer(cc/hiwat/lowat/state)	Displays send buffer information in the following order: • **cc**—Used space.

Field	Description

	• **hiwat**—Maximum space.
	• **lowat**—Minimum space.
	• **state**—Buffer state:
	  ○ **CANTSENDMORE**—Unable to send data to the peer.
	  ○ **CANTRCVMORE**—Unable to receive data from the peer.
	  ○ **RCVATMARK**—Receiving tag.
	  ○ **N/A**—None of the above states.

Type	Socket type: • **1**—**SOCK_STREAM**. This socket uses TCP to provide reliable transmission of byte streams. • **2**—**SOCK_DGRAM**. This socket uses UDP to provide datagram transmission. • **3**—**SOCK_RAW**. This socket allows an application to change the next upper-layer protocol header. • **N/A**—None of the above types.
Protocol	Number of protocol using the socket. 58 represents ICMP.
Connection info	Connection information, including the source and destination IPv6 addresses.
Inpcb flags	Flags in the Internet PCB: • **INP_RECVOPTS**—Receives IPv6 options. • **INP_RECVRETOPTS**—Receives replied IPv6 options. • **INP_RECVDSTADDR**—Receives destination IPv6 address. • **INP_HDRINCL**—Provides the entire IPv6 header. • **INP_REUSEADDR**—Reuses the IPv6 address. • **INP_REUSEPORT**—Reuses the port number. • **INP_ANONPORT**—Port number not specified. • **INP_PROTOCOL_PACKET**—Identifies a protocol packet. • **INP_RCVVLANID**—Receives the VLAN ID of the packet. Only UDP and RawIP support this flag. • **IN6P_IPV6_V6ONLY**—Only supports IPv6 protocol stack. • **IN6P_PKTINFO**—Receives the source IPv6 address and input interface of the packet. • **IN6P_HOPLIMIT**—Receives the hop limit. • **IN6P_HOPOPTS**—Receives the hop-by-hop options extension header. • **IN6P_DSTOPTS**—Receives the destination options extension header. • **IN6P_RTHDR**—Receives the routing extension header. • **IN6P_RTHDRDSTOPTS**—Receives the destination options extension header preceding the routing extension header. • **IN6P_TCLASS**—Receives the traffic class of the packet. • **IN6P_AUTOFLOWLABEL**—Attaches a flow label automatically. • **IN6P_RFC2292**—Uses the API specified in RFC 2292. • **IN6P_MTU**—Discovers differences in the MTU size of every link along a given data path. TCP does not support

Field	Description
	this flag. • **INP_RCVMACADDR**—Receives the MAC address of the frame. • **INP_USEICMPSRC**—Uses the specified IPv6 address as the source IPv6 address for outgoing ICMP packets. • **INP_SYNCPCB**—Waits until Internet PCB is synchronized. • **N/A**—None of the above flags.
Inpcb extflag	Extension flags in the Internet PCB: • **INP_EXTRCVPVCIDX**—Records the PVC index of the received packet. • **INP_RCVPWID**—Records the PW ID of the received packet. • **INP_EXTRCVICMPERR**—Receives an ICMP error packet. • **INP_EXTFILTER**—Filters the contents in the received packet. • **N/A**—None of the above flags.
Inpcb vflag	IP version flag in the Internet PCB: • **INP_IPV4**—IPv4 protocol. • **INP_IPV6**—IPv6 protocol. • **INP_IPV6PROTO**—Creates an Internet PCB based on IPv6 protocol. • **INP_TIMEWAIT**—In **TIMEWAIT** state. • **INP_ONESBCAST**—Sends broadcast packets. • **INP_DROPPED**—Protocol dropped flag. • **INP_SOCKREF**—Strong socket reference. • **INP_DONTBLOCK**—Do not block synchronization of the Internet PCB. • **N/A**—None of the above flags.
Hop limit	Hop limit in the Internet PCB.
Send VRF	VRF from which packets are sent.
Receive VRF	VRF from which packets are received.

11.1.9. display ipv6 statistics

Use **display ipv6 statistics** to display IPv6 and ICMPv6 packet statistics.

Syntax

display ipv6 statistics [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays IPv6 and ICMPv6 packet statistics for all member devices.

Examples

Display IPv6 and ICMPv6 packet statistics.

```
<Switch> display ipv6 statistics
  IPv6 statistics:

    Sent packets:
      Total:      0
        Sent locally:          0            Forwarded:               0
        Raw packets:           0            Discarded:               0
        Fragments:             0            Fragments failed:      0
        Routing failed:        0

    Received packets:
      Total:      0
        Received locally:      0            Hop limit exceeded:  0
        Fragments:              0            Reassembled:            0
        Reassembly failures:   0            Reassembly timeout:  0
        Format errors:          0            Option errors:         0
        Protocol errors:       0

  ICMPv6 statistics:

    Sent packets:
      Total:      0
        Unreachable:            0             Too big:                 0
        Hop limit exceeded:    0            Reassembly timeouts: 0
        Parameter problems:    0
        Echo requests:          0             Echo replies:           0
        Neighbor solicits:     0            Neighbor adverts:      0
        Router solicits:       0            Router adverts:         0
        Redirects:              0              Router renumbering:    0
      Send failed:
        Rate limitation:       0            Other errors:           0

    Received packets:
      Total:      0
        Checksum errors:       0            Too short:               0
        Bad codes:              0
        Unreachable:            0             Too big:                  0
        Hop limit exceeded:    0            Reassembly timeouts:    0
        Parameter problems:    0            Unknown error types:    0
        Echo requests:          0             Echo replies:             0
        Neighbor solicits:     0            Neighbor adverts:       0
        Router solicits:        0             Router adverts:         0
```

```
    Redirects:                0            Router renumbering:    0
    Unknown info types:    0
  Deliver failed:
    Bad length:            0
```

Related commands

reset ipv6 statistics

11.1.10. display ipv6 tcp

Use **display ipv6 tcp** to display brief information about IPv6 TCP connections.

Syntax

display ipv6 tcp [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays brief information about IPv6 TCP connections for all member devices.

Examples

Display brief information about IPv6 TCP connections.

```
<Switch> display ipv6 tcp
*: TCP connection with authentication
 LAddr->port          FAddr->port       State        Slot   PCB
*2001:2002:2003:2    3001:3002:3003:3 ESTABLISHED 1      0x000000000000c387
004:2005:2006:20     004:3005:3006:30
07:2008->1200         07:3008->1200
2001::1->23           2001::5->1284     ESTABLISHED 2      0x0000000000000008
2003::1->25           2001::2->1283     LISTEN       3      0x0000000000000009
```

Table 11-9 Command output

Field	Description
*	Indicates that the TCP connection uses authentication.
LAddr->port	Local IPv6 address and port number.
FAddr->port	Peer IPv6 address and port number.
State	IPv6 TCP connection state.
PCB	PCB index.

11.1.11. display ipv6 tcp verbose

Use **display ipv6 tcp verbose** to display detailed information about IPv6 TCP connections.

Syntax

display ipv6 tcp verbose [**slot** *slot-number* [**pcb** *pcb-index*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

pcb *pcb-index*: Displays detailed information about IPv6 TCP connections of the specified PCB. The value range for the *pcb-index* argument is 1 to 16.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays detailed information about IPv6 TCP connections for all member devices.

Examples

Display detailed information about an IPv6 TCP connection.

```
<Switch> display ipv6 tcp verbose
TCP inpcb number: 1(tcpcb number: 1)

 Location: Slot: 6
 NSR standby: N/A
 Creator: bgpd[199]
 State: ISCONNECTED
 Options: N/A
 Error: 0
 Receiving buffer(cc/hiwat/lowat/state): 0 / 65536 / 1 / N/A
 Sending buffer(cc/hiwat/lowat/state): 0 / 65536 / 512 / N/A
 Type: 1
 Protocol: 6
 Connection info: src = 2001::1->179 ,  dst = 2001::2->4181
 Inpcb flags: N/A
 Inpcb extflag: N/A
 Inpcb vflag: INP_IPV6
 Hop limit: 255 (minimum hop limit: 0)
 Connection state: ESTABLISHED
 TCP options: TF_REQ_SCALE TF_REQ_TSTMP TF_SACK_PERMIT TF_NSR
 NSR state: READY(M)
 Send VRF: 0x0
 Receive VRF: 0x0
```

Table 11-10 Command output

Field	Description
TCP inpcb number	Number of IPv6 TCP Internet PCBs.
tcpcb number	Number of IPv6 TCP PCBs (excluding PCBs of TCP in TIME_WAIT state).
Creator	Task name of the socket. The process number is in the square brackets.
State	Socket state.
Options	Socket options.
Error	Error code.

Receiving buffer(cc/hiwat/lowat/state)	Displays receive buffer information in the following order:
	• **cc**—Used space.
	• **hiwat**—Maximum space.
	• **lowat**—Minimum space.
	• **state**—Buffer state:
	  ○ **CANTSENDMORE**—Unable to send data to the peer.
	  ○ **CANTRCVMORE**—Unable to receive data from the peer.
	  ○ **RCVATMARK**—Receiving tag.
	  ○ **N/A**—None of the above states.

Sending buffer(cc/hiwat/lowat/state)	Displays send buffer information in the following order:
	• **cc**—Used space.
	• **hiwat**—Maximum space.
	• **lowat**—Minimum space.
	• **state**—Buffer state:
	  ○ **CANTSENDMORE**—Unable to send data to the peer.
	  ○ **CANTRCVMORE**—Unable to receive data from the peer.
	  ○ **RCVATMARK**—Receiving tag.
	  ○ **N/A**—None of the above states.

Type	Socket type: • **1**—**SOCK_STREAM**. This socket uses TCP to provide reliable transmission of byte streams. • **2**—**SOCK_DGRAM**. This socket uses UDP to provide datagram transmission. • **3**—**SOCK_RAW**. This socket allows an application to change the next upper-layer protocol header. • **N/A**—None of the above types.
Protocol	Number of the protocol using the socket. 6 represents TCP.
Connection info	Connection information, including source IPv6 address and port number, and destination IPv6 address and port number.
Inpcb flags	Flags in the Internet PCB: • **INP_RECVOPTS**—Receives IPv6 options. • **INP_RECVRETOPTS**—Receives replied IPv6 options. • **INP_RECVDSTADDR**—Receives destination IPv6 address.

Field	Description
	• **INP_HDRINCL**—Provides the entire IPv6 header. • **INP_REUSEADDR**—Reuses the IPv6 address. • **INP_REUSEPORT**—Reuses the port number. • **INP_ANONPORT**—Port number not specified. • **INP_PROTOCOL_PACKET**—Identifies a protocol packet. • **INP_RCVVLANID**—Receives the VLAN ID of the packet. Only UDP and RawIP support this flag. • **IN6P_IPV6_V6ONLY**—Only supports IPv6 protocol stack. • **IN6P_PKTINFO**—Receives the source IPv6 address and input interface of the packet. • **IN6P_HOPLIMIT**—Receives the hop limit. • **IN6P_HOPOPTS**—Receives the hop-by-hop options extension header. • **IN6P_DSTOPTS**—Receives the destination options extension header. • **IN6P_RTHDR**—Receives the routing extension header. • **IN6P_RTHDRDSTOPTS**—Receives the destination options extension header preceding the routing extension header. • **IN6P_TCLASS**—Receives the traffic class of the packet. • **IN6P_AUTOFLOWLABEL**—Attaches a flow label automatically. • **IN6P_RFC2292**—Uses the API specified in RFC 2292. • **IN6P_MTU**—Discovers differences in the MTU size of every link along a given data path. TCP does not support this flag. • **INP_RCVMACADDR**—Receives the MAC address of the frame. • **INP_SYNCPCB**—Waits until Internet PCB is synchronized. • **N/A**—None of the above flags.
Inpcb extflag	Extension flags in the Internet PCB: • **INP_EXTRCVPVCIDX**—Records the PVC index of the received packet. • **INP_RCVPWID**—Records the PW ID of the received packet. • **INP_EXTDONTDROP**—Does not drop the received packet. • **INP_EXLISTEN**—Listening socket. • **N/A**—None of the above flags.
Inpcb vflag	IP version flags in the Internet PCB: • **INP_IPV4**—IPv4 protocol. • **INP_IPV6**—IPv6 protocol. • **INP_IPV6PROTO**—Creates an Internet PCB based on IPv6 protocol. • **INP_TIMEWAIT**—In **TIMEWAIT** state. • **INP_ONESBCAST**—Sends broadcast packets. • **INP_DROPPED**—Protocol dropped flag. • **INP_SOCKREF**—Strong socket reference. • **INP_DONTBLOCK**—Do not block synchronization of

Field	Description
	the Internet PCB. • **N/A**—None of the above flags.
Hop limit	Hop limit in the Internet PCB.
Connection state	TCP connection state: • **CLOSED**—The server receives a disconnection request's reply from the client. • **LISTEN**—The server is waiting for connection requests. • **SYN_SENT**—The client is waiting for the server to reply to the connection request. • **SYN_RCVD**—The server receives a connection request. • **ESTABLISHED**—The server and client have established connections and can transmit data bidirectionally. • **CLOSE_WAIT**—The server receives a disconnection request from the client. • **FIN_WAIT_1**—The client is waiting for the server to reply to a disconnection request. • **CLOSING**—The server and client are waiting for peer's disconnection reply when receiving disconnection requests from each other. • **LAST_ACK**—The server is waiting for the client to reply to a disconnection request. • **FIN_WAIT_2**—The client receives a disconnection reply from the server. • **TIME_WAIT**—The client receives a disconnection request from the server.
TCP options	TCP options: • **TF_MD5SIG**—Enables MD5 signature. • **TF_NODELAY**—Disables the Nagle algorithm that buffers the sent data inside the TCP. • **TF_NOOPT**—No TCP options. • **TF_NOPUSH**—Forces TCP to delay sending any TCP data until a full sized segment is buffered in the TCP buffers. • **TF_BINDFOREIGNADDR**—Binds the peer IP address. • **TF_NSR**—Enables TCP NSR. • **TF_REQ_SCALE**—Enables the TCP window scale option. • **TF_REQ_TSTMP**—Enables the time stamp option. • **TF_SACK_PERMIT**—Enables the TCP selective acknowledgement option. • **TF_ENHANCED_AUTH**—Enables the enhanced authentication option.
NSR state	State of the TCP connections. Between the parentheses is the role of the connection: • **M**—Main connection. • **S**—Standby connection.
Send VRF	VRF from which packets are sent.
Receive VRF	VRF from which packets are received.

11.1.12. display ipv6 udp

Use **display ipv6 udp** to display brief information about IPv6 UDP connections.

Syntax

display ipv6 udp [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays brief information about IPv6 UDP connections for all member devices.

Examples

Displays brief information about IPv6 UDP connections.

```
<Switch> display ipv6 udp
 LAddr->port          FAddr->port          Slot    PCB
 2001:2002:2003:2    3001:3002:3003:3    1        0x000000000000c387
 004:2005:2006:20    004:3005:3006:30
 07:2008->1200       07:3008->1200
 2001::1->23          2001::5->1284        2        0x0000000000000008
 2003::1->25          2001::2->1283        3        0x0000000000000009
```

Table 11-11 Command output

Field	Description
LAddr->port	Local IPv6 address and port number.
FAddr->port	Peer IPv6 address and port number.
PCB	PCB index.

11.1.13. display ipv6 udp verbose

Use **display ipv6 udp verbose** to display detailed information about IPv6 UDP connections.

Syntax

display ipv6 udp verbose [**slot** *slot-number* [**pcb** *pcb-index*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

pcb *pcb-index*: Displays detailed information about IPv6 UDP connections of the specified PCB. The value range for the *pcb-index* argument is 1 to 16.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays detailed information about IPv6 UDP connections for all member devices.

Examples

Display detailed information about an IPv6 UDP connection.

```
<Switch> display ipv6 udp verbose
Total UDP socket number: 1

 Location: slot: 6
 Creator: sock_test_mips[250]
 State: N/A
 Options: N/A
 Error: 0
 Receiving buffer(cc/hiwat/lowat/drop/state): 0 / 41600 / 1 / 0 / N/A
 Sending buffer(cc/hiwat/lowat/state): 0 / 9216 / 512 / N/A
 Type: 2
 Protocol: 17
 Connection info: src = ::->69, dst = ::->0
 Inpcb flags: N/A
 Inpcb extflag: N/A
 Inpcb vflag: INP_IPV6
 Hop limit: 255 (minimum hop limit: 0)
 Send VRF: 0xffff
 Receive VRF: 0xffff
```

Table 11-12 Command output

Field	Description
Total UDP socket number	Total number of IPv6 UDP sockets.
Creator	Task name of the socket. The progress number is in the square brackets.
State	Socket state.
Options	Socket options.
Error	Error code.

Receiving buffer(cc/hiwat/lowat/drop/state)	Displays receive buffer information in the following order:
	• **cc**—Used space.
	• **hiwat**—Maximum space.
	• **lowat**—Minimum space.
	• **drop**—Number of dropped packets.
	• **state**—Buffer state:
	  ○ **CANTSENDMORE**—Unable to send data to the peer.
	  ○ **CANTRCVMORE**—Unable to receive data from the peer.
	  ○ **RCVATMARK**—Receiving tag.

Field	Description
	○ **N/A**—None of the above states.
Sending buffer(cc/hiwat/lowat/state)	Displays send buffer information in the following order: • **cc**—Used space. • **hiwat**—Maximum space. • **lowat**—Minimum space. • **state**—Buffer state: ○ **CANTSENDMORE**—Unable to send data to the peer. ○ **CANTRCVMORE**—Unable to receive data from the peer. ○ **RCVATMARK**—Receiving tag. ○ **N/A**—None of the above states.
Type	Socket type: • **1**—**SOCK_STREAM**. This socket uses TCP to provide reliable transmission of byte streams. • **2**—**SOCK_DGRAM**. This socket uses UDP to provide datagram transmission. • **3**—**SOCK_RAW**. This socket allows an application to change the next upper-layer protocol header. • **N/A**—None of the above types.
Protocol	Number of the protocol using the socket. 17 represents UDP.
Connection info	Connection information, including source IPv6 address and port number, and destination IPv6 address and port number.
Inpcb flags	Flags in the Internet PCB: • **INP_RECVOPTS**—Receives IPv6 options. • **INP_RECVRETOPTS**—Receives replied IPv6 options. • **INP_RECVDSTADDR**—Receives destination IPv6 address. • **INP_HDRINCL**—Provides the entire IPv6 header. • **INP_REUSEADDR**—Reuses the IPv6 address. • **INP_REUSEPORT**—Reuses the port number. • **INP_ANONPORT**—Port number not specified. • **INP_PROTOCOL_PACKET**—Identifies a protocol packet. • **INP_RCVVLANID**—Receives the VLAN ID of the packet. Only UDP and RawIP support this flag. • **IN6P_IPV6_V6ONLY**—Only supports IPv6 protocol stack. • **IN6P_PKTINFO**—Receives the source IPv6 address and input interface of the packet. • **IN6P_HOPLIMIT**—Receives the hop limit. • **IN6P_HOPOPTS**—Receives the hop-by-hop options extension header. • **IN6P_DSTOPTS**—Receives the destination options extension header. • **IN6P_RTHDR**—Receives the routing extension header. • **IN6P_RTHDRDSTOPTS**—Receives the destination options extension header preceding the routing

Field	Description
	extension header. • **IN6P_TCLASS**—Receives the traffic class of the packet. • **IN6P_AUTOFLOWLABEL**—Attaches a flow label automatically. • **IN6P_RFC2292**—Uses the API specified in RFC 2292. • **IN6P_MTU**—Discovers differences in the MTU size of every link along a given data path. TCP does not support this flag. • **INP_RCVMACADDR**—Receives the MAC address of the frame. • **INP_SYNCPCB**—Waits until Internet PCB is synchronized. • **N/A**—None of the above flags.
Inpcb extflag	Extension flags in the Internet PCB: • **INP_EXTRCVPVCIDX**—Records the PVC index of the received packet. • **INP_RCVPWID**—Records the PW ID of the received packet. • **N/A**—None of the above flags.
Inpcb vflag	IP version flags in the Internet PCB: • **INP_IPV4**—IPv4 protocol. • **INP_IPV6**—IPv6 protocol. • **INP_IPV6PROTO**—Creates an Internet PCB based on IPv6 protocol. • **INP_TIMEWAIT**—In **TIMEWAIT** state. • **INP_ONESBCAST**—Sends broadcast packets. • **INP_DROPPED**—Protocol dropped flag. • **INP_SOCKREF**—Strong socket reference. • **INP_DONTBLOCK**—Do not block synchronization of the Internet PCB. • **N/A**—None of the above flags.
Hop limit	Hop limit in the Internet PCB.
Send VRF	VRF from which packets are sent.
Receive VRF	VRF from which packets are received.

11.1.14. ipv6 address

Use **ipv6 address** to configure an IPv6 global unicast address for an interface.

Use **undo ipv6 address** to delete an IPv6 global unicast address of the interface.

Syntax

ipv6 address { *ipv6-address prefix-length* | *ipv6-address*/*prefix-length* }

undo ipv6 address [*ipv6-address prefix-length* | *ipv6-address*/*prefix-length*]

Default

No IPv6 global unicast address is configured for an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies an IPv6 address.

prefix-length: Specifies a prefix length in the range of 1 to 128.

Usage guidelines

Like public IPv4 addresses, IPv6 global unicast addresses are assigned to ISPs. This type of address allows for prefix aggregation to reduce the number of global routing entries.

If you do not specify any parameters, the **undo ipv6 address** command deletes all IPv6 addresses of an interface.

Examples

Set the IPv6 global unicast address of VLAN-interface 100 to 2001::1 with prefix length 64.

Method 1:

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ipv6 address 2001::1/64
```

Method 2:

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ipv6 address 2001::1 64
```

11.1.15. ipv6 address anycast

Use **ipv6 address anycast** to configure an IPv6 anycast address for an interface.

Use **undo ipv6 address anycast** to delete the IPv6 anycast address of the interface.

Syntax

ipv6 address { *ipv6-address prefix-length* | *ipv6-address*/*prefix-length* } **anycast**

undo ipv6 address { *ipv6-address prefix-length* | *ipv6-address*/*prefix-length* } **anycast**

Default

No IPv6 anycast address is configured for an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

*ipv6-address*s: Specifies an IPv6 anycast address.

prefix-length: Specifies a prefix length in the range of 1 to 128.

Examples

Set the IPv6 anycast address of VLAN-interface 100 to 2001::1 with prefix length 64.

Method 1:

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ipv6 address 2001::1/64 anycast
```

Method 2:

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ipv6 address 2001::1 64 anycast
```

11.1.16. ipv6 address auto

Use **ipv6 address auto** to enable the stateless address autoconfiguration feature on an interface, so that the interface can automatically generate a global unicast address.

Use **undo ipv6 address auto** to disable this feature.

Syntax

ipv6 address auto

undo ipv6 address auto

Default

The stateless address autoconfiguration feature is disabled.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

After a global unicast address is generated through stateless autoconfiguration, a link-local address is generated automatically.

To delete the global unicast address and the link-local address that are automatically generated, use either of the following commands:

- **undo ipv6 address auto**
- **undo ipv6 address**

Examples

Enable stateless address autoconfiguration on VLAN-interface 100.

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ipv6 address auto
```

11.1.17. ipv6 address auto link-local

Use **ipv6 address auto link-local** to automatically generate a link-local address for an interface.

Use **undo ipv6 address auto link-local** to restore the default.

Syntax

ipv6 address auto link-local

undo ipv6 address auto link-local

Default

No link-local address is configured on an interface. A link-local address is automatically generated after an IPv6 global unicast address is configured for the interface.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

Link-local addresses are used for neighbor discovery and stateless autoconfiguration on the local link. Packets using link-local addresses as the source or destination addresses cannot be forwarded to other links.

After an IPv6 global unicast address is configured for an interface, a link-local address is automatically generated. This link-local address is the same as the one generated by using the **ipv6 address auto link-local** command.

The **undo ipv6 address auto link-local** command deletes only the link-local addresses generated through the **ipv6 address auto link-local** command. If the **undo** command is executed on an interface with an IPv6 global unicast address configured, the interface still has a link-local address.

You can also manually assign an IPv6 link-local address for an interface by using the **ipv6 address link-local** command. Manual assignment takes precedence over automatic generation for IPv6 link-local addresses.

- If you first use automatic generation and then manual assignment, the manually assigned link-local address overwrites the automatically generated address.
- If you first use manual assignment and then automatic generation, both of the following occur:
  - The automatically generated link-local address does not take effect.
  - The link-local address of an interface is still the manually assigned address.

  If you delete the manually assigned address, the automatically generated link-local address takes effect.

Examples

Configure VLAN-interface 100 to automatically generate a link-local address.

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ipv6 address auto link-local
```

Related commands

ipv6 address link-local

11.1.18. ipv6 address eui-64

Use **ipv6 address eui-64** to configure an EUI-64 IPv6 address for an interface.

Use **undo ipv6 address eui-64** to delete an EUI-64 IPv6 address from an interface.

Syntax

ipv6 address { *ipv6-address prefix-length* | *ipv6-address/prefix-length* } **eui-64**

undo ipv6 address [*ipv6-address prefix-length* | *ipv6-address/prefix-length*] **eui-64**

Default

No EUI-64 IPv6 address is configured for an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

ipv6-address/prefix-length: Specifies an IPv6 address and IPv6 prefix length. The *ipv6-address* and *prefix-length* arguments jointly specify the prefix of an EUI-64 IPv6 address. The value range for the *prefix-length* argument is 1 to 64.

Usage guidelines

An EUI-64 IPv6 address is generated based on the specified prefix and the automatically generated interface ID. To display the EUI-64 IPv6 address, use the **display ipv6 interface** command.

The prefix length of an EUI-64 IPv6 address cannot be greater than 64.

Examples

Configure an EUI-64 IPv6 address for VLAN-interface 100. The prefix of the address is the same as that of 2001::1/64, and the interface ID is generated based on the MAC address of the device.

Method 1:

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ipv6 address 2001::1/64 eui-64
```

Method 2:

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ipv6 address 2001::1 64 eui-64
```

Related commands

display ipv6 interface

11.1.19. ipv6 address link-local

Use **ipv6 address link-local** to configure a link-local address for the interface.

Use **undo ipv6 address link-local** to restore the default.

Syntax

ipv6 address *ipv6-address* **link-local**

undo ipv6 address *ipv6-address* **link-local**

Default

No link-local address is configured for the interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies an IPv6 link-local address. The first 10 bits of an address must be 1111111010 (binary). The first group of hexadecimals in the address must be FE80 to FEBF.

Usage guidelines

Manual assignment takes precedence over automatic generation.

If you use automatic generation, and then use manual assignment, the manually assigned link-local address overwrites the one that is automatically generated.

If you use manual assignment and then use automatic generation, both of the following occur:

- The automatically generated link-local address does not take effect.
- The manually assigned link-local address of an interface remains.

After you delete the manually assigned address, the automatically generated link-local address takes effect. For automatic generation of an IPv6 link-local address, see the **ipv6 address auto link-local** command.

Examples

Configure a link-local address for VLAN-interface 100.

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ipv6 address fe80::1 link-local
```

Related commands

ipv6 address auto link-local

11.1.20. ipv6 hop-limit

Use **ipv6 hop-limit** to set the Hop Limit field in the IPv6 header.

Use **undo ipv6 hop-limit** to restore the default.

Syntax

ipv6 hop-limit *value*

undo ipv6 hop-limit

Default

The hop limit is 64.

Views

System view

Predefined user roles

network-admin

Parameters

value: Specifies the number of hops, in the range of 1 to 255.

Usage guidelines

The hop limit determines the number of hops that an IPv6 packet generated by the device can travel.

The device advertises the hop limit in RA messages. All RA message receivers use the advertised value to fill in the Hop Limit field for IPv6 packets to be sent.

Examples

Set the maximum number of hops to 100.

```
<Switch> system-view
[Switch] ipv6 hop-limit 100
```

11.1.21. ipv6 hoplimit-expires enable

Use **ipv6 hoplimit-expires enable** to enable sending ICMPv6 time exceeded messages.

Use **undo ipv6 hoplimit-expires** to disable sending ICMPv6 time exceeded messages.

Syntax

ipv6 hoplimit-expires enable

undo ipv6 hoplimit-expires enable

Default

Sending ICMPv6 time exceeded messages is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

ICMPv6 time exceeded messages are sent to the source of IPv6 packets after the device discards IPv6 packets because hop or reassembly times out.

To prevent too many ICMPv6 error messages from affecting device performance, disable this feature. Even with the feature disabled, the device still sends fragment reassembly time exceeded messages.

Examples

Disable sending ICMPv6 time exceeded messages.

```
<Switch> system-view
[Switch] undo ipv6 hoplimit-expires enable
```

11.1.22. ipv6 icmpv6 error-interval

Use **ipv6 icmpv6 error-interval** to set the bucket size and the interval for tokens to arrive in the bucket for ICMPv6 error messages.

Use **undo ipv6 icmpv6 error-interval** to restore the default.

Syntax

ipv6 icmpv6 error-interval *interval* [*bucketsize*]

undo ipv6 icmpv6 error-interval

Default

The bucket allows a maximum of 10 tokens, and a token is placed in the bucket every 100 milliseconds.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the interval for tokens to arrive in the bucket. The value range is 0 to 2147483647 milliseconds. To disable the ICMPv6 rate limit, set the value to 0.

bucketsize: Specifies the maximum number of tokens allowed in the bucket. The value range is 1 to 200.

Usage guidelines

This command limits the rate at which ICMPv6 error messages are sent. Use this command to prevent network congestion caused by excessive ICMPv6 error messages generated within a short period. A token bucket algorithm is used with one token representing one ICMPv6 error message.

A token is placed in the bucket at intervals until the maximum number of tokens that the bucket can hold is reached.

A token is removed from the bucket when an ICMPv6 error message is sent. When the bucket is empty, ICMPv6 error messages are not sent until a new token is placed in the bucket.

Examples

Set the bucket size to 40 tokens and the interval for tokens to arrive in the bucket to 200 milliseconds for ICMPv6 error messages.

```
<Switch> system-view
[Switch] ipv6 icmpv6 error-interval 200 40
```

11.1.23. ipv6 icmpv6 multicast-echo-reply enable

Use **ipv6 icmpv6 multicast-echo-reply enable** to enable replying to multicast echo requests.

Use **undo ipv6 icmpv6 multicast-echo-reply** to restore the default.

Syntax

ipv6 icmpv6 multicast-echo-reply enable

undo ipv6 icmpv6 multicast-echo-reply enable

Default

The device is disabled from replying to multicast echo requests.

Views

System view

Predefined user roles

network-admin

Usage guidelines

If a host is configured to reply to multicast echo requests, an attacker can use this mechanism to attack the host. For example, the attacker can send an echo request to a multicast address with Host A as the source. All hosts in the multicast group will send echo replies to Host A.

To prevent attacks, do not enable the device to reply to multicast echo requests unless necessary.

Examples

Enable replying to multicast echo requests.

```
<Switch> system-view
[Switch] ipv6 icmpv6 multicast-echo-reply enable
```

11.1.24. ipv6 mtu

Use **ipv6 mtu** to configure the MTU of IPv6 packets sent over an interface.

Use **undo ipv6 mtu** to restore the default MTU.

Syntax

ipv6 mtu *size*

undo ipv6 mtu

Default

No MTU is configured for an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

size: Specifies the size of the MTUs of an interface in bytes. The following are value ranges for different interface types:

- 1280 to 9216 for VLAN interfaces.
- 1280 to 1500 for management Ethernet interfaces.
- 1280 to 1560 for Layer 3 Ethernet interfaces.
- 1280 to 64000 for tunnel interfaces.

Usage guidelines

IPv6 routers do not support packet fragmentation. After an IPv6 router receives an IPv6 packet, if the packet size is greater than the MTU of the forwarding interface, the router discards the packet. Meanwhile, the router sends the MTU to the source host through an ICMPv6 packet — Packet Too Big message. The source host fragments the packet according to the MTU and resends it. To reduce the extra flow overhead resulting from packet drops, set an appropriate interface MTU for your network.

Examples

Set the MTU of IPv6 packets sent over VLAN-interface 100 to 1280 bytes.

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ipv6 mtu 1280
```

11.1.25. ipv6 nd autoconfig managed-address-flag

Use **ipv6 nd autoconfig managed-address-flag** to set the managed address configuration flag (M) to 1 in RA advertisements to be sent.

Use **undo ipv6 nd autoconfig managed-address-flag** to restore the default.

Syntax

ipv6 nd autoconfig managed-address-flag

undo ipv6 nd autoconfig managed-address-flag

Default

The M flag is set to **0** in RA advertisements. Hosts receiving the advertisements will obtain IPv6 addresses through stateless autoconfiguration.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

The M flag in RA advertisements determines whether receiving hosts use stateful autoconfiguration to obtain IPv6 addresses.

- If the M flag is set to 1 in RA advertisements, receiving hosts use stateful autoconfiguration (for example, from an DHCPv6 server) to obtain IPv6 addresses.
- If the M flag is set to 0 in RA advertisements, receiving hosts use stateless autoconfiguration. Stateless autoconfiguration generates IPv6 addresses according to link-layer addresses and the prefix information in the RA advertisements.

Examples

Set the M flag to 1 in RA advertisements to be sent.

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ipv6 nd autoconfig managed-address-flag
```

11.1.26. ipv6 nd autoconfig other-flag

Use **ipv6 nd autoconfig other-flag** to set the other stateful configuration flag (O) to 1 in RA advertisements to be sent.

Use **undo ipv6 nd autoconfig other-flag** to restore the default.

Syntax

ipv6 nd autoconfig other-flag

undo ipv6 nd autoconfig other-flag

Default

The O flag is set to **0** in RA advertisements. Hosts receiving the advertisements will acquire other information through stateless autoconfiguration.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

The O flag in RA advertisements determines whether receiving hosts use stateful autoconfiguration to obtain configuration information other than IPv6 addresses.

- If the O flag is set to 1 in RA advertisements, receiving hosts use stateful autoconfiguration (for example, from a DHCPv6 server) to obtain configuration information other than IPv6 addresses.
- If the O flag is set to 0 in RA advertisements, receiving hosts use stateless autoconfiguration to obtain configuration information other than IPv6 addresses.

Examples

Set the O flag to 0 in RA advertisements to be sent.

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] undo ipv6 nd autoconfig other-flag
```

11.1.27. ipv6 nd dad attempts

Use **ipv6 nd dad attempts** to set the number of attempts to send an NS message for DAD.

Use **undo ipv6 nd dad attempts** to restore the default.

Syntax

ipv6 nd dad attempts *interval*

undo ipv6 nd dad attempts

Default

The number of attempts to send an NS message for DAD is 1.

Views

Interface view

Predefined user roles

network-admin

Parameters

interval: Specifies the number of attempts to send an NS message for DAD, in the range of 0 to 600. If it is set to 0, DAD is disabled.

Usage guidelines

An interface sends an NS message for DAD after obtaining an IPv6 address.

If the interface does not receive a response within the time specified by using **ipv6 nd ns retrans-timer**, it resends an NS message.

If the interface receives no response after making the maximum sending attempts (set by using **ipv6 nd dad attempts**), the interface uses the obtained address.

Examples

Set the number of attempts to send an NS message for DAD to 20.

```
<Switch> system-view
[Switch] interface vlan-interface 100
```

```
[Switch-Vlan-interface100] ipv6 nd dad attempts 20
```

Related commands

display ipv6 interface

ipv6 nd ns retrans-timer

11.1.28. ipv6 nd ns retrans-timer

Use **ipv6 nd ns retrans-timer** to set the interval for retransmitting an NS message.

Use **undo ipv6 nd ns retrans-timer** to restore the default.

Syntax

ipv6 nd ns retrans-timer *value*

undo ipv6 nd ns retrans-timer

Default

The local interface sends NS messages at every an interval of 1000 milliseconds, and the Retrans Timer field in the RA messages sent is 0. The interval for retransmitting an NS message is determined by the receiving device.

Views

Interface view

Predefined user roles

network-admin

Parameters

value: Specifies the interval value in the range of 1000 to 4294967295 milliseconds.

Usage guidelines

If a device does not receive a response from the peer within the specified interval, the device resends an NS message. The device retransmits an NS message at the specified interval and uses the interval value to fill the Retrans Timer field in RA messages to be sent.

Examples

Specify VLAN-interface 100 to retransmit NS messages every 10000 milliseconds.

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ipv6 nd ns retrans-timer 10000
```

Related commands

display ipv6 interface

11.1.29. ipv6 nd nud reachable-time

Use **ipv6 nd nud reachable-time** to set the neighbor reachable time on an interface.

Use **undo ipv6 nd nud reachable-time** to restore the default.

Syntax

ipv6 nd nud reachable-time *time*

undo ipv6 nd nud reachable-time

Default

The neighbor reachable time on the local interface is 30000 milliseconds, and the value of the Reachable Time field in RA messages is 0. The reachable time is determined by the receiving device.

Views

Interface view

Predefined user roles

network-admin

Parameters

time: Specifies the neighbor reachable time in the range of 1 to 3600000 milliseconds.

Usage guidelines

If the neighbor reachability detection shows that a neighbor is reachable, the device considers the neighbor reachable within the specified reachable time. If the device must send a packet to the neighbor after the specified reachable time expires, the device reconfirms whether the neighbor is reachable. The device sets the specified value as the neighbor reachable time on the local interface and uses the value to fill the Reachable Time field in RA messages to be sent.

Examples

Set the neighbor reachable time on VLAN-interface 100 to 10000 milliseconds.

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ipv6 nd nud reachable-time 10000
```

Related commands

display ipv6 interface

11.1.30. ipv6 nd ra halt

Use **ipv6 nd ra halt** to suppress an interface from advertising RA messages.

Use **undo ipv6 nd ra halt** to disable this feature.

Syntax

ipv6 nd ra halt

undo ipv6 nd ra halt

Default

An interface is suppressed from sending RA messages.

Views

Interface view

Predefined user roles

network-admin

Examples

Disable RA message suppression on VLAN-interface 100.

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] undo ipv6 nd ra halt
```

11.1.31. ipv6 nd ra interval

Use **ipv6 nd ra interval** to set the maximum and minimum intervals for advertising RA messages.

Use **undo ipv6 nd ra interval** to restore the default.

Syntax

ipv6 nd ra interval *max-interval min-interval*

undo ipv6 nd ra interval

Default

The maximum interval between RA messages is 600 seconds, and the minimum interval is 200 seconds.

Views

Interface view

Predefined user roles

network-admin

Parameters

max-interval: Specifies the maximum interval value in seconds, in the range of 4 to 1800.

min-interval: Specifies the minimum interval value in the range of 3 seconds to three-fourths of the maximum interval.

Usage guidelines

The device advertises RA messages randomly between the maximum interval and the minimum interval.

The maximum interval for sending RA messages should be less than or equal to the router lifetime in RA messages.

Examples

Set the maximum interval for advertising RA messages to 1000 seconds and the minimum interval to 700 seconds.

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ipv6 nd ra interval 1000 700
```

Related commands

ipv6 nd ra router-lifetime

11.1.32. ipv6 nd ra prefix

Use **ipv6 nd ra prefix** to configure the prefix information in RA messages.

Use **undo ipv6 nd ra prefix** to restore the default.

Syntax

ipv6 nd ra prefix { *ipv6-prefix prefix-length* | *ipv6-prefix*/*prefix-length* } [*valid-lifetime preferred-lifetime* [**no-autoconfig** | **off-link**] *]

undo ipv6 nd ra prefix { *ipv6-prefix* | *ipv6-prefix*/*prefix-length* }

Default

No prefix information is configured for RA messages. Instead, the IPv6 address of the interface sending RA messages is used as the prefix information.

If the IPv6 address is manually configured, the prefix uses the fixed valid lifetime 2592000 seconds (30 days) and preferred lifetime 604800 seconds (7 days).

If the IPv6 address is automatically obtained (through DHCP, for example), the prefix uses the valid and preferred lifetime of the IPv6 address.

Views

Interface view

Predefined user roles

network-admin

Parameters

ipv6-prefix: Specifies the IPv6 prefix.

prefix-length: Specifies the prefix length of the IPv6 address.

valid-lifetime: Specifies the valid lifetime of a prefix, in the range of 0 to 4294967295 seconds. The default value is 2592000 seconds (30 days).

preferred-lifetime: Specifies the preferred lifetime of a prefix used for stateless autoconfiguration, in the range of 0 to 4294967295 seconds. The preferred lifetime cannot be longer than the valid lifetime. The default value is 604800 seconds (7 days).

no-autoconfig: Specifies a prefix not to be used for stateless autoconfiguration. If you do not specify this keyword, the prefix is used for stateless autoconfiguration.

off-link: Indicates that the address with the prefix is not directly reachable on the link. If you do not specify this keyword, the address with the prefix is directly reachable on the link.

Usage guidelines

After hosts on the same link receive RA messages, they can use the prefix information in the RA messages for stateless autoconfiguration.

The prefix uses the following settings:

- Valid lifetime of 2592000 seconds (30 days).
- Preferred lifetime of 604800 seconds (7 days).
- The prefix is used for stateless autoconfiguration.
- The address with the prefix is directly reachable on the link.

Examples

Configure the prefix information in RA messages on VLAN-interface 100.

Method 1:

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ipv6 nd ra prefix 2001:10::100/64 100 10
```

Method 2:

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ipv6 nd ra prefix 2001:10::100 64 100 10
```

11.1.33. ipv6 nd ra router-lifetime

Use **ipv6 nd ra router-lifetime** to set the router lifetime in RA messages.

Use **undo ipv6 nd ra router-lifetime** to restore the default.

Syntax

ipv6 nd ra router-lifetime *time*

undo ipv6 nd ra router-lifetime

Default

The router lifetime in RA messages is 1800 seconds.

Views

Interface view

Predefined user roles

network-admin

Parameters

time: Specifies the router lifetime in the range of 0 to 9000 seconds. If the value is set to 0, the router does not act as the default router.

Usage guidelines

The router lifetime in RA messages specifies how long the router sending the RA messages acts as the default router. Hosts receiving the RA messages check this value to determine whether to use the sending router as the default router. If the router lifetime is 0, the router cannot be used as the default router.

The router lifetime in RA messages must be greater than or equal to the advertising interval.

Examples

Set the router lifetime in RA messages on VLAN-interface 100 to 1000 seconds.

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ipv6 nd ra router-lifetime 1000
```

Related commands

ipv6 nd ra interval

11.1.34. ipv6 neighbor

Use **ipv6 neighbor** to configure a static neighbor entry.

Use **undo ipv6 neighbor** to delete a static neighbor entry.

Syntax

ipv6 neighbor *ipv6-address mac-address* { *vlan-id port-type port-number* | **interface** *interface-type interface-number* } [**vpn-instance** *vpn-instance-name*]

undo ipv6 neighbor *ipv6-address interface-type interface-number*

Default

No static neighbor entries exist.

Views

System view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies the IPv6 address of the static neighbor entry.

mac-address: Specifies the MAC address (48 bits) of the static neighbor entry, in the format of H-H-H.

vlan-id: Specifies the VLAN ID of the static neighbor entry, in the range of 1 to 4094.

port-type port-number: Specifies a Layer 2 port of the static neighbor entry by its type and number.

interface *interface-type interface-number*: Specifies a Layer 3 interface of the static neighbor entry by its type and number.

vpn-instance *vpn-instance-name*: Specifies a VPN instance to which the static neighbor entry belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command configures a static neighbor entry for the public network.

Usage guidelines

A neighbor entry stores information about a link-local node. The entry can be created dynamically through NS and NA messages, or configured statically.

The device uniquely identifies a static neighbor entry by using the neighbor's IPv6 address and the number of the Layer 3 interface that connects to the neighbor. You can configure a static neighbor entry by using either of the following methods:

- **Method 1**—Associate a neighbor IPv6 address and link-layer address with the Layer 3 interface of the local node.
- **Method 2**—Associate a neighbor IPv6 address and link-layer address with a Layer 2 port in a VLAN containing the local node.

You can use either of the previous configuration methods to configure a static neighbor entry for a VLAN interface.

- If Method 1 is used, the neighbor entry is in INCMP state. After the device obtains the corresponding Layer 2 port information, the neighbor entry goes into REACH state.
- If Method 2 is used, the port specified by *port-type port-number* must belong to the VLAN specified by *vlan-id* and the corresponding VLAN interface must already exist. After the static neighbor entry is configured, the device associates the VLAN interface with the IPv6 address to uniquely identify the static neighbor entry. The entry will be in REACH state.

To delete a static neighbor entry for a VLAN interface, specify only the corresponding VLAN interface.

Examples

Configure a static neighbor entry for VLAN-interface 1.

```
<Switch> system-view
[Switch] ipv6 neighbor 2000::1 fe-e0-89 interface Vlan-interface 1
```

Related commands

display ipv6 neighbors

reset ipv6 neighbors

11.1.35. ipv6 neighbor stale-aging

Use **ipv6 neighbor stale-aging** to set the aging timer for ND entries in stale state.

Use **undo ipv6 neighbor stale-aging** to restore the default.

Syntax

ipv6 neighbor stale-aging *aging-time*

undo ipv6 neighbor stale-aging

Default

The aging timer for ND entries in stale state is 240 minutes.

Views

System view

Predefined user roles

network-admin

Parameters

aging-time: Specifies the aging timer for ND entries in stale state, in the range of 1 to 1440 minutes.

Usage guidelines

This aging time applies to all ND entries in stale state. If an ND entry in stale state is not updated before the timer expires, it moves to the delay state. If it is still not updated in 5 seconds, the ND entry moves to the probe state. The device sends an NS message for detection a maximum of three times. If no response is received, the device deletes the ND entry.

Examples

Set the aging timer for ND entries in stale state to 120 minutes.

```
<Switch> system-view
[Switch] ipv6 neighbor stale-aging 120
```

11.1.36. ipv6 neighbors max-learning-num

Use **ipv6 neighbors max-learning-num** to set the maximum number of dynamic neighbor entries that an interface can learn. This prevents the interface from occupying too many neighbor table resources.

Use **undo ipv6 neighbors max-learning-num** to restore the default.

Syntax

ipv6 neighbors max-learning-num *max-number*

undo ipv6 neighbors max-learning-num

Default

An interface can learn a maximum of 7680 dynamic neighbor entries.

Views

Layer 2/Layer 3 interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

max-number: Specifies the maximum number of dynamic neighbor entries that an interface can learn. The value range for this argument is 1 to 7680.

Usage guidelines

The device can dynamically acquire the link-layer address of a neighboring node through NS and NA messages and add it into the neighbor table.

When the number of dynamic neighbor entries reaches the threshold, the interface stops learning neighbor information.

Examples

Set the maximum number of dynamic neighbor entries that VLAN-interface 100 can learn to 10.

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ipv6 neighbors max-learning-num 10
```

11.1.37. ipv6 pathmtu

Use **ipv6 pathmtu** to set a static Path MTU for an IPv6 address.

Use **undo ipv6 pathmtu** to delete the Path MTU configuration for an IPv6 address.

Syntax

ipv6 pathmtu [**vpn-instance** *vpn-instance-name*] *ipv6-address value*

undo ipv6 pathmtu [**vpn-instance** *vpn-instance-name*] *ipv6-address*

Default

No static Path MTU is set.

Views

System view

Predefined user roles

network-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies a VPN instance to which the Path MTU belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command sets the Path MTU for the public network.

ipv6-address: Specifies an IPv6 address.

value: Specifies the Path MTU of the specified IPv6 address, in the range of 1280 to 10240 bytes.

Usage guidelines

You can set a static Path MTU for a destination IPv6 address. When a source host sends a packet through an interface, it compares the interface MTU with the static Path MTU of the specified destination IPv6 address. If the packet size is larger than the smaller one of the two values, the host fragments the packet according to the smaller value.

Examples

Set a static Path MTU for an IPv6 address.

```
<Switch> system-view
[Switch] ipv6 pathmtu fe80::12 1300
```

Related commands

display ipv6 pathmtu

reset ipv6 pathmtu

11.1.38. ipv6 pathmtu age

Use **ipv6 pathmtu age** to set the aging time for a dynamic Path MTU.

Use **undo ipv6 pathmtu age** to restore the default.

Syntax

ipv6 pathmtu age *age-time*

undo ipv6 pathmtu age

Default

The aging time for dynamic Path MTU is 10 minutes.

Views

System view

Predefined user roles

network-admin

Parameters

age-time: Specifies the aging time for Path MTU in minutes, in the range of 10 to 100.

Usage guidelines

After the path MTU from a source host to a destination host is dynamically determined, the source host sends subsequent packets to the destination host based on this MTU. After the aging time expires, the following events occur:

- The dynamic Path MTU is removed.
- The source host determines a dynamic path MTU through the Path MTU mechanism again.

The aging time is invalid for a static Path MTU.

Examples

Set the aging time for a dynamic Path MTU to 40 minutes.

```
<Switch> system-view
[Switch] ipv6 pathmtu age 40
```

Related commands

display ipv6 pathmtu

11.1.39. ipv6 unreachables enable

Use **ipv6 unreachables enable** to enable sending ICMPv6 destination unreachable messages.

Use **undo ipv6 unreachables** to disable sending ICMPv6 destination unreachable messages.

Syntax

ipv6 unreachables enable

undo ipv6 unreachables enable

Default

Sending ICMPv6 destination unreachable messages is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

If the device fails to forward a received IPv6 packet because of a destination unreachable error, it performs the following operations:

- Drops the packet.
- Sends an ICMPv6 destination unreachable message to the source.

If the device is generating ICMPv6 destination unreachable messages incorrectly, disable sending ICMPv6 destination unreachable messages to prevent attack risks.

Examples

Enable sending ICMPv6 destination unreachable messages.

```
<Switch> system-view
[Switch] ipv6 unreachables enable
```

11.1.40. local-proxy-nd enable

Use **local-proxy-nd enable** to enable local ND proxy.

Use **undo local-proxy-nd enable** to disable local ND proxy.

Syntax

local-proxy-nd enable

undo local-proxy-nd enable

Default

Local ND proxy is disabled.

Views

VLAN interface view

Layer 3 Ethernet interface view

Predefined user roles

network-admin

Examples

Enable local ND proxy on VLAN-interface 100.

```
<Switch> system-view
[Switch] interface vlan-interface 100
```

```
[Switch-Vlan-interface100] local-proxy-nd enable
```

11.1.41. reset ipv6 neighbors

Use **reset ipv6 neighbors** to clear IPv6 neighbor information.

Syntax

reset ipv6 neighbors { **all** | **dynamic** | **interface** *interface-type interface-number* | **slot** *slot-number* | **static** }

Views

User view

Predefined user roles

network-admin

Parameters

all: Clears static and dynamic neighbor information for all interfaces.

dynamic: Clears dynamic neighbor information for all interfaces.

interface *interface-type interface-number*: Clears dynamic neighbor information for the interface specified by its type and number.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears dynamic neighbor information for all member devices.

static: Clears static neighbor information for all interfaces.

Examples

Clear neighbor information for all interfaces.

```
<Switch> reset ipv6 neighbors all
This will delete all the entries. Continue? [Y/N]:Y
```

Clear dynamic neighbor information for all interfaces.

```
<Switch> reset ipv6 neighbors dynamic
This will delete all the dynamic entries. Continue? [Y/N]:Y
```

Clear all neighbor information for GigabitEthernet 1/0/1.

```
<Switch> reset ipv6 neighbors interface gigabitethernet 1/0/1
This will delete all the dynamic entries by the interface you specified. Continue? [Y/N]:Y
```

Related commands

display ipv6 neighbors

ipv6 neighbor

11.1.42. reset ipv6 pathmtu

Use **reset ipv6 pathmtu** to clear the Path MTU information.

Syntax

reset ipv6 pathmtu { **all** | **dynamic** | **static** }

Views

User view

Predefined user roles

network-admin

Parameters

all: Clears all Path MTUs.

dynamic: Clears all dynamic Path MTUs.

static: Clears all static Path MTUs.

Examples

Clear all Path MTUs.

```
<Switch> reset ipv6 pathmtu all
```

Related commands

display ipv6 pathmtu

11.1.43. reset ipv6 statistics

Use **reset ipv6 statistics** to clear IPv6 and ICMPv6 packet statistics.

Syntax

reset ipv6 statistics [**slot** *slot-number*]

Views

User view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears IPv6 and ICMPv6 packet statistics for all member devices.

Examples

Clear IPv6 and ICMPv6 packet statistics.

```
<Switch> reset ipv6 statistics
```

Related commands

display ipv6 statistics

Contents

A page of this section is **4-x-x**

12. Tunneling commands 12-1
12.1. Tunneling commands 12-1
12.1.1. description 12-1
12.1.2. destination 12-1
12.1.3. display interface tunnel 12-2
12.1.4. interface tunnel 12-6
12.1.5. mtu 12-7
12.1.6. reset counters interface tunnel 12-7
12.1.7. shutdown 12-8
12.1.8. source 12-9
12.1.9. tunnel vpn-instance 12-10

12. Tunneling commands

12.1. Tunneling commands

12.1.1. description

Use **description** to configure the description of an interface.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

The description of a tunnel interface is **Tunnel***number* **Interface**, for example, **Tunnel1 Interface**.

Views

Tunnel interface view

Predefined user roles

network-admin

Parameters

text: Specifies a description, a case-sensitive string of 1 to 255 characters.

Usage guidelines

Configure descriptions for different interfaces for identification and management purposes.

You can use the **display interface** command to display the configured interface description.

Examples

Configure the description of Tunnel 1 as **tunnel1**.

```
<Switch> system-view
[Switch] interface tunnel 1
[Switch-Tunnel1] description tunnel1
```

Related commands

display interface tunnel

12.1.2. destination

Use **destination** to specify the destination address for a tunnel interface.

Use **undo destination** to restore the default.

Syntax

destination { *ipv4-address* | *ipv6-address* }

undo destination

Default

No tunnel destination address is configured.

Views

Tunnel interface view

Predefined user roles

network-admin

Parameters

ipv4-address: Specifies the tunnel destination IPv4 address.

ipv6-address: Specifies the tunnel destination IPv6 address.

Usage guidelines

The tunnel destination address must be the address of the receiving interface on the tunnel peer. It is used as the destination address of tunneled packets.

The destination address of the local tunnel interface must be the source address of the peer tunnel interface. The source address of the local tunnel interface must be the destination address of the peer tunnel interface.

Do not specify the same tunnel source and destination addresses for the tunnel interfaces on the same device.

Examples

VLAN-interface 100 on Switch1 uses the IP address 193.101.1.1 and VLAN-interface 100 on Switch2 uses the IP address 192.100.1.1. Configure the source address 193.101.1.1 and destination address 192.100.1.1 for the tunnel interface on Switch1.

```
<Switch1> system-view
[Switch1] interface tunnel 1 mode ipv6-ipv4
[Switch1-Tunnel1] source 193.101.1.1
[Switch1-Tunnel1] destination 192.100.1.1
```

Configure the source address 192.100.1.1 and destination address 193.101.1.1 for the tunnel interface on Switch2.

```
<Switch2> system-view
[Switch2] interface tunnel 1 mode ipv6-ipv4
[Switch2-Tunnel1] source 192.100.1.1
[Switch2-Tunnel1] destination 193.101.1.1
```

Related commands

display interface tunnel

interface tunnel

source

12.1.3. display interface tunnel

Use **display interface tunnel** to display tunnel interface information.

Syntax

display interface [**tunnel** [*number*]] [**brief** [**description** | **down**]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

tunnel [*number*]: Specifies a tunnel interface. The *number* argument specifies the tunnel interface number. The specified tunnel interface must have been created. If you do not specify the **tunnel** keyword, this command displays information about all interfaces on the device. If you specify the **tunnel** keyword without the *number* argument, this command displays information about all existing tunnel interfaces.

brief: Displays brief interface information. If you do not specify this keyword, the command displays detailed interface information.

description: Displays complete interface descriptions. If you do not specify this keyword, the command displays only the first 27 characters of interface descriptions.

down: Displays information about interfaces in the physical state of DOWN and the causes. If you do not specify this keyword, the command displays information about interfaces in all states.

Examples

Display detailed IPv4 information about Tunnel 1.

```
<Switch> display interface tunnel 1
Tunnel1
Current state: UP
Line protocol state: UP
Description: Tunnel1 Interface
Bandwidth: 64kbps
Maximum transmission unit: 1476
Internet address: 10.1.2.1/24 (primary)
Tunnel source 2002::1:1 (Vlan-interface10), destination 2001::2:1
Tunnel TTL 255
Tunnel protocol/transport GRE/IPv6
    GRE key disabled
    Checksumming of GRE packets disabled
Last clearing of counters: Never
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops
```

Table 12-1 Command output

Field	Description
Tunnel1	Information about the tunnel interface Tunnel 1.
Current state	Physical link state of the tunnel interface: • **Administratively DOWN**—The interface has been shut down by using the **shutdown** command. • **DOWN**—The interface is administratively up, but its physical state is down (possibly because no physical

Field	Description
	link exists or the link has failed). • **UP**—The interface is both administratively and physically up.
Line protocol state	Data link layer state of the interface. The state is determined through automatic parameter negotiation at the data link layer. • **UP**—The data link layer protocol is up. • **UP (spoofing)**—The data link layer protocol is up, but the link is an on-demand link or does not exist. This attribute is typical of null interfaces and loopback interfaces. • **DOWN**—The data link layer protocol is down.
Description	Description of the tunnel interface.
Bandwidth	Expected bandwidth of the tunnel interface.
Maximum transmission unit	MTU of the tunnel interface.
Internet protocol processing: Disabled	The tunnel interface is not assigned an IP address and cannot process IP packets.
Internet address	IP address of the tunnel interface. The **primary** attribute indicates that the address is the primary IP address.
Tunnel source	Source address of the tunnel. If a source interface is specified for the tunnel interface, this field also displays the source interface in parentheses.
destination	Destination address of the tunnel.
Tunnel TTL	TTL of tunneled packets.
Tunnel protocol/transport	Tunnel mode and transport protocol: • **GRE/IP**—GRE/IPv4 tunnel mode. • **GRE/IPv6**—GRE/IPv6 tunnel mode. • **IP/IP**—IPv4 over IPv4 tunnel mode. • **IP/IPv6**—IPv4 over IPv6 tunnel mode. • **IPv6/IP**—IPv6 over IPv4 tunnel mode. • **IPv6/IPv6**—IPv6 over IPv6 tunnel mode. • **UDP_VXLAN/IP**—UDP-encapsulated IPv4 VXLAN tunnel mode.
GRE key disabled	No GRE tunnel interface key is configured.
Checksumming of GRE packets disabled	The GRE packet checksum feature is disabled.
Last clearing of counters	Last time when counters were cleared.
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec	Average input rate in the last 300 seconds.
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec	Average output rate in the last 300 seconds.
Input: 0 packets, 0 bytes, 0 drops	Total input packets, total input bytes, and total input packets dropped. Input packets are counted after they are de-encapsulated by software.

Field	Description
Output: 0 packets, 0 bytes, 0 drops	Total output packets, total output bytes, and total output packets dropped. Output packets are counted before they are encapsulated by software.

Display brief information about Tunnel 1.

```
<Switch> display interface tunnel 1 brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Primary IP     Description
Tun1                 UP   UP       1.1.1.1        aaaaaaaaaaaaaaaaaaaaaaaaaaa
```

Display brief information about Tunnel 1, including the complete interface description.

```
<Switch> display interface tunnel 1 brief description
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Primary IP     Description
Tun1                 UP    UP      1.1.1.1        aaaaaaaaaaaaaaaaaaaaaaaaaaaaa
Aaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

Table 12-2 Command output

Field	Description
Interface	Abbreviated interface name.
Link	Physical link state of the interface: • **UP**—The interface is physically up. • **DOWN**—The interface is physically down. • **ADM**—The interface has been shut down by using the **shutdown** command. To restore the physical state of the interface, use the **undo shutdown** command. • **Stby**—The interface is a backup interface in standby state.
Protocol	Data link layer protocol state of the interface: • **UP**—The data link layer protocol of the interface is up. • **DOWN**—The data link layer protocol of the interface is down. • **UP(s)**—The data link layer protocol of the interface is up, but the link is an on-demand link or does not exist. The **(s)** attribute represents the spoofing flag. This value is typical of null interfaces and loopback interfaces.
Primary IP	Primary IP address of the interface. This field displays two hyphens (**--**) if the interface does not have an IP address.
Description	Description of the interface.
Cause	Cause for the physical link state of an interface to be **DOWN**: • **Administratively**—The interface has been manually shut down by using the **shutdown** command. To restore the physical state of the interface, use the **undo shutdown** command.

Field	Description
	• **Not connected**—The tunnel is not established.

Related commands

destination

interface tunnel

source

12.1.4. interface tunnel

Use **interface tunnel** to create a tunnel interface, specify the tunnel mode, and enter tunnel interface view, or enter the view of an existing tunnel interface.

Use **undo interface tunnel** to delete a tunnel interface.

Syntax

interface tunnel *number* [**mode** { **gre** [**ipv6**] | **ipv4-ipv4** | **ipv4-ipv6** | **ipv6-ipv4** | **ipv6-ipv6** | **vxlan** }]

undo interface tunnel *number*

Default

No tunnel interfaces exist.

Views

System view

Predefined user roles

network-admin

Parameters

number: Specifies the number of the tunnel interface. The value range is 0 to 8.

mode gre: Specifies the GRE/IPv4 tunnel mode.

mode gre ipv6: Specifies the GRE/IPv6 tunnel mode.

mode ipv4-ipv4: Specifies the IPv4 over IPv4 tunnel mode.

mode ipv4-ipv6: Specifies the IPv4 over IPv6 tunnel mode.

mode ipv6-ipv4: Specifies the IPv6 over IPv4 tunnel mode.

mode ipv6-ipv6: Specifies the IPv6 over IPv6 tunnel mode.

mode vxlan: Specifies the VXLAN tunnel mode.

Usage guidelines

To create a new tunnel interface, you must specify the tunnel mode in this command. To enter the view of an existing tunnel interface, you do not need to specify the tunnel mode.

A tunnel interface number is locally significant. The tunnel interfaces on the two ends of a tunnel can use the same or different interface numbers.

Examples

Create GRE/IPv4 tunnel interface Tunnel 1 and enter tunnel interface view.

```
<Switch> system-view
```

```
[Switch] interface tunnel 1 mode gre
[Switch-Tunnel1]
```

Related commands

destination

display interface tunnel

source

12.1.5. mtu

Use **mtu** to set the MTU on a tunnel interface.

Use **undo mtu** to restore the default.

Syntax

mtu *size*

undo mtu

Default

If the tunnel interface has never been up, the MTU is 64000 bytes.

If the tunnel interface is up, its MTU is identical to the outgoing interface's MTU minus the length of the tunnel headers. The outgoing interface is automatically obtained through routing table lookup based on the tunnel destination address.

Views

Tunnel interface view

Predefined user roles

network-admin

Parameters

size: Specifies the MTU, in the range of 100 to 64000 bytes.

Usage guidelines

After you configure an MTU for a tunnel interface, the configured MTU applies regardless of the tunnel interface status (up/down) and the outgoing interface MTU.

To avoid fragmentation after tunnel encapsulation, set the tunnel interface MTU no greater than the value of the outgoing interface MTU minus the length of the tunnel headers.

Examples

Set the MTU on Tunnel 1 to 10000 bytes.

```
<Switch> system-view
[Switch] interface tunnel 1
[Switch-Tunnel1] mtu 10000
```

Related commands

display interface tunnel

12.1.6. reset counters interface tunnel

Use **reset counters interface tunnel** to clear tunnel interface statistics.

Syntax

reset counters interface [**tunnel** [*number*]]

Views

User view

Predefined user roles

network-admin

Parameters

tunnel [*number*]: Specifies a tunnel interface. The *number* argument specifies the tunnel interface number. If you do not specify the **tunnel** keyword, this command clears statistics for all interfaces. If you specify the **tunnel** keyword without the *number* argument, this command clears statistics for all tunnel interfaces.

Usage guidelines

Use this command to clear old statistics so you can observe new traffic statistics on a tunnel interface.

Examples

Clear statistics for Tunnel 1.

```
<Switch> reset counters interface tunnel 1
```

Related commands

display interface tunnel

12.1.7. shutdown

Use **shutdown** to shut down a tunnel interface.

Use **undo shutdown** to bring up a tunnel interface.

Syntax

shutdown

undo shutdown

Default

A tunnel interface is down.

Views

Tunnel interface view

Predefined user roles

network-admin

Usage guidelines

This command disconnects all links set up on the interface. Make sure you fully understand the impact of the command on your network.

Examples

Shut down Tunnel 1.

```
<Switch> system-view
[Switch] interface tunnel 1
[Switch-Tunnel1] shutdown
```

Related commands

display interface tunnel

12.1.8. source

Use **source** to specify the source address or source interface for a tunnel interface.

Use **undo source** to restore the default.

Syntax

source { *ipv4-address* | *ipv6-address* | *interface-type interface-number* }

undo source

Default

No source address or source interface is specified for a tunnel interface.

Views

Tunnel interface view

Predefined user roles

network-admin

Parameters

ipv4-address: Specifies the tunnel source IPv4 address.

ipv6-address: Specifies the tunnel source IPv6 address.

interface-type interface-number: Specifies the source interface by its type and number. The interface must be up and must have an IP address.

Usage guidelines

The specified source address or the address of the specified source interface is used as the source address of tunneled packets. To display the configured tunnel source address, use the **display interface tunnel** command.

The destination address of the local tunnel interface must be the source address of the peer tunnel interface. The source address of the local tunnel interface must be the destination address of the peer tunnel interface.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify VLAN-interface 10 as the source interface of Tunnel 1.

```
<Switch> system-view
[Switch] interface tunnel 1 mode gre
[Switch-Tunnel1] source vlan-interface 10
```

Specify 192.100.1.1 as the source address of Tunnel 1.

```
<Switch> system-view
[Switch] interface tunnel 1 mode gre
[Switch-Tunnel1] source 192.100.1.1
```

Related commands

destination

display interface tunnel

interface tunnel

12.1.9. tunnel vpn-instance

Use **tunnel vpn-instance** to specify a VPN instance for the destination address of a tunnel interface.

Use **undo tunnel vpn-instance** to restore the default.

Syntax

tunnel vpn-instance *vpn-instance-name*

undo tunnel vpn-instance

Default

No VPN instance for the destination address of a tunnel interface.

Views

Tunnel interface view

Predefined user roles

network-admin

Parameters

vpn-instance-name: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

After this command is executed, the device looks up the routing table of the specified VPN instance to forward tunneled packets on the tunnel interface.

For a tunnel interface to come up, the tunnel source and destination must belong to the same VPN instance. To specify a VPN instance for the tunnel source, use the ip binding vpn-instance command on the tunnel source interface.

Examples

Specify VPN instance **vpn10** for the tunnel destination on Tunnel 1.

```
<Switch> system-view
[Switch] ip vpn-instance vpn10
[Switch-vpn-instance-vpn10] route-distinguisher 1:1
[Switch-vpn-instance-vpn10] vpn-target 1:1
[Switch-vpn-instance-vpn10] quit
[Switch] interface tunnel 1 mode vxlan
[Switch-Tunnel1] source 2.2.2.2
[Switch-Tunnel1] destination 1.1.1.1
[Switch-Tunnel1] tunnel vpn-instance vpn10
```

NOTE:

The **tunnel vpn-instance** command is supported on Ver7.4.45 and later.

Contents

A page of this section is **4-x-x**

13. HTTP redirect commands 13-1
13.1. HTTP redirect commands 13-1
13.1.1. http-redirect https-port 13-1
13.1.2. http-redirect ssl-server-policy 13-1

13. HTTP redirect commands

13.1. HTTP redirect commands

13.1.1. http-redirect https-port

Use **http-redirect https-port** to specify the HTTPS redirect listening port number.

Use **undo http-redirect https-port** to disable.

Syntax

http-redirect https-port *port-number*

undo http-redirect https-port

Default

HTTPS redirect listening port number is 8443.

Views

System view

Predefined user roles

network-admin

Parameters

port-number: Specifies the TCP port number on which the HTTPS redirect service listens for HTTPS requests. The value range for the port number is 1 to 65535.

Usage guidelines

To avoid service unavailability caused by port conflict, do not specify a TCP port number used by a well-known protocol or used by any other service. To display TCP port numbers that have been used by services, use the **display tcp** command.

If you execute this command multiple times, the most recent configuration takes effect.

Using **undo http-redirect https-port** redirects to port 6654. You must use the **http-redirect https-port 8443** command to reconfigure the HTTPS redirect listening port number.

If you set **undo http-redirect https-port** command, QX does not redirect user HTTPS requests to the Web authentication. NEC recommends that you do not change this setting to disable.

Examples

Specify 8888 as the HTTPS redirect listening port number.

```
<Switch> system-view
[Switch] http-redirect https-port 8888
```

13.1.2. http-redirect ssl-server-policy

Use **http-redirect ssl-server-policy** to associate an SSL server policy with the HTTPS redirect service.

Use **undo http-redirect ssl-server-policy** to restore the default.

Syntax

http-redirect ssl-server-policy *policy-name*

undo http-redirect ssl-server-policy

Default

No SSL server policy is associated with the HTTPS redirect service. The HTTPS redirect service uses a self-assigned certificate and the default SSL parameters.

Views

System view

Predefined user roles

network-admin

Parameters

policy-name: Specifies an SSL server policy by its name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

HTTPS redirect is unavailable if the associated SSL server policy does not exist. You can first associate a nonexistent SSL server policy with the HTTPS redirect service and then configure the SSL server policy.

If you change the SSL server policy associated with the HTTPS redirect service, the new policy takes effect immediately.

If you perform this task multiple times, the most recent configuration takes effect.

Examples

Associate SSL server policy **policy1** with the HTTPS redirect service.

```
<Switch> system-view
[Switch] http-redirect ssl-server-policy policy1
```

Related commands

ssl server-policy

Contents

A page of this section is **4-x-x**

14. ARP direct route advertisement commands ····· 14-1
14.1. ARP direct route advertisement commands ····· 14-1
14.1.1. arp route-direct advertise ····· 14-1

14. ARP direct route advertisement commands

14.1. ARP direct route advertisement commands

14.1.1. arp route-direct advertise

Use **arp route-direct advertise** to enable ARP direct route advertisement.

Use **undo arp route-direct advertise** to disable ARP direct route advertisement.

Syntax

arp route-direct advertise

undo arp route-direct advertise

Default

ARP direct route advertisement is disabled.

Views

Layer 3 Ethernet interface view

Layer 3 Ethernet subinterface view

VLAN interface view

Predefined user roles

network-admin

Examples

Enable ARP direct route advertisement on Layer 3 Ethernet interface GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] arp route-direct advertise
```

QX-S5600G Series Ethernet Switches

Command References

5.Layer 3 - IP Routing

This manual is including the following chapters.

01-Basic IP routing commands

02-Static routing commands

03-RIP commands

04-OSPF commands

05-BGP commands

06-Policy-based routing commands

07-IPv6 static routing commands

08-RIPng commands

09-OSPFv3 commands

10-IPv6 policy-based routing commands

11-Routing policy commands

Contents

A page of this section is **5-x-x**

1. Basic IP routing commands ····· 1-1
1.1. Basic IP routing commands ····· 1-1
1.1.1. address-family ipv4 ····· 1-1
1.1.2. address-family ipv6 ····· 1-1
1.1.3. display ip routing-table ····· 1-2
1.1.4. display ip routing-table acl ····· 1-8
1.1.5. display ip routing-table *ip-address* ····· 1-10
1.1.6. display ip routing-table prefix-list ····· 1-13
1.1.7. display ip routing-table protocol ····· 1-14
1.1.8. display ip routing-table statistics ····· 1-16
1.1.9. display ipv6 rib graceful-restart ····· 1-18
1.1.10. display ipv6 routing-table ····· 1-19
1.1.11. display ipv6 routing-table acl ····· 1-24
1.1.12. display ipv6 routing-table *ipv6-address* ····· 1-28
1.1.13. display ipv6 routing-table prefix-list ····· 1-31
1.1.14. display ipv6 routing-table protocol ····· 1-32
1.1.15. display max-ecmp-num ····· 1-34
1.1.16. display ipv6 routing-table statistics ····· 1-35
1.1.17. display rib graceful-restart ····· 1-37
1.1.18. ip route fast-switchover enable ····· 1-39
1.1.19. ipv6 route fast-switchover enable ····· 1-40
1.1.20. max-ecmp-num ····· 1-40
1.1.21. non-stop-routing ····· 1-41
1.1.22. protocol lifetime ····· 1-42
1.1.23. reset ip routing-table statistics protocol ····· 1-42
1.1.24. reset ipv6 routing-table statistics protocol ····· 1-43
1.1.25. rib ····· 1-43
1.1.26. routing-table limit ····· 1-44

1. Basic IP routing commands

1.1. Basic IP routing commands

1.1.1. address-family ipv4

Use **address-family ipv4** to create the RIB IPv4 address family and enter its view, or enter the view of the existing RIB IPv4 address family.

Use **undo address-family ipv4** to delete the RIB IPv4 address family and all configurations in the view.

Syntax

address-family ipv4

undo address-family ipv4

Default

No RIB IPv4 address family exists.

Views

RIB view

Predefined user roles

network-admin

Examples

Create the RIB IPv4 address family and enter its view.

```
<Switch> system-view
[Switch] rib
[Switch-rib] address-family ipv4
[Switch-rib-ipv4]
```

1.1.2. address-family ipv6

Use **address-family ipv6** to create the RIB IPv6 address family and enter its view, or enter the view of the existing RIB IPv6 address family.

Use **undo address-family ipv6** to delete the RIB IPv6 address family and all configurations in the view.

Syntax

address-family ipv6

undo address-family ipv6

Default

No RIB IPv6 address family exists.

Views

RIB view

Predefined user roles

network-admin

Examples

Create the RIB IPv6 address family and enter its view.

```
<Switch> system-view
[Switch] rib
[Switch-rib] address-family ipv6
[Switch-rib-ipv6]
```

1.1.3. display ip routing-table

Use **display ip routing-table** to display routing table information.

Syntax

display ip routing-table [**vpn-instance** *vpn-instance-name*] [**verbose**]

display ip routing-table [**all-routes**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters.

all-routes: Displays routing table information for the public network and all VPN instances.

verbose: Displays detailed routing table information, including information about both active and inactive routes. If you do not specify this keyword, the command displays only brief information about active routes.

Usage guidelines

If you do not specify any parameters, the command displays routing table information for the public network.

Examples

Display brief information about active routes in the routing table.

```
<Switch> display ip routing-table

Destinations : 12        Routes : 12

Destination/Mask    Proto   Pre  Cost         NextHop         Interface
0.0.0.0/32          Direct  0    0            127.0.0.1       InLoop0
127.0.0.0/8         Direct  0    0            127.0.0.1       InLoop0
127.0.0.0/32        Direct  0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct  0    0            127.0.0.1       InLoop0
127.255.255.255/32  Direct  0    0            127.0.0.1       InLoop0
192.168.1.0/24      Direct  0    0            192.168.1.40    Vlan11
```

```
192.168.1.0/32      Direct 0    0           192.168.1.40    Vlan11
192.168.1.40/32     Direct 0    0           127.0.0.1       InLoop0
192.168.1.255/32    Direct 0    0           192.168.1.40    Vlan11
224.0.0.0/4         Direct 0    0           0.0.0.0         NULL0
224.0.0.0/24        Direct 0    0           0.0.0.0         NULL0
255.255.255.255/32  Direct 0    0           127.0.0.1       InLoop0
```

Display brief information about active routes in the routing table for the public network and all VPN instances.

```
<Switch> display ip routing-table all-routes

VPN instance: public instance
Destinations : 10        Routes : 10

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
0.0.0.0/32          Direct 0    0           127.0.0.1       InLoop0
1.1.1.0/24          Static 60   0           192.168.47.4    Vlan11
127.0.0.0/8         Direct 0    0           127.0.0.1       InLoop0
127.0.0.0/32        Direct 0    0           127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0           127.0.0.1       InLoop0
127.255.255.255/32  Direct 0    0           127.0.0.1       InLoop0
192.168.1.40/32     Direct 0    0           127.0.0.1       InLoop0
224.0.0.0/4         Direct 0    0           0.0.0.0         NULL0
224.0.0.0/24        Direct 0    0           0.0.0.0         NULL0
255.255.255.255/32  Direct 0    0           127.0.0.1       InLoop0

VPN instance: vpn1
Destinations : 10        Routes : 10

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
0.0.0.0/32          Direct 0    0           127.0.0.1       InLoop0
1.1.2.0/24          Static 60   0           2.2.1.1         Vlan11
3.3.1.0/24          BGP    255  0           55.1.1.2        Vlan12
127.0.0.0/8         Direct 0    0           127.0.0.1       InLoop0
127.0.0.0/32        Direct 0    0           127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0           127.0.0.1       InLoop0
127.255.255.255/32  Direct 0    0           127.0.0.1       InLoop0
224.0.0.0/4         Direct 0    0           0.0.0.0         NULL0
224.0.0.0/24        Direct 0    0           0.0.0.0         NULL0
255.255.255.255/32  Direct 0    0           127.0.0.1       InLoop0
```

Display information about IPv4 routes for all VPN instances.

```
<Switch> display ip routing-table all-vpn-instance

VPN instance: vpn1
Destinations : 10        Routes : 10

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
0.0.0.0/32          Direct 0    0           127.0.0.1       InLoop0
```

```
1.1.2.0/24          Static 60   0            2.2.1.1         Vlan11
3.3.1.0/24          BGP    255  0            55.1.1.2        Vlan12
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.0/32        Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
127.255.255.255/32  Direct 0    0            127.0.0.1       InLoop0
224.0.0.0/4         Direct 0    0            0.0.0.0         NULL0
224.0.0.0/24        Direct 0    0            0.0.0.0         NULL0
255.255.255.255/32  Direct 0    0            127.0.0.1       InLoop0

VPN instance: vpn2
Destinations : 9        Routes : 9

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
0.0.0.0/32          Direct 0    0            127.0.0.1       InLoop0
1.1.3.0/24          Static 60   0            3.3.1.1         Vlan13
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.0/32        Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
127.255.255.255/32  Direct 0    0            127.0.0.1       InLoop0
224.0.0.0/4         Direct 0    0            0.0.0.0         NULL0
224.0.0.0/24        Direct 0    0            0.0.0.0         NULL0
255.255.255.255/32  Direct 0    0            127.0.0.1       InLoop0
```

Table 1-1 Command output

Field	Description
VPN instance	Public network or VPN instance that the routing table belongs to. For the public network, this field displays **public instance**. For a VPN instance, this field displays the VPN instance name.
Destinations	Number of destination addresses.
Routes	Number of routes.
Destination/Mask	Destination address/mask length.
Proto	Protocol that installed the route.
Pre	Preference of the route.
Cost	Cost of the route.
NextHop	Next hop address of the route.
Interface	Output interface for packets to be forwarded along the route.
Summary count	Number of routes.

Display detailed information about all routes in the routing table.

```
<Switch> display ip routing-table verbose

Destinations : 2        Routes : 2

Destination: 0.0.0.0/32
   Protocol: Direct
```

```
 Process ID: 0
  SubProtID: 0x0                    Age: 08h34m37s
       Cost: 0                Preference: 0
      IpPre: N/A              QosLocalID: N/A
        Tag: 0                     State: Active NoAdv
  OrigTblID: 0x0                OrigVrf: default-vrf
    TableID: 0x2                 OrigAs: 0
      NibID: 0x10000000          LastAs: 0
     AttrID: 0xffffffff        Neighbor: 0.0.0.0
      Flags: 0x1000c         OrigNextHop: 127.0.0.1
      Label: NULL            RealNextHop: 127.0.0.1
    BkLabel: NULL              BkNextHop: N/A
  Tunnel ID: Invalid           Interface: InLoopBack0
BkTunnel ID: Invalid         BkInterface: N/A
   FtnIndex: 0x0            TrafficIndex: N/A
  Connector: N/A

Destination: 1.1.1.0/24
   Protocol: Static
 Process ID: 0
  SubProtID: 0x0                    Age: 04h20m37s
       Cost: 0                Preference: 60
      IpPre: N/A              QosLocalID: N/A
        Tag: 0                     State: Active Adv
  OrigTblID: 0x0                OrigVrf: default-vrf
    TableID: 0x2                 OrigAs: 0
      NibID: 0x10000003          LastAs: 0
     AttrID: 0xffffffff        Neighbor: 0.0.0.0
      Flags: 0x1008c         OrigNextHop: 192.168.47.4
      Label: NULL            RealNextHop: 192.168.47.4
    BkLabel: NULL              BkNextHop: N/A
  Tunnel ID: Invalid           Interface: Vlan-interface11
BkTunnel ID: Invalid         BkInterface: N/A
   FtnIndex: 0x0            TrafficIndex: N/A
  Connector: N/A
```

Display detailed information about all routes in the routing table for all VPN instances.

```
<Switch> display ip routing-table all-vpn-instance verbose

VPN instance: vpn1
Destinations : 1        Routes : 1

Destination: 0.0.0.0/32
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x0                    Age: 08h34m37s
       Cost: 0                Preference: 0
      IpPre: N/A              QosLocalID: N/A
```

```
        Tag: 0                    State: Active NoAdv
  OrigTblID: 0x0                OrigVrf: vpn1
    TableID: 0x2                 OrigAs: 0
      NibID: 0x10000000          LastAs: 0
     AttrID: 0xffffffff        Neighbor: 0.0.0.0
      Flags: 0x1000c        OrigNextHop: 127.0.0.1
      Label: NULL           RealNextHop: 127.0.0.1
    BkLabel: NULL             BkNextHop: N/A
  Tunnel ID: Invalid          Interface: InLoopBack0
BkTunnel ID: Invalid        BkInterface: N/A
   FtnIndex: 0x0            TrafficIndex: N/A
  Connector: N/A

VPN instance: vpn2
Destinations : 1        Routes : 1

Destination: 1.1.1.0/24
   Protocol: Static
 Process ID: 0
  SubProtID: 0x0                  Age: 04h20m37s
       Cost: 0              Preference: 60
      IpPre: N/A            QosLocalID: N/A
        Tag: 0                  State: Active Adv
  OrigTblID: 0x0               OrigVrf: vpn2
    TableID: 0x2                OrigAs: 0
      NibID: 0x10000003         LastAs: 0
     AttrID: 0xffffffff       Neighbor: 0.0.0.0
      Flags: 0x1008c        OrigNextHop: 192.168.47.4
      Label: NULL           RealNextHop: 192.168.47.4
    BkLabel: NULL             BkNextHop: N/A
  Tunnel ID: Invalid          Interface: Vlan-interface11
BkTunnel ID: Invalid        BkInterface: N/A
   FtnIndex: 0x0            TrafficIndex: N/A
  Connector: N/A
```

Table 1-2 Command output

Field	Description
VPN instance	Public network or VPN instance that the routing table belongs to. For the public network, this field displays **public instance**. For a VPN instance, this field displays the VPN instance name.
Destinations	Number of destination addresses.
Routes	Number of routes.
Destination	Destination address/mask length.
Protocol	Protocol that installed the route.
SubProtID	ID of the subprotocol for routing.
Age	Time for which the route has been in the routing table.

Field	Description
Cost	Cost of the route.
Preference	Preference of the route.
IpPre	IP precedence.
QosLocalID	This field is not supported in the current software version. Local QoS ID.
Tag	Route tag.
State	Route status: • **Active**—Active unicast route. • **Adv**—Route that can be advertised. • **Inactive**—Inactive route. • **NoAdv**—Route that the router must not advertise. • **Vrrp**—Routes generated by VRRP. • **Nat**—Routes generated by NAT. • **TunE**—Tunnel.
OrigTblID	Original routing table ID.
OrigVrf	Original VPN instance that the route belongs to. This field displays **default-vrf** if the route is on the IPv4 public network.
TableID	ID of the routing table.
OrigAs	Original AS number.
NibID	ID of the next hop.
LastAs	Last AS number.
AttrID	Attribute ID.
Neighbor	Address of the neighbor determined by the routing protocol.
Flags	Flags of the route.
OrigNextHop	Next hop address of the route.
RealNextHop	Real next hop of the route.
BkLabel	Backup label.
BkNexthop	Backup next hop.
Tunnel ID	Tunnel ID.
Interface	Output interface for packets to be forwarded along the route.
BkTunnel ID	Backup tunnel ID.
BkInterface	Backup output interface.
FtnIndex	Index of the FTN entry.
TrafficIndex	Traffic index in the range of 1 to 64. This field displays **N/A** when the value is invalid.
Connector	BGP connector attribute exchanged between BGP peers along with a VPN IPv4 route. The value of the attribute is the IP address of the remote PE device. The BGP connector attribute is used for MD VPN. This field displays **N/A** if the BGP connector attribute is not supported.
Summary count	Number of routes.

1.1.4. display ip routing-table acl

Use **display ip routing-table acl** to display information about routes permitted by a basic ACL.

Syntax

display ip routing-table [**vpn-instance** *vpn-instance-name*] **acl** *ipv4-acl-number* [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command displays routing information for the public network.

ipv4-acl-number: Specifies a basic ACL by its number in the range of 2000 to 2999.

verbose: Displays detailed information about all routes permitted by the basic ACL. If you do not specify this keyword, the command displays only brief information about active routes permitted by the basic ACL.

Usage guidelines

If the specified ACL does not exist or has no rules configured, the command displays information about all routes.

Examples

Define basic ACL 2000 and set the route filtering rules.

```
<Switch> system-view
[Switch] acl basic 2000
[Switch-acl-ipv4-basic-2000] rule permit source 192.168.1.0 0.0.0.255
[Switch-acl-ipv4-basic-2000] rule deny source any
```

Display brief information about active routes permitted by basic ACL 2000.

```
[Switch-acl-ipv4-basic-2000] display ip routing-table acl 2000

Summary count : 4

Destination/Mask    Proto   Pre  Cost         NextHop         Interface
192.168.1.0/24      Direct  0    0            192.168.1.111   Vlan11
192.168.1.0/32      Direct  0    0            192.168.1.111   Vlan11
192.168.1.111/32    Direct  0    0            127.0.0.1       InLoop0
192.168.1.255/32    Direct  0    0            192.168.1.111   Vlan11
```

For command output, see Table 1-1 .

Display detailed information about all routes permitted by basic ACL 2000.

```
<Switch> display ip routing-table acl 2000 verbose
```

```
Summary count : 4

Destination: 192.168.1.0/24
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x1                    Age: 04h20m37s
       Cost: 0                Preference: 0
      IpPre: N/A              QosLocalID: N/A
        Tag: 0                     State: Active Adv
  OrigTblID: 0x0                OrigVrf: default-vrf
    TableID: 0x2                 OrigAs: 0
      NibID: 0x10000003          LastAs: 0
     AttrID: 0xffffffff        Neighbor: 0.0.0.0
      Flags: 0x10080        OrigNextHop: 192.168.1.111
      Label: NULL           RealNextHop: 192.168.1.111
    BkLabel: NULL             BkNextHop: N/A
  Tunnel ID: Invalid          Interface: Vlan-interface11
BkTunnel ID: Invalid        BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A

Destination: 192.168.1.0/32
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x0                    Age: 04h20m37s
       Cost: 0                Preference: 0
      IpPre: N/A              QosLocalID: N/A
        Tag: 0                     State: Active NoAdv
  OrigTblID: 0x0                OrigVrf: default-vrf
    TableID: 0x2                 OrigAs: 0
      NibID: 0x10000003          LastAs: 0
     AttrID: 0xffffffff        Neighbor: 0.0.0.0
      Flags: 0x1008c        OrigNextHop: 192.168.1.111
      Label: NULL           RealNextHop: 192.168.1.111
    BkLabel: NULL             BkNextHop: N/A
  Tunnel ID: Invalid          Interface: Vlan-interface11
BkTunnel ID: Invalid        BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A

Destination: 192.168.1.111/32
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x1                    Age: 04h20m37s
       Cost: 0                Preference: 0
      IpPre: N/A              QosLocalID: N/A
        Tag: 0                     State: Active NoAdv
  OrigTblID: 0x0                OrigVrf: default-vrf
```

```
    TableID: 0x2                OrigAs: 0
      NibID: 0x10000000         LastAs: 0
     AttrID: 0xffffffff       Neighbor: 0.0.0.0
      Flags: 0x10004       OrigNextHop: 127.0.0.1
      Label: NULL          RealNextHop: 127.0.0.1
    BkLabel: NULL            BkNextHop: N/A
  Tunnel ID: Invalid           Interface: InLoopBack0
BkTunnel ID: Invalid       BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A

Destination: 192.168.1.255/32
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x0                   Age: 04h20m37s
       Cost: 0               Preference: 0
      IpPre: N/A             QosLocalID: N/A
        Tag: 0                    State: Active NoAdv
  OrigTblID: 0x0               OrigVrf: default-vrf
    TableID: 0x2                OrigAs: 0
      NibID: 0x10000003         LastAs: 0
     AttrID: 0xffffffff       Neighbor: 0.0.0.0
      Flags: 0x1008c       OrigNextHop: 192.168.1.111
      Label: NULL          RealNextHop: 192.168.1.111
    BkLabel: NULL            BkNextHop: N/A
  Tunnel ID: Invalid           Interface: Vlan-interface11
BkTunnel ID: Invalid       BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A
```

For command output, see Table 1-2 .

1.1.5. display ip routing-table *ip-address*

Use **display ip routing-table** *ip-address* to display information about routes to a specific destination address.

Use **display ip routing-table** *ip-address1* **to** *ip-address2* to display information about routes to a range of destination addresses.

Syntax

display ip routing-table [**vpn-instance** *vpn-instance-name*] *ip-address* [*mask-length* | *mask*] [**longer-match**] [**verbose**]

display ip routing-table [**vpn-instance** *vpn-instance-name*] *ip-address1* **to** *ip-address2* [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command displays routing information for the public network.

ip-address: Specifies a destination IP address in dotted decimal notation.

mask-length: Specifies the mask length, an integer in the range of 0 to 32.

mask: Specifies the IP address mask in dotted decimal notation.

longer-match: Displays the route entry with the longest mask.

ip-address1 **to** *ip-address2*: Specifies a destination IP address range.

verbose: Displays detailed routing table information, including information about both active and inactive routes. If you do not specify this keyword, the command displays brief information about active routes.

Usage guidelines

Executing the command with different parameters yields different outputs.

- **display ip routing-table** *ip-address*
  - The system ANDs the entered destination IP address with the subnet mask in each active route entry.
  - The system ANDs the destination IP address in each active route entry with its own subnet mask.

  If the two operations yield the same result for an entry, the entry is displayed.
- **display ip routing-table** *ip-address mask*
  - The system ANDs the entered destination IP address with the entered subnet mask.
  - The system ANDs the destination IP address in each active route entry with the entered subnet mask.

  If the two operations yield the same result for an entry with a subnet mask not greater than the entered subnet mask, the entry is displayed.
- **display ip routing-table** *ip-address* **longer-match**
  - The system ANDs the entered destination IP address with the subnet mask in each active route entry.
  - The system ANDs the destination IP address in each active route entry with its own subnet mask.

  If the two operations yield the same result for multiple entries, the entry with the longest mask length is displayed.
- **display ip routing-table** *ip-address mask* **longer-match**
  - The system ANDs the entered destination IP address with the entered subnet mask.
  - The system ANDs the destination IP address in each active route entry with the entered subnet mask.

  If the two operations yield the same result for multiple entries with a mask not greater than the entered subnet mask, the entry with the longest mask length is displayed.
- **display ip routing-table** *ip-address1* **to** *ip-address2*

  The system displays active route entries with destinations in the range of *ip-address1*/32 to *ip-address2*/32.

Examples

Display brief information about the routes to the destination IP address 11.0.0.1.

```
<Switch> display ip routing-table 11.0.0.1

Summary count : 3

Destination/Mask    Proto   Pre  Cost         NextHop         Interface
11.0.0.0/8          Static  60   0            0.0.0.0         NULL0
11.0.0.0/16         Static  60   0            0.0.0.0         NULL0
11.0.0.0/24         Static  60   0            0.0.0.0         NULL0
```

Display brief information about the routes to the destination IP address 11.0.0.1 and mask length 20.

```
<Switch> display ip routing-table 11.0.0.1 20

Summary count : 2

Destination/Mask    Proto   Pre  Cost         NextHop         Interface
11.0.0.0/8          Static  60   0            0.0.0.0         NULL0
11.0.0.0/16         Static  60   0            0.0.0.0         NULL0
```

Display brief information about the most specific route to the destination address 11.0.0.1.

```
<Switch> display ip routing-table 11.0.0.1 longer-match

Summary count : 1

Destination/Mask    Proto   Pre  Cost         NextHop         Interface
11.0.0.0/24         Static  60   0            0.0.0.0         NULL0
```

Display brief information about the most specific route to the destination IP address 11.0.0.1 and mask length 20.

```
<Switch> display ip routing-table 11.0.0.1 20 longer-match

Summary count : 1

Destination/Mask    Proto   Pre  Cost         NextHop         Interface
11.0.0.0/16         Static  60   0            0.0.0.0         NULL0
```

Display brief information about the routes to destination addresses in the range of 1.1.1.0 to 5.5.5.0.

```
<Switch> display ip routing-table 1.1.1.0 to 5.5.5.0

Summary count : 4

Destination/Mask    Proto   Pre  Cost         NextHop         Interface
1.1.1.1/32          Direct  0    0            127.0.0.1       InLoop0
2.2.2.0/24          Direct  0    0            2.2.2.1         Vlan2
3.3.3.1/32          Direct  0    0            127.0.0.1       InLoop0
4.4.4.1/32          Direct  0    0            127.0.0.1       InLoop0
```

Display detailed information about the routes to the destination IP address 1.2.3.4.

```
<Switch> display ip routing-table 1.2.3.4 verbose
```

```
Summary count : 1

Destination: 1.2.3.4/32
   Protocol: BGP instance test
 Process ID: 0
  SubProtID: 0x1                    Age: 00h00m37s
       Cost: 0                Preference: 255
      IpPre: N/A              QosLocalID: N/A
        Tag: 0                     State: Active Adv
  OrigTblID: 0x0                OrigVrf: default-vrf
    TableID: 0x2                 OrigAs: 200
      NibID: 0x15000000          LastAs: 200
     AttrID: 0x0                Neighbor: 192.168.47.2
      Flags: 0x10060         OrigNextHop: 192.168.47.2
      Label: NULL            RealNextHop: 192.168.47.2
    BkLabel: NULL              BkNextHop: N/A
  Tunnel ID: Invalid           Interface: Vlan-interface11
BkTunnel ID: Invalid         BkInterface: N/A
   FtnIndex: 0x0            TrafficIndex: N/A
  Connector: N/A
```

For command output, see Table 1-1 .

1.1.6. display ip routing-table prefix-list

Use **display ip routing-table prefix-list** to display routes permitted by an IP prefix list.

Syntax

display ip routing-table [**vpn-instance** *vpn-instance-name*] **prefix-list** *prefix-list-name* [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command displays routing information for the public network.

prefix-list-name: Specifies an IP prefix list by its name, a case-sensitive string of 1 to 63 characters.

verbose: Displays detailed information about all routes permitted by the IP prefix list. If you do not specify this keyword, the command displays brief information about active routes permitted by the IP prefix list.

Usage guidelines

If the specified IP prefix list does not exist, the command displays information about all routes.

Examples

Create an IP prefix list named **test** to permit the route 1.1.1.0/24.

```
<Switch> system-view
[Switch] ip prefix-list test permit 1.1.1.0 24
```

Display brief information about the active route permitted by the IP prefix list.

```
[Switch] display ip routing-table prefix-list test

Summary count : 1

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
1.1.1.0/24          Direct 0    0            1.1.1.2         Vlan11
```

For command output, see Table 1-1 .

Display detailed information about all routes permitted by the IP prefix list.

```
[Switch] display ip routing-table prefix-list test verbose

Summary count : 1

Destination: 1.1.1.0/24
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x1                  Age: 04h20m37s
       Cost: 0               Preference: 0
      IpPre: N/A             QosLocalID: N/A
        Tag: 0                    State: Active Adv
  OrigTblID: 0x0                OrigVrf: default-vrf
    TableID: 0x2                 OrigAs: 0
      NibID: 0x10000003          LastAs: 0
     AttrID: 0xffffffff        Neighbor: 0.0.0.0
      Flags: 0x1008c        OrigNextHop: 1.1.1.2
      Label: NULL           RealNextHop: 1.1.1.2
    BkLabel: NULL             BkNextHop: N/A
  Tunnel ID: Invalid            Interface: Vlan-interface11
BkTunnel ID: Invalid         BkInterface: N/A
   FtnIndex: 0x0            TrafficIndex: N/A
  Connector: N/A
```

For command output, see Table 1-2 .

1.1.7. display ip routing-table protocol

Use **display ip routing-table protocol** to display information about routes installed by a protocol.

Syntax

display ip routing-table [**vpn-instance** *vpn-instance-name*] **protocol** *protocol* [**inactive** | **verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command displays routing information for the public network.

protocol: Specifies a routing protocol.

inactive: Displays information about inactive routes. If you do not specify this keyword, the command displays information about both active and inactive routes.

verbose: Displays detailed routing table information. If you do not specify this keyword, the command displays brief routing information.

Examples

Display brief information about direct routes.

```
<Switch> display ip routing-table protocol direct

Summary count : 9

Direct Routing Table Status : <Active>
Summary count : 9

Destination/Mask    Proto   Pre  Cost         NextHop         Interface
0.0.0.0/32          Direct  0    0            127.0.0.1       InLoop0
2.2.2.0/24          Direct  0    0            2.2.2.1         Vlan2
2.2.2.0/32          Direct  0    0            2.2.2.1         Vlan2
2.2.2.2/32          Direct  0    0            127.0.0.1       InLoop0
2.2.2.255/32        Direct  0    0            2.2.2.1         Vlan2
127.0.0.0/8         Direct  0    0            127.0.0.1       InLoop0
127.0.0.0/32        Direct  0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct  0    0            127.0.0.1       InLoop0
127.255.255.255/32  Direct  0    0            127.0.0.1       InLoop0

Direct Routing Table Status : <Inactive>
Summary count : 0
```

Display brief information about static routes.

```
<Switch> display ip routing-table protocol static

Summary count : 1

Static Routing Table Status : <Active>
Summary count : 0

Static Routing Table Status : <Inactive>
```

```
Summary count : 1

Destination/Mask    Proto   Pre  Cost         NextHop         Interface
1.2.3.0/24          Static  60   0            1.2.4.5         Vlan10
```

Display detailed information about BGP routes.

```
<Switch> display ip routing-table protocol bgp verbose

Summary count : 1

Destination: 1.1.1.2/32
   Protocol: BGP instance default
 Process ID: 0
  SubProtID: 0x6                  Age: 00h03m54s
       Cost: 0              Preference: 255
      IpPre: N/A            QosLocalID: N/A
        Tag: 0                   State: Active Adv
  OrigTblID: 0x0               OrigVrf: default-vrf
    TableID: 0x2                OrigAs: 200
      NibID: 0x16000000         LastAs: 200
     AttrID: 0x0              Neighbor: 192.168.47.2
      Flags: 0x10060       OrigNextHop: 192.168.47.2
      Label: NULL          RealNextHop: 192.168.47.2
    BkLabel: NULL            BkNextHop: N/A
  Tunnel ID: Invalid          Interface: Vlan-interface11
BkTunnel ID: Invalid       BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A
```

For command output, see Table 1-1 .

1.1.8. display ip routing-table statistics

Use **display ip routing-table statistics** to display IPv4 route statistics, including numbers of total routes, routes installed by the protocol, routes marked as deleted, and active routes.

Syntax

display ip routing-table [**all-routes** | **all-vpn-instance** | **vpn-instance** *vpn-instance-name*] **statistics**

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

all-routes: Displays IPv4 route statistics for the public network and all VPN instances.

all-vpn-instance: Specifies all VPN instances.

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

If you do not specify any parameters, the command displays IPv4 route statistics for the public network.

Examples

Display IPv4 route statistics for the public network.

```
<Switch> display ip routing-table statistics

Total prefixes: 15        Active prefixes: 15

Proto       route       active      added       deleted
DIRECT      12          12          30          18
STATIC      3           3           5           2
RIP         0           0           0           0
OSPF        0           0           0           0
IS-IS       0           0           0           0
BGP         0           0           0           0
Total       15          15          35          20
```

Display IPv4 route statistics for the public network and all VPN instances.

```
<Switch> display ip routing-table all-routes statistics

VPN instance: public instance
Total prefixes: 11        Active prefixes: 11

Proto       route       active      added       deleted
DIRECT      8           8           8           0
STATIC      3           3           5           2
RIP         0           0           0           0
OSPF        0           0           0           0
IS-IS       0           0           0           0
LISP        0           0           0           0
BGP         0           0           0           0
Total       11          11          13          2

VPN instance: vpn1
Total prefixes: 20        Active prefixes: 20

Proto       route       active      added       deleted
DIRECT      8           8           8           0
STATIC      0           0           0           0
RIP         0           0           0           0
OSPF        0           0           0           0
IS-IS       0           0           0           0
LISP        0           0           0           0
BGP         12          12          12          0
Total       20          20          20          0
```

Display IPv4 route statistics for all VPN instances.

```
<Switch> display ip routing-table all-vpn-instance statistics

VPN instance: vpn1
Total prefixes: 11        Active prefixes: 11

Proto       route       active      added       deleted
DIRECT      8           8           8           0
STATIC      3           3           5           2
RIP         0           0           0           0
OSPF        0           0           0           0
IS-IS       0           0           0           0
LISP        0           0           0           0
BGP         0           0           0           0
Total       11          11          13          2

VPN instance: vpn2
Total prefixes: 8         Active prefixes: 8

Proto       route       active      added       deleted
DIRECT      8           8           8           0
STATIC      0           0           0           0
RIP         0           0           0           0
OSPF        0           0           0           0
IS-IS       0           0           0           0
LISP        0           0           0           0
BGP         0           0           0           0
Total       8           8           8           0
```

Table 1-3 Command output

Field	Description
VPN instance	Public network or VPN instance that the routing table belongs to. For the public network, this field displays **public instance**. For a VPN instance, this field displays the VPN instance name.
Proto	Protocol that installed the route.
route	Number of routes installed by the protocol.
active	Number of active routes.
added	Number of routes added to the routing table after the router started up or the routing table was cleared most recently.
deleted	Number of routes marked as deleted, which will be cleared after a period.
Total	Total number of routes.

1.1.9. display ipv6 rib graceful-restart

Use **display ipv6 rib graceful-restart** to display IPv6 RIB GR state information.

Syntax

display ipv6 rib graceful-restart

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display IPv6 RIB GR state information.

```
<Switch> display ipv6 rib graceful-restart
RIB GR state     : Phase2-calculation end
RCOM GR state    : Flush end
Protocol GR state:
 No.  Protocol   Lifetime FD   State    Start/End
-------------------------------------------------
 1    DIRECT6    480      29   End      No/No
 2    STATIC6    480      32   End      No/No
 3    ISISV6     480      30   End      No/No
 4    BGP4+ instance default
                 480      31   End      No/No
 5    BGP4+ instance ebcdefg
                 480      32   End      No/No
```

For command output, see Table 1-8 .

1.1.10. display ipv6 routing-table

Use **display ipv6 routing-table** to display IPv6 routing table information.

Syntax

display ipv6 routing-table [**all-vpn-instance** | **vpn-instance** *vpn-instance-name*] [**verbose**]

display ipv6 routing-table [**all-routes**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

all-vpn-instance: Specifies all VPN instances.

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters.

all-routes: Displays IPv6 routing table information for the public network and all VPN instances.

verbose: Displays detailed routing table information, including information about both active and inactive routes. If you do not specify this keyword, the command displays only brief information about active routes.

Usage guidelines

If you do not specify any parameters, the command displays IPv6 routing table information for the public network.

Examples

Display brief information about active routes in the IPv6 routing table.

```
<Switch> display ipv6 routing-table

Destinations : 2 Routes : 2

Destination: ::1/128                                Protocol  : Direct
NextHop    : ::1                                    Preference: 0
Interface  : InLoop0                                Cost      : 0

Destination: FE80::/10                              Protocol  : Direct
NextHop    : ::                                     Preference: 0
Interface  : InLoop0                                Cost      : 0
```

Display brief information about active routes in the IPv6 routing table for the public network and all VPN instances.

```
<Switch> display ipv6 routing-table all-routes

VPN instance: public instance
Destinations : 2 Routes : 2

Destination: ::1/128                                Protocol  : Direct
NextHop    : ::1                                    Preference: 0
Interface  : InLoop0                                Cost      : 0

Destination: FE80::/10                              Protocol  : Direct
NextHop    : ::                                     Preference: 0
Interface  : InLoop0                                Cost      : 0

VPN instance: vpn1
Destinations : 2 Routes : 2

Destination: ::1/128                                Protocol  : Direct
NextHop    : ::1                                    Preference: 0
Interface  : InLoop0                                Cost      : 0

Destination: 1:2::3:4/128                           Protocol  : Static
NextHop    : ::                                     Preference: 60
Interface  : NULL0                                  Cost      : 0
```

Display IPv6 routing table information for all VPN instances.

```
<Switch> display ipv6 routing-table all-vpn-instance
```

```
VPN instance: vpn1
Destinations : 2 Routes : 2

Destination: ::1/128                                    Protocol   : Direct
NextHop    : ::1                                        Preference: 0
Interface  : InLoop0                                    Cost       : 0

Destination: 1:2::3:4/128                               Protocol   : Static
NextHop    : ::                                         Preference: 60
Interface  : NULL0                                      Cost       : 0

VPN instance: vpn2
Destinations : 1 Routes : 1

Destination: ::1/128                                    Protocol   : Direct
NextHop    : ::1                                        Preference: 0
Interface  : InLoop0                                    Cost       : 0
```

Table 1-4 Command output

Field	Description
VPN instance	Public network or VPN instance that the IPv6 routing table belongs to. For the public network, this field displays **public instance**. For a VPN instance, this field displays the VPN instance name.
Destinations	Number of destination addresses.
Routes	Number of routes.
Destination	IPv6 address and prefix of the destination network or host.
NextHop	Next hop address of the route.
Preference	Preference of the route.
Interface	Output interface for packets to be forwarded along the route.
Protocol	Protocol that installed the route.
Cost	Cost of the route.
Summary count	Number of routes.

Display detailed information about all routes in the IPv6 routing table.

```
<Switch> display ipv6 routing-table verbose

Destinations : 2 Routes : 2

Destination: ::1/128
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x0                    Age: 19h23m02s
       Cost: 0                Preference: 0
      IpPre: N/A              QosLocalID: N/A
        Tag: 0                     State: Active NoAdv
```

```
  OrigTblID: 0x0               OrigVrf: default-vrf
    TableID: 0xa                OrigAs: 0
      NibID: 0x20000000         LastAs: 0
     AttrID: 0xffffffff       Neighbor: ::
      Flags: 0x10004       OrigNextHop: ::1
      Label: NULL          RealNextHop: ::1
    BkLabel: NULL            BkNextHop: N/A
  Tunnel ID: Invalid          Interface: InLoopBack0
BkTunnel ID: Invalid       BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A

Destination: 12::/96
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x0                  Age: 00h01m47s
       Cost: 0              Preference: 0
      IpPre: N/A            QosLocalID: N/A
        Tag: 0                   State: Active Adv
  OrigTblID: 0x0               OrigVrf: default-vrf
    TableID: 0xa                OrigAs: 0
      NibID: 0x20000003         LastAs: 0
     AttrID: 0xffffffff       Neighbor: ::
      Flags: 0x10080       OrigNextHop: ::
      Label: NULL          RealNextHop: ::
    BkLabel: NULL            BkNextHop: N/A
  Tunnel ID: Invalid          Interface: Vlan-interface11
BkTunnel ID: Invalid       BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A
```

Display detailed information about all routes in the IPv6 routing table for all VPN instances.

```
<Switch> display ipv6 routing-table all-vpn-instance verbose

VPN instance: vpn1
Destinations : 2 Routes : 2

Destination: ::1/128
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x0                  Age: 19h23m02s
       Cost: 0              Preference: 0
      IpPre: N/A            QosLocalID: N/A
        Tag: 0                   State: Active NoAdv
  OrigTblID: 0x0               OrigVrf: default-vrf
    TableID: 0xa                OrigAs: 0
      NibID: 0x20000000         LastAs: 0
     AttrID: 0xffffffff       Neighbor: ::
```

```
      Flags: 0x10004        OrigNextHop: ::1
      Label: NULL           RealNextHop: ::1
    BkLabel: NULL             BkNextHop: N/A
  Tunnel ID: Invalid          Interface: InLoopBack0
BkTunnel ID: Invalid        BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A

Destination: 12::1/128
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x0                  Age: 00h01m45s
       Cost: 0              Preference: 0
      IpPre: N/A            QosLocalID: N/A
        Tag: 0                   State: Active NoAdv
  OrigTblID: 0x0               OrigVrf: default-vrf
    TableID: 0xa                OrigAs: 0
      NibID: 0x20000000         LastAs: 0
     AttrID: 0xffffffff       Neighbor: ::
      Flags: 0x10004        OrigNextHop: ::1
      Label: NULL           RealNextHop: ::1
    BkLabel: NULL             BkNextHop: N/A
  Tunnel ID: Invalid          Interface: Vlan-interface11
BkTunnel ID: Invalid        BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A
```

Table 1-5 Command output

Field	Description
VPN instance	Public network or VPN instance that the routing table belongs to. For the public network, this field displays **public instance**. For a VPN instance, this field displays the VPN instance name.
Destination	IPv6 address and prefix of the destination network or host.
Protocol	Protocol that installed the route.
SubProtID	ID of the subprotocol for routing.
Age	Time for which the route has been in the routing table.
Cost	Cost of the route.
Preference	Preference of the route.
IpPre	IP precedence.
QosLocalID	This field is not supported in the current software version. Local QoS ID.
Tag	Tag of the route.
State	Route status: • **Active**—Active unicast route. • **Adv**—Route that can be advertised.

Field	Description
	• **Inactive**—Inactive route. • **NoAdv**—Route that the router must not advertise. • **Vrrp**—Routes generated by VRRP. • **Nat**—Routes generated by NAT. • **TunE**—Tunnel.
OrigTblID	Original routing table ID.
OrigVrf	Original VPN instance that the route belongs to. This field displays **default-vrf** if the route is on an IPv6 network.
TableID	ID of the routing table.
OrigAs	Original AS number.
NibID	ID of the next hop.
LastAs	Last AS number.
AttrID	Attribute ID.
Neighbor	Address of the neighbor determined by the routing protocol.
Flags	Flags of the route.
OrigNextHop	Next hop address of the route.
RealNextHop	Real next hop of the route.
BkLabel	Backup label.
BkNexthop	Backup next hop.
Tunnel ID	Tunnel ID.
Interface	Output interface for packets to be forwarded along the route.
BkTunnel ID	Backup tunnel ID.
BkInterface	Backup output interface.
FtnIndex	Index of the FTN entry.
TrafficIndex	Traffic index in the range of 1 to 64. This field displays **N/A** when the value is invalid.
Connector	BGP connector attribute exchanged between BGP peers along with a VPN IPv4 route. The value of the attribute is the IP address of the remote PE device. The BGP connector attribute is used for MD VPN. This field displays **N/A** if BGP connector attribute is not supported.
Summary count	Number of routes.

1.1.11. display ipv6 routing-table acl

Use **display ipv6 routing-table acl** to display routing information permitted by an IPv6 basic ACL.

Syntax

display ipv6 routing-table [**vpn-instance** *vpn-instance-name*] **acl** *ipv6-acl-number* [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command displays routing information for the public network.

ipv6-acl-number: Specifies a basic IPv6 ACL by its number in the range of 2000 to 2999.

verbose: Displays detailed information about all routes permitted by the basic IPv6 ACL. If you do not specify this keyword, the command displays only brief information about active routes permitted by the basic IPv6 ACL.

Usage guidelines

If the specified IPv6 ACL does not exist or has no rules configured, the command displays information about all IPv6 routes.

Examples

Display brief information about active routes permitted by IPv6 ACL 2000.

```
<Switch> display ipv6 routing-table acl 2000

Summary count : 6

Destination : ::1/128                                 Protocol  : Direct
NextHop     : ::1                                     Preference: 0
Interface   : InLoop0                                 Cost      : 0

Destination: 12::/96                                  Protocol  : Direct
NextHop    : ::                                       Preference: 0
Interface  : Vlan11                                   Cost      : 0

Destination: 12::1/128                                Protocol  : Direct
NextHop    : ::1                                      Preference: 0
Interface  : InLoop0                                  Cost      : 0

Destination: 11::1/128                                Protocol  : O_INTER
NextHop    : FE80::A1F:3FFF:FE45:206                  Preference: 10
Interface  : Vlan11                                   Cost      : 2

Destination: FE80::/10                                Protocol  : Direct
NextHop    : ::                                       Preference: 0
Interface  : InLoop0                                  Cost      : 0

Destination: FF00::/8                                 Protocol  : Direct
NextHop    : ::                                       Preference: 0
Interface  : NULL0                                    Cost      : 0
```

For command output, see Table 1-4 .

Display detailed information about all routes permitted by IPv6 ACL 2000.

```
<Switch> display ipv6 routing-table acl 2000 verbose

Summary count : 6

Destination: ::1/128
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x0                  Age: 19h29m12s
       Cost: 0              Preference: 0
      IpPre: N/A            QosLocalID: N/A
        Tag: 0                   State: Active NoAdv
  OrigTblID: 0x0               OrigVrf: default-vrf
    TableID: 0xa                OrigAs: 0
      NibID: 0x20000000         LastAs: 0
     AttrID: 0xffffffff       Neighbor: ::
      Flags: 0x10004       OrigNextHop: ::1
      Label: NULL          RealNextHop: ::1
    BkLabel: NULL            BkNextHop: N/A
  Tunnel ID: Invalid          Interface: InLoopBack0
BkTunnel ID: Invalid       BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A

Destination: 12::/96
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x0                  Age: 00h07m57s
       Cost: 0              Preference: 0
      IpPre: N/A            QosLocalID: N/A
        Tag: 0                   State: Active Adv
  OrigTblID: 0x0               OrigVrf: default-vrf
    TableID: 0xa                OrigAs: 0
      NibID: 0x20000003         LastAs: 0
     AttrID: 0xffffffff       Neighbor: ::
      Flags: 0x10080       OrigNextHop: ::
      Label: NULL          RealNextHop: ::
    BkLabel: NULL            BkNextHop: N/A
  Tunnel ID: Invalid          Interface: Vlan-interface11
BkTunnel ID: Invalid       BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A

Destination: 12::1/128
   Protocol: Direct
 Process ID: 0
```

```
  SubProtID: 0x0                  Age: 00h07m55s
       Cost: 0              Preference: 0
      IpPre: N/A            QosLocalID: N/A
        Tag: 0                   State: Active NoAdv
  OrigTblID: 0x0               OrigVrf: default-vrf
    TableID: 0xa                OrigAs: 0
      NibID: 0x20000000         LastAs: 0
     AttrID: 0xffffffff        Neighbor: ::
      Flags: 0x10004        OrigNextHop: ::1
      Label: NULL           RealNextHop: ::1
    BkLabel: NULL             BkNextHop: N/A
  Tunnel ID: Invalid          Interface: InLoopBack0
BkTunnel ID: Invalid        BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A

Destination: 11::1/128
   Protocol: O_INTER
 Process ID: 1
  SubProtID: 0x2                  Age: 00h06m43s
       Cost: 2              Preference: 10
      IpPre: N/A            QosLocalID: N/A
        Tag: 0                   State: Active Adv
  OrigTblID: 0x0               OrigVrf: default-vrf
    TableID: 0xa                OrigAs: 0
      NibID: 0x23000003         LastAs: 0
     AttrID: 0x ffffffff       Neighbor: ::
      Flags: 0x10041        OrigNextHop: FE80::A1F:3FFF:FE45:206
      Label: NULL           RealNextHop: FE80::A1F:3FFF:FE45:206
    BkLabel: NULL             BkNextHop: N/A
  Tunnel ID: Invalid          Interface: Vlan-interface11
BkTunnel ID: Invalid        BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A

Destination: FE80::/10
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x0                  Age: 19h29m12s
       Cost: 0              Preference: 0
      IpPre: N/A            QosLocalID: N/A
        Tag: 0                   State: Active NoAdv
  OrigTblID: 0x0               OrigVrf: default-vrf
    TableID: 0xa                OrigAs: 0
      NibID: 0x20000002         LastAs: 0
     AttrID: 0xffffffff        Neighbor: ::
      Flags: 0x10084        OrigNextHop: ::
      Label: NULL           RealNextHop: ::
```

```
     BkLabel: NULL              BkNextHop: N/A
   Tunnel ID: Invalid           Interface: InLoopBack0
BkTunnel ID: Invalid         BkInterface: N/A
    FtnIndex: 0x0           TrafficIndex: N/A
   Connector: N/A

Destination: FF00::/8
    Protocol: Direct
 Process ID: 0
   SubProtID: 0x0                    Age: 19h29m12s
        Cost: 0               Preference: 0
       IpPre: N/A             QosLocalID: N/A
         Tag: 0                    State: Active NoAdv
  OrigTblID: 0x0               OrigVrf: default-vrf
     TableID: 0xa                OrigAs: 0
       NibID: 0x20000001          LastAs: 0
      AttrID: 0xffffffff        Neighbor: ::
       Flags: 0x10014        OrigNextHop: ::
       Label: NULL           RealNextHop: ::
     BkLabel: NULL              BkNextHop: N/A
   Tunnel ID: Invalid           Interface: NULL0
BkTunnel ID: Invalid         BkInterface: N/A
    FtnIndex: 0x0           TrafficIndex: N/A
   Connector: N/A
```

For command output, see Table 1-5 .

1.1.12. display ipv6 routing-table *ipv6-address*

Use **display ipv6 routing-table** *ipv6-address* to display information about routes to an IPv6 destination address.

Use **display ipv6 routing-table** *ipv6-address1* **to** *ipv6-address2* to display information about routes to a range of IPv6 destination addresses.

Syntax

display ipv6 routing-table [**vpn-instance** *vpn-instance-name*] *ipv6-address* [*prefix-length*] [**longer-match**] [**verbose**]

display ipv6 routing-table [**vpn-instance** *vpn-instance-name*] *ipv6-address1* **to** *ipv6-address2* [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command displays routing information for the public network.

ipv6-address: Specifies a destination IPv6 address.

prefix-length: Specifies the prefix length in the range of 0 to 128.

longer-match: Displays the route entry with the longest prefix.

ipv6-address1 **to** *ipv6-address2*: Specifies a destination IPv6 address range.

verbose: Displays detailed routing table information, including information about both active and inactive routes. If you do not specify this keyword, the command displays only brief information about active routes.

Usage guidelines

Executing the command with different parameters yields different output.

- **display ipv6 routing-table** *ipv6-address*
  - The system ANDs the entered destination IPv6 address with the prefix length in each active route entry.
  - The system ANDs the destination IPv6 address in each active route entry with the prefix length in the entry.

  If the two operations yield the same result for an entry, the entry is displayed.
- **display ipv6 routing-table** *ipv6-address prefix-length*
  - The system ANDs the entered destination IPv6 address with the entered prefix length.
  - The system ANDs the destination IPv6 address in each active route entry with the entered prefix length.

  If the two operations yield the same result for an entry with a prefix length not greater than the entered prefix length, the entry is displayed.
- **display ipv6 routing-table** *ipv6-address* **longer-match**
  - The system ANDs the entered destination IPv6 address with the prefix length in each active route entry.
  - The system ANDs the destination IPv6 address in each active route entry with the prefix length in the entry.

  If the two operations yield the same result for multiple entries, the entry with the longest prefix length is displayed.
- **display ipv6 routing-table** *ipv6-address prefix-length* **longer-match**
  - The system ANDs the entered destination IPv6 address with the entered prefix length.
  - The system ANDs the destination IPv6 address in each active route entry with the entered prefix length.

  If the two operations yield the same result for multiple entries with a prefix length not greater than the entered prefix length, the entry with the longest prefix length is displayed.
- **display ipv6 routing-table** *ipv6-address1* **to** *ipv6-address2*

  The system displays route entries with destinations in the range of *ipv6-address1*/128 to *ipv6-address2*/128.

Examples

Display brief information about the routes to the destination IPv6 address 10::1 127.

```
<Switch> display ipv6 routing-table 10::1 127
```

```
Summary count: 3

Destination: 10::/64                                  Protocol  : Static
NextHop    : ::                                       Preference: 60
Interface  : NULL0                                    Cost      : 0

Destination: 10::/68                                  Protocol  : Static
NextHop    : ::                                       Preference: 60
Interface  : NULL0                                    Cost      : 0

Destination: 10::/120                                 Protocol  : Static
NextHop    : ::                                       Preference: 60
Interface  : NULL0                                    Cost      : 0
```

Display brief information about the most specific route to the destination IPv6 address 10::1 and prefix length 127.

```
<Switch> display ipv6 routing-table 10::1 127 longer-match

Summary count : 1

Destination: 10::/120                                 Protocol  : Static
NextHop    : ::                                       Preference: 60
Interface  : NULL0                                    Cost      : 0
```

Display brief information about the routes to destination addresses in the range of 100:: to 300::.

```
<Switch> display ipv6 routing-table 100:: to 300::

Summary count : 3

Destination: 100::/64                                 Protocol  : Static
NextHop    : ::                                       Preference: 60
Interface  : NULL0                                    Cost      : 0

Destination: 200::/64                                 Protocol  : Static
NextHop    : ::                                       Preference: 60
Interface  : NULL0                                    Cost      : 0

Destination: 300::/64                                 Protocol  : Static
NextHop    : ::                                       Preference: 60
Interface  : NULL0                                    Cost      : 0
```

Display detailed information about the routes to destination IPv6 addresses 1:2::3:4/128.

```
<Switch> display ipv6 routing-table 1:2::3:4 128 verbose

Summary count : 1

Destination: 1:2::3:4/128
   Protocol: O_INTRA
 Process ID: 1
```

```
  SubProtID: 0x1                    Age: 00h01m14s
       Cost: 1                Preference: 10
      IpPre: N/A              QosLocalID: N/A
        Tag: 0                     State: Active Adv
  OrigTblID: 0x0                OrigVrf: default-vrf
    TableID: 0xa                 OrigAs: 0
      NibID: 0x23000002          LastAs: 0
     AttrID: 0xffffffff         Neighbor: ::
      Flags: 0x10041         OrigNextHop: FE80::A1F:3FFF:FE45:206
      Label: NULL            RealNextHop: FE80::A1F:3FFF:FE45:206
    BkLabel: NULL              BkNextHop: N/A
  Tunnel ID: Invalid           Interface: Vlan-interface11
BkTunnel ID: Invalid         BkInterface: N/A
   FtnIndex: 0x0            TrafficIndex: N/A
  Connector: N/A
```

For command output, see Table 1-4 .

1.1.13. display ipv6 routing-table prefix-list

Use **display ipv6 routing-table prefix-list** to display information about IPv6 routes permitted by an IPv6 prefix list.

Syntax

display ipv6 routing-table [**vpn-instance** *vpn-instance-name*] **prefix-list** *prefix-list-name* [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command displays routing information for the public network.

prefix-list-name: Specifies an IPv6 prefix list by its name, a case-sensitive string of 1 to 63 characters.

verbose: Displays detailed information about all IPv6 routes permitted by the IPv6 prefix list. If you do not specify this keyword, the command displays brief information about active IPv6 routes permitted by the IPv6 prefix list.

Usage guidelines

If the specified IPv6 prefix list does not exist, the command displays information about all routes.

Examples

Create an IPv6 prefix list named test to permit the prefix ::1/128.

```
<Switch> system-view
[Switch] ipv6 prefix-list test permit ::1 128
```

Display brief information about the active IPv6 route permitted by the IPv6 prefix list.

```
[Switch] display ipv6 routing-table prefix-list test

Summary count : 1

Destination: ::1/128                                    Protocol   : Direct
NextHop    : ::1                                        Preference: 0
Interface  : InLoop0                                    Cost       : 0
```

For command output, see Table 1-4 .

Display detailed information about all routes permitted by the IPv6 prefix list.

```
[Switch] display ipv6 routing-table prefix-list test verbose

Summary count : 1

Destination: ::1/128
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x0                    Age: 08h57m19s
       Cost: 0                Preference: 0
      IpPre: N/A              QosLocalID: N/A
        Tag: 0                     State: Active NoAdv
  OrigTblID: 0x0                OrigVrf: default-vrf
    TableID: 0xa                 OrigAs: 0
      NibID: 0x20000000          LastAs: 0
     AttrID: 0xffffffff        Neighbor: ::
      Flags: 0x10004        OrigNextHop: ::1
      Label: NULL           RealNextHop: ::1
    BkLabel: NULL             BkNextHop: N/A
  Tunnel ID: Invalid           Interface: InLoopBack0
BkTunnel ID: Invalid        BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A
```

For command output, see Table 1-5 .

1.1.14. display ipv6 routing-table protocol

Use **display ipv6 routing-table protocol** to display information about IPv6 routes installed by a protocol.

Syntax

display ipv6 routing-table [**vpn-instance** *vpn-instance-name*] **protocol** *protocol* [**inactive** | **verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command displays routing information for the public network.

protocol: Specifies a routing protocol.

inactive: Displays information about inactive routes. If you do not specify this keyword, the command displays information about both active and inactive routes.

verbose: Displays detailed routing table information. If you do not specify this keyword, the command displays brief routing information.

Examples

Display brief information about IPv6 direct routes.

```
<Switch> display ipv6 routing-table protocol direct

Summary count : 3

Direct Routing Table Status : <Active>
Summary count : 3

Destination: ::1/128                                Protocol  : Direct
NextHop    : ::1                                    Preference: 0
Interface  : InLoop0                                Cost      : 0

Destination: FE80::/10                              Protocol  : Direct
NextHop    : ::                                     Preference: 0
Interface  : InLoop0                                Cost      : 0

Destination: FF00::/8                               Protocol  : Direct
NextHop    : ::                                     Preference: 0
Interface  : NULL0                                  Cost      : 0

Direct Routing Table Status : <Inactive>
Summary count : 0
```

Display brief information about IPv6 static routes.

```
<Switch> display ipv6 routing-table protocol static

Summary count : 3

Static Routing table Status : <Active>
Summary count : 3

Destination: 2::2/128                               Protocol  : Static
NextHop    : fe80::2                                Preference: 60
Interface  : Vlan12                                 Cost      : 0

Destination: 2::2/128                               Protocol  : Static
```

```
NextHop     : fe80::3                                Preference: 60
Interface   : Vlan12                                 Cost      : 0

Destination: 3::3/128                                Protocol  : Static
NextHop     : 2::2                                   Preference: 60
Interface   : Vlan12                                 Cost      : 0

Static Routing table Status : <Inactive>
Summary count : 0
```

Display detailed information about IPv6 BGP routes.

```
<Switch> display ipv6 routing-table protocol bgp4+ verbose

Summary count : 1

Destination: 22::22/128
   Protocol: BGP4+ instance abc
 Process ID: 0
  SubProtID: 0x6                    Age: 00h04m15s
       Cost: 0                Preference: 255
      IpPre: N/A              QosLocalID: N/A
        Tag: 0                     State: Active Adv
  OrigTblID: 0x0                OrigVrf: default-vrf
    TableID: 0xa                 OrigAs: 200
      NibID: 0x25000001          LastAs: 200
     AttrID: 0x3                Neighbor: 121::2
      Flags: 0x10060         OrigNextHop: 121::2
      Label: NULL            RealNextHop: 121::2
    BkLabel: NULL              BkNextHop: N/A
  Tunnel ID: Invalid           Interface: Vlan-interface11
BkTunnel ID: Invalid         BkInterface: N/A
   FtnIndex: 0x0            TrafficIndex: N/A
  Connector: N/A
```

For command output, see Table 1-4 .

1.1.15. display max-ecmp-num

Use **display max-ecmp-num** to display the maximum number of IPv4 ECMP routes.

Syntax

display max-ecmp-num

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display the maximum number of IPv4 ECMP routes.

```
<Switch> display max-ecmp-num
  Max-ECMP-Num in use: 6
  Max-ECMP-Num at the next reboot: 10
```

Table 1-6 Command output

Field	Description
Max-ECMP-Num in use	Maximum number of current IPv4 ECMP routes in use.
Max-ECMP-Num at the next reboot	Maximum number of IPv4 ECMP routes at the next reboot of the device.

Related commands

max-ecmp-num

1.1.16. display ipv6 routing-table statistics

Use **display ipv6 routing-table statistics** to display IPv6 route statistics, including numbers of total routes, routes installed and deleted by the protocol, and active routes.

Syntax

display ipv6 routing-table [**all-routes** | **all-vpn-instance** | **vpn-instance** *vpn-instance-name*] **statistics**

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

all-routes: Displays IPv6 route statistics for the public network and all VPN instances.

all-vpn-instance: Specifies all VPN instances.

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

If you do not specify any parameters, the command displays IPv6 route statistics for the public network.

Examples

Display IPv6 route statistics for the public network.

```
<Switch> display ipv6 routing-table statistics

Total prefixes: 8        Active prefixes: 8

Proto       route       active      added       deleted
```

```
DIRECT     5           5           5           0
STATIC     3           3           3           0
RIPng      0           0           0           0
OSPFv3     0           0           0           0
IS-ISv6    0           0           0           0
BGP4+      0           0           0           0
Total      8           8           8           0
```

Display IPv6 route statistics for the public network and all VPN instances.

```
<Switch> display ipv6 routing-table all-routes statistics

VPN instance: public instance
Total prefixes: 6        Active prefixes: 6

Proto      route       active      added       deleted
DIRECT     3           3           3           0
STATIC     3           3           5           2
RIP        0           0           0           0
OSPF       0           0           0           0
IS-IS      0           0           0           0
LISP       0           0           0           0
BGP        0           0           0           0
Total      6           6           8           2

VPN instance: vpn1
Total prefixes: 20        Active prefixes: 20

Proto      route       active      added       deleted
DIRECT     8           8           8           0
STATIC     0           0           0           0
RIP        0           0           0           0
OSPF       0           0           0           0
IS-IS      0           0           0           0
LISP       0           0           0           0
BGP        12          12          12          0
Total      20          20          20          0
```

Display IPv6 route statistics for all VPN instances.

```
<Switch> display ipv6 routing-table all-vpn-instance statistics

VPN instance: vpn1
Total prefixes: 11        Active prefixes: 11

Proto      route       active      added       deleted
DIRECT     8           8           8           0
STATIC     3           3           5           2
RIP        0           0           0           0
OSPF       0           0           0           0
IS-IS      0           0           0           0
```

```
LISP        0           0           0           0
BGP         0           0           0           0
Total       11          11          13          2

VPN instance: vpn2
Total prefixes: 8        Active prefixes: 8

Proto       route       active      added       deleted
DIRECT      8           8           8           0
STATIC      0           0           0           0
RIP         0           0           0           0
OSPF        0           0           0           0
IS-IS       0           0           0           0
LISP        0           0           0           0
BGP         0           0           0           0
Total       8           8           8           0
```

Table 1-7 Command output

Field	Description
Proto	Public network or VPN instance that the IPv6 routing table belongs to. For the public network, this field displays **public instance**. For a VPN instance, this field displays the VPN instance name.
Proto	Protocol that installed the route.
route	Number of routes installed by the protocol.
active	Number of active routes.
added	Number of routes added to the routing table after the router started up or the routing table was cleared most recently.
deleted	Number of routes marked as deleted, which will be cleared after a period.
Total	Total number of routes.

1.1.17. display rib graceful-restart

Use **display rib graceful-restart** to display RIB GR state information.

Syntax

display rib graceful-restart

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display RIB GR state information.

```
<Switch> display rib graceful-restart
```

```
RIB GR state     : Phase2-calculation end
RCOM GR state    : Flush end
Protocol GR state:
 No.  Protocol   Lifetime FD   State    Start/End
-----------------------------------------------
 1    DIRECT     100      30   End      No/No
 2    STATIC     480      34   End      No/No
 3    OSPF       480      36   End      No/No
 4    ISIS       480      32   End      No/No
 5    BGP instance abc
                 480      22   End      No/No
 6    BGP instance default
                 480      25   End      No/No
 7    LDP        480      35   End      No/No
 8    SLSP       480      29   End      No/No
```

Table 1-8 Command output

Field	Description
RIB GR state	RIB GR status: • **Start**—GR starts. • **IGP end**—All IGP protocols complete GR. • **VPN-triggering end**—Optimal route selection triggered by VPN routes completes. • **VPN-calculation end**—Optimal VPN route selection completes. • **Routing protocol end**—All routing protocols complete GR. • **NSR-calculation unfinished**—NSR has not finished optimal route selection. • **Triggering start**—All triggered optimal route selection starts. • **Triggering end**—All triggered optimal route selection completes. • **Phase1-calculation end**—Optimal route selection phase 1 completes. • **All end**—All protocols complete GR. • **Phase2-calculation end**—Optimal route selection phase 2 completes.
RCOM GR state	RCOM GR status: • **Start**—GR starts. • **VPN-calculation end**—Optimal VPN route selection completes. • **VPN-notification end**—VPN routes have been delivered to the route management module. • **Routing protocol end**—All routing protocols complete GR. • **NSR-calculation unfinished**—NSR has not finished optimal route selection. • **Phase1-calculation end**—Optimal route selection phase 1 completes. • **Notification end**—All routes have been delivered to the route management module. • **Phase2-calculation end**—Optimal route selection phase 2 completes.

Field	Description
	• **Flush start**—Starts to flush routes to the FIB. • **Flush end**—Completes flushing routes to the FIB.
No.	Protocol number.
Lifetime	Lifetime (in seconds) of routes/labels in the RIB during GR.
FD	Handle between the protocol and the RIB.
State	Protocol GR state: • **Init**—Initialization state. • **Listen**—Listening state. • Idle. • Active. • **Start**—GR starts. • **End**—GR completes.
Start/End	Message sending state: • **No**—The message has not been sent. • **Yes**—The message has been sent.

1.1.18. ip route fast-switchover enable

Use **ip route fast-switchover enable** to enable IPv4 route fast switchover.

Use **undo ip route fast-switchover enable** to disable IPv4 route fast switchover.

Syntax

```
ip route fast-switchover enable
undo ip route fast-switchover enable
```

Default

IPv4 route fast switchover is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command applies to a device that provides the same physical output interface for large numbers of routes, including ECMP routes and primary/secondary routes. When a link failure occurs on the interface, the device must perform the following tasks before switching the traffic to another route:

1. Deletes all ARP entries for the link.
2. Instructs the FIB to delete the associated FIB entries.

This procedure is time consuming and interrupts traffic for a long time. To resolve this problem, you can enable route fast switchover. This feature allows the device to first instruct the FIB to delete the invalid FIB entries for route switchover.

Examples

Enable IPv4 route fast switchover.

```
<Switch> system-view
[Switch] ip route fast-switchover enable
```

1.1.19. ipv6 route fast-switchover enable

Use **ipv6 route fast-switchover enable** to enable IPv6 route fast switchover.

Use **undo ipv6 route fast-switchover enable** to disable IPv6 route fast switchover.

Syntax

ipv6 route fast-switchover enable

undo ipv6 route fast-switchover enable

Default

IPv6 route fast switchover is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command applies to a device that provides the same physical output interface for large numbers of routes, including ECMP routes and primary/secondary routes. When a link failure occurs on the interface, the device must perform the following tasks before switching the traffic to another route:

1. Deletes all ND entries for the link.
2. Instructs the FIB to delete the associated FIB entries.

This procedure is time consuming and interrupts traffic for a long time. To resolve this problem, you can enable route fast switchover. This feature allows the device to instruct the FIB to delete the invalid FIB entries for route switchover first.

Examples

Enable IPv6 route fast switchover.

```
<Switch> system-view
[Switch] ipv6 route fast-switchover enable
```

1.1.20. max-ecmp-num

Use **max-ecmp-num** to set the maximum number of IPv4 ECMP routes.

Syntax

max-ecmp-num *number*

Default

The maximum number of ECMP routes is 8.

Views

System view

Predefined user roles

network-admin

Parameters

number: Specifies the maximum number of IPv4 ECMP routes. The value range for this argument is 1 to 32.

Usage guidelines

This command takes effect after a device reboot. Before you reboot the device, make sure you understand the potential impact on the network.

Examples

Set the maximum number of IPv4 ECMP routes to 10.

```
<Switch> system-view
[Switch] max-ecmp-num 10
The configuration will take effect at the next reboot. Continue? [Y/N]:y
Reboot device to make the configuration take effect.
```

After reboot, the maximum number of IPv4 ECMP routes is 10.

Related commands

display max-ecmp-num

1.1.21. non-stop-routing

MEMO:

non-stop-routing command is supported from later software, including Version 7.2.16.

Use **non-stop-routing** to enable RIB NSR.

Use **undo non-stop-routing** to disable RIB NSR.

Syntax

non-stop-routing

undo non-stop-routing

Default

RIB NSR is disabled.

Views

RIB IPv4 address family view

RIB IPv6 address family view

Predefined user roles

network-admin

Examples

Enable NSR for the RIB IPv4 address family.

```
<Switch> system-view
[Switch] rib
[Switch-rib] address-family ipv4
[Switch-rib-ipv4] non-stop-routing
```

1.1.22. protocol lifetime

Use **protocol lifetime** to set the maximum lifetime for IPv4 or IPv6 routes and labels in the RIB.

Use **undo protocol lifetime** to restore the default.

Syntax

protocol *protocol* **lifetime** *seconds*

undo protocol *protocol* **lifetime**

Default

The maximum lifetime for IPv4 or IPv6 routes and labels in the RIB is 480 seconds.

Views

RIB IPv4 address family view

RIB IPv6 address family view

Predefined user roles

network-admin

Parameters

protocol: Specifies a routing protocol.

seconds: Specifies the maximum lifetime for routes and labels in the RIB, in the range of 1 to 6000 seconds.

Usage guidelines

When GR is enabled, make sure the protocol can complete GR and install all route entries to the RIB within the lifetime configured in this command.

Examples

Set the maximum lifetime for RIP routes and labels in the RIB to 60 seconds.

```
<Switch> system-view
[Switch] rib
[Switch-rib] address-family ipv4
[Switch-rib-ipv4] protocol rip lifetime 60
```

1.1.23. reset ip routing-table statistics protocol

Use **reset ip routing-table statistics protocol** to clear IPv4 route statistics.

Syntax

reset ip routing-table statistics protocol [**vpn-instance** *vpn-instance-name*] { *protocol* | **all** }

Views

User view

Predefined user roles

network-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command clears IPv4 route statistics for the public network.

protocol: Clears route statistics for a routing protocol.

all: Clears route statistics for all IPv4 routing protocols.

Examples

Clear all IPv4 route statistics for the public network.

```
<Switch> reset ip routing-table statistics protocol all
```

1.1.24. reset ipv6 routing-table statistics protocol

Use **reset ipv6 routing-table statistics protocol** to clear IPv6 route statistics.

Syntax

reset ipv6 routing-table statistics protocol [**vpn-instance** *vpn-instance-name*] { *protocol* | **all** }

Views

User view

Predefined user roles

network-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command clears the IPv6 route statistics for the public network.

protocol: Clears route statistics for an IPv6 routing protocol.

all: Clears route statistics for all IPv6 routing protocols.

Examples

Clear all IPv6 route statistics for the public network.

```
<Switch> reset ipv6 routing-table statistics protocol all
```

1.1.25. rib

Use **rib** to enter RIB view.

Use **undo rib** to remove all configurations in RIB view.

Syntax

rib

undo rib

Views

System view

Predefined user roles

network-admin

Examples

Enter RIB view.

```
<Switch> system-view
[Switch] rib
[Switch-rib]
```

1.1.26. routing-table limit

Use **routing-table limit** to set the maximum number of active IPv4/IPv6 routes supported by the device.

Use **undo routing-table limit** to restore the default.

Syntax

routing-table limit *number* **simply-alert**

undo routing-table limit

Default

The maximum number of active IPv4/IPv6 routes is not set for the device.

Views

RIB IPv4 address family view

RIB IPv6 address family view

Predefined user roles

network-admin

Parameters

number: Specifies the maximum number of active IPv4/IPv6 routes supported by the device, in the range of 1 to 4294967295.

simply-alert: Enables the device to still accept active routes but generate a log message when the number of active IPv4/IPv6 routes exceed the maximum number.

Usage guidelines

Configuration in RIB IPv4 address family view limits the number of active IPv4 routes for the public network and all VPN instances.

Configuration in RIB IPv6 address family view limits the number of active IPv6 routes for the public network and all VPN instances.

Examples

In RIB IPv4 address family view, set the maximum number of active IPv4 routes to 1000 for the public network and all VPN instances. The device still accepts new active routes but generates a system log message when the maximum number of active routes is exceeded.

<Switch> system-view

[Switch] rib

[Switch-rib] address-family ipv4

[Switch-rib-ipv4] routing-table limit 1000 simply-alert

Contents

A page of this section is **5-x-x**

2. Static routing commands 2-1
2.1. Static routing commands 2-1
2.1.1. delete static-routes all 2-1
2.1.2. ip route-static 2-1
2.1.3. ip route-static default-preference 2-4

2. Static routing commands

2.1. Static routing commands

2.1.1. delete static-routes all

Use **delete static-routes all** to delete all static routes.

Syntax

delete [**vpn-instance** *vpn-instance-name*] **static-routes all**

Views

System view

Predefined user roles

network-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command deletes all static routes for the public network.

Usage guidelines

When you use this command, the system will prompt you to confirm the operation before deleting all the static routes.

To delete one static route, use the **undo ip route-static** command. To delete all static routes, including the default route, use the **delete static-routes all** command.

Examples

Delete all static routes.

```
<Switch> system-view
[Switch] delete static-routes all
This will erase all IPv4 static routes and their configurations, you must reconfigure all
static routes.
Are you sure?[Y/N]:y
```

Related commands

ip route-static

2.1.2. ip route-static

Use **ip route-static** to configure a static route.

Use **undo ip route-static** to delete a static route.

Syntax

ip route-static *dest-address* { *mask-length* | *mask* } { *interface-type interface-number* [*next-hop-address*] | *next-hop-address* [**bfd control-packet bfd-source** *ip-address* | **permanent** | **track**

track-entry-number | **vpn-instance** *d-vpn-instance-name next-hop-address*]} [**preference** *preference*][**tag** *tag-value*][**description** *text*]

undo ip route-static *dest-address* { *mask-length* | *mask* } [*interface-type interface-number* [*next-hop-address*] | *next-hop-address* | **vpn-instance** *d-vpn-instance-name next-hop-address*] [**preference** *preference*]

ip route-static vpn-instance *s-vpn-instance-name dest-address* { *mask-length* | *mask* } { *interface-type interface-number* [*next-hop-address*] | *next-hop-address* [**public**] [**bfd control-packet bfd-source** *ip-address* | **permanent** | **track** *track-entry-number*] | **vpn-instance** *d-vpn-instance-name next-hop-address* [**bfd control-packet bfd-source** *ip-address* | **permanent** | **track** *track-entry-number*] } [**preference** *preference*] [**tag** *tag-value*] [**description** *text*]

undo ip route-static vpn-instance *s-vpn-instance-name dest-address* { *mask-length* | *mask* } [*interface-type interface-number* [*next-hop-address*] | *next-hop-address* [**public**] | **vpn-instance** *d-vpn-instance-name next-hop-address*] [**preference** *preference*]

Default

No static route is configured.

Views

System view

Predefined user roles

network-admin

Parameters

vpn-instance *s-vpn-instance-name*: Specifies a source VPN instance by its name, a case-sensitive string of 1 to 31 characters. Each VPN instance has its own routing table, and the configured static route is installed in the routing tables of the specified VPN instances.

dest-address: Specifies the destination IP address of the static route, in dotted decimal notation.

mask-length: Specifies the mask length, an integer in the range of 0 to 32.

mask: Specifies the subnet mask in dotted decimal notation.

vpn-instance *d-vpn-instance-name*: Specifies a destination VPN instance by its name, a case-sensitive string of 1 to 31 characters. If a destination VPN instance is specified, packets will search for the output interface in the destination VPN instance based on the configured next hop address.

interface-type interface-number: Specifies an output interface by its type and number. For more information, see *Layer 3—IP Routing Configuration Guide*.

next-hop-address: Specifies the IP address of the next hop, in dotted decimal notation. For more information, see *Layer 3—IP Routing Configuration Guide*.

bfd: Enables BFD to detect reachability of the static route's next hop. When the next hop is unreachable, the system immediately switches to the backup route.

control-packet: Specifies the BFD control mode.

bfd-source *ip-address*: Specifies the source IP address of BFD packets. As a best practice, specify the loopback interface address.

echo-packet: Specifies the BFD echo mode.

permanent: Specifies the route as a permanent static route. If the output interface is down, the permanent static route is still active.

track *track-entry-number*: Associates the static route with a track entry specified by its number in the range of 1 to 1024. For more information about Track, see *High Availability Configuration Guide*.

public: Indicates that the specified next hop address is on the public network.

preference *preference*: Specifies a preference for the static route, in the range of 1 to 255. The default is 60.

tag *tag-value*: Sets a tag value for marking the static route, in the range of 1 to 4294967295. The default is 0. Tags of routes are used for route control in routing policies. For more information about routing policies, see *Layer 3—IP Routing Configuration Guide*.

description *text*: Configures a description of 1 to 60 characters for the static route. The description can include special characters, such as the space, except the question mark (?).

Usage guidelines

If the destination IP address and the mask are both 0.0.0.0 (or 0), the configured route is a default route. The default route is used for forwarding a packet matching no entry in the routing table.

Implement different routing policies to configure different route preferences. For example, to enable load sharing for multiple routes to the same destination, assign the same preference to the routes. To enable the routes to back up one another, assign different preferences to them.

Follow these guidelines when you specify the output interface or the next hop address of the static route:

- If the output interface is a Null 0 interface, no next hop address is required.
- If the output interface is a point-to-point interface, you can specify only the output interface. You do not need to change the configuration of the route even if the peer address is changed.
- NBMA or P2MP interfaces need IP address-to-link layer address mappings for successful packet delivery. As a best practice, specify the next hop address for the route at the same time if the output interface is an NBMA or P2MP interface.
- If the output interface is a broadcast interface, the device uses the next hop IP address to obtain the MAC address of the next hop. Therefore, you must specify both the output interface and next hop IP address, except for certain cases such as the VXLAN across VPNs networking.

Follow these guidelines when you configure a static route:

- Enabling BFD for a flapping route could worsen the route flapping situation. Therefore, use it with caution. For more information about BFD, see *High Availability Configuration Guide*.
- For static routing-Track-NQA collaboration, you must configure the same VPN instance ID for the next hop to be detected and the NQA operation.
- Do not specify the **permanent** keyword together with the **bfd** or **track** keyword.

Examples

Configure a static route, whose destination address is 1.1.1.1/24, next hop address is 2.2.2.2, tag value is 45, and description information is **for internet**.

```
<Switch> system-view
[Switch] ip route-static 1.1.1.1 24 2.2.2.2 tag 45 description for internet
```

Related commands

display ip routing-table protocol

2.1.3. ip route-static default-preference

Use **ip route-static default-preference** to configure a default preference for static routes.

Use **undo ip route-static default-preference** to restore the default.

Syntax

ip route-static default-preference *default-preference*

undo ip route-static default-preference

Default

The default preference of static routes is 60.

Views

System view

Predefined user roles

network-admin

Parameters

default-preference: Specifies a default preference for static routes, in the range of 1 to 255.

Usage guidelines

If no preference is specified for a static route, the default preference applies.

When the default preference is reconfigured, it applies only to newly added static routes.

Examples

Set a default preference of 120 for static routes.

```
<Switch> system-view
[Switch] ip route-static default-preference 120
```

Related commands

display ip routing-table protocol

Contents

A page of this section is **5-x-x**

3. RIP commands 3-1
3.1. RIP commands 3-1
3.1.1. checkzero 3-1
3.1.2. default cost 3-1
3.1.3. default-route 3-2
3.1.4. display rip 3-3
3.1.5. display rip database 3-5
3.1.6. display rip interface 3-6
3.1.7. display rip route 3-8
3.1.8. filter-policy export 3-10
3.1.9. filter-policy import 3-12
3.1.10. graceful-restart 3-14
3.1.11. host-route 3-14
3.1.12. import-route 3-15
3.1.13. maximum load-balancing 3-16
3.1.14. network 3-17
3.1.15. non-stop-routing 3-18
3.1.16. output-delay 3-19
3.1.17. peer 3-19
3.1.18. preference 3-20
3.1.19. reset rip process 3-21
3.1.20. reset rip statistics 3-22
3.1.21. rip 3-22
3.1.22. rip authentication-mode 3-23
3.1.23. rip bfd enable 3-24
3.1.24. rip default-route 3-25
3.1.25. rip input 3-26
3.1.26. rip metricin 3-26
3.1.27. rip metricout 3-28
3.1.28. rip mib-binding 3-29
3.1.29. rip output 3-29
3.1.30. rip poison-reverse 3-30
3.1.31. rip split-horizon 3-31
3.1.32. rip summary-address 3-31
3.1.33. rip version 3-32
3.1.34. silent-interface 3-33
3.1.35. summary 3-34
3.1.36. timers 3-35
3.1.37. validate-source-address 3-36
3.1.38. version 3-36

3. RIP commands

3.1. RIP commands

3.1.1. checkzero

Use **checkzero** to enable zero field check on RIPv1 messages.

Use **undo checkzero** to disable zero field check.

Syntax

checkzero

undo checkzero

Default

The zero field check function is enabled.

Views

RIP view

Predefined user roles

network-admin

Usage guidelines

When the zero field check is enabled, the router discards RIPv1 messages in which zero fields contain non-zero values. If all messages are trustworthy, disable this feature to reduce the workload of the CPU.

Examples

Disable zero field check on RIPv1 messages for RIP process 1.

```
<Switch> system-view
[Switch] rip
[Switch-rip-1] undo checkzero
```

3.1.2. default cost

Use **default cost** to configure a default metric for redistributed routes.

Use **undo default cost** to restore the default.

Syntax

default cost *cost-value*

undo default cost

Default

The default metric of redistributed routes is 0.

Views

RIP view

Predefined user roles

network-admin

Parameters

cost-value: Specifies a default metric for redistributed routes, in the range of 0 to 16.

Usage guidelines

When you use the **import-route** command to redistribute routes from another routing protocol without specifying a metric, the metric specified by the **default cost** command applies.

Examples

Configure a default metric of 3 for redistributed routes.

```
<Switch> system-view
[Switch] rip 1
[Switch-rip-1] default cost 3
```

Related commands

import-route

3.1.3. default-route

Use **default-route** to configure all interfaces running a RIP process to advertise a default route with a specified metric to RIP neighbors.

Use **undo default-route** to restore the default.

Syntax

default-route { **only** | **originate** } [**cost** *cost-value*] *

undo default-route

Default

No default route is sent to RIP neighbors.

Views

RIP view

Predefined user roles

network-admin

Parameters

only: Advertises only a default route.

originate: Advertises both a default route and other routes.

cost-value: Specifies a cost for the default route, in the range of 1 to 15. The default is 1.

Usage guidelines

A RIP router configured with this feature does not receive any default route from RIP neighbors.

Examples

Configure all interfaces running RIP process 100 to send only a default route with a metric of 2 to RIP neighbors.

```
<Switch> system-view
[Switch] rip 100
[Switch-rip-100] default-route only cost 2
```

Related commands

rip default-route

3.1.4. display rip

Use **display rip** to display state and configuration information for a RIP process.

Syntax

display rip [*process-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies a RIP process by its ID in the range of 1 to 65535. If no process is specified, the command displays state and configuration information for all RIP processes.

Examples

Display current state and configuration information for all RIP processes.

```
<Switch> display rip
  Public VPN-instance name:
    RIP process: 1
       RIP version: 1
       Preference: 100
           Routing policy: abc
       Fast-reroute:
           Routing policy: frr
       Checkzero: Enabled
       Default cost: 0
```

```
Summary: Enabled
Host routes: Enabled
Maximum number of load balanced routes: 8
Update time   :   30 secs  Timeout time         :  180 secs
Suppress time :  120 secs  Garbage-collect time :  120 secs
Update output delay:   20(ms)  Output count:    3
Graceful-restart interval:   60 secs
Triggered Interval : 5 50 200
Silent interfaces: None
Default routes: Originate  Default routes cost: 3
Verify-source: Enabled
Networks:
    1.0.0.0
Configured peers:
    197.168.6.2
Triggered updates sent: 0
Number of routes changes: 1
Number of replies to queries: 0
```

Table 3-1 Command output

Field	Description
Public VPN-instance name	The RIP process runs on the public network.
Private VPN-instance name	VPN instance where the RIP process runs.
RIP process	RIP process ID.
RIP version	RIP version 1 or 2.
Preference	RIP preference.
Fast-reroute	RIP FRR.
Checkzero	Indicates whether the zero field check is enabled for RIPv1 messages: **Enabled** or **Disabled**.
Default cost	Default cost of redistributed routes.
Summary	Indicates whether route summarization is enabled: **Enabled** or **Disabled**.
Host routes	Indicates whether to receive host routes: **Enabled** or **Disabled**.
Maximum number of load balanced routes	Maximum number of ECMP routes for load balancing.
Update time	RIP update interval, in seconds.
Timeout time	RIP timeout time, in seconds.
Suppress time	RIP suppress interval, in seconds.
Garbage-collect time	RIP garbage-collect interval, in seconds.
Update output delay	RIP packet sending interval, in seconds.
Output count	Maximum number of RIP packets sent at each interval.

Field	Description
Graceful-restart interval	GR interval, in seconds.
Triggered Interval	Triggered update sending interval.
Silent interfaces	Silent interfaces, which do not periodically send updates.
Default routes	Indicates whether a default route is sent to RIP neighbors. • **only**—Only a default route is advertised. • **originate**—A default route is advertised along with other routes. • **disable**—No default route is advertised.
Default routes cost	Metric for a default route.
Verify-source	Indicates whether the source IP address is checked for received RIP routing updates: **Enabled** or **Disabled**.
Networks	Networks enabled with RIP.
Configured peers	Configured neighbors.
Triggered updates sent	Number of triggered updates sent.
Number of routes changes	Number of route changes.
Number of replies to queries	Number of RIP responses.

3.1.5. display rip database

Use **display rip database** to display active routes for a RIP process.

Syntax

display rip *process-id* **database** [*ip-address* { *mask-length* | *mask* }]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies a RIP process by its ID in the range of 1 to 65535.

ip-address { *mask-length* | *mask* }: Displays active routes for the specified IP address. If you do not specify this argument, the command displays all actives routes for a RIP process.

Examples

Display active routes for RIP process 100.

```
<Switch> display rip 100 database
   1.0.0.0/8, auto-summary
       1.1.1.0/24, cost 16, interface summary
       1.1.1.0/24, cost 0, nexthop 1.1.1.1, RIP-interface
       1.1.2.0/24, cost 0, imported
   2.0.0.0/8, auto-summary
   2.0.0.0/8, cost 1, nexthop 1.1.1.2
```

Display active routes with destination IP address 1.1.1.0 and mask length 24 for RIP process 100.

```
<Switch> display rip 100 database 1.1.1.0 24
   1.1.1.0/24, cost 16, interface summary
   1.1.1.0/24, cost 0, nexthop 1.1.1.1, RIP-interface
```

Table 3-2 Command output

Field	Description
cost	Cost of the route.
auto-summary	Indicates that the route is a RIP automatic summary route.
interface summary	Indicates that the route is a RIP interface summary route.
nexthop	Address of the next hop.
RIP-interface	Direct route on a RIP-enabled interface.
imported	Indicates that the route is redistributed from another routing protocol.

3.1.6. display rip interface

Use **display rip interface** to display RIP interface information for a RIP process.

Syntax

display rip *process-id* **interface** [*interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies a RIP process by its ID in the range of 1 to 65535.

interface-type interface-number: Specifies an interface by its type and number. If no interface is specified, the command displays information about all RIP interfaces for the RIP process.

Examples

Display information about all interfaces for RIP process 1.

```
<Switch> display rip 1 interface
Total: 1

 Interface: Vlan-interface10
    Address/Mask: 1.1.1.1/24          Version: RIPv1
    MetricIn: 0                       MetricIn route policy: Not designated
    MetricOut: 1                      MetricOut route policy: Not designated
    Split-horizon/Poison-reverse: On/Off  Input/Output: On/On
    Default route: Off
    Update output delay:  20(ms)      Output count: 3
    Current number of packets/Maximum number of packets: 0/2000
```

Table 3-3 Command output

Field	Description
Total	Number of interfaces running RIP.
Interface	Name of an interface running RIP.
Address/Mask	IP address and mask of the interface.
Version	RIP version running on the interface.
MetricIn	Additional metric added to incoming routes.
MetricIn route policy	Name of the routing policy used to add an additional metric for incoming routes. If no routing policy is used, the field displays **Not designated**.
MetricOut	Additional metric added to outgoing routes.
MetricOut route policy	Name of the routing policy used to add an additional routing metric for outgoing routes. If no routing policy is used, the field displays **Not designated**.
Split-horizon	Indicates whether split horizon is enabled: • **on**—Enabled. • **off**—Disabled.
Poison-reverse	Indicates whether poison reverse is enabled: • **on**—Enabled. • **off**—Disabled.
Input/Output	Indicates whether the interface is enabled to receive and send RIP messages: • **on**—Enabled. • **off**—Disabled.
Default route	Indicates whether to send a default route to RIP neighbors: • **Only**—Advertises only a default route. • **Originate**—Advertises both a default route and other routes. • **No-originate**—Advertises only non-default routes. • **Off**—Advertises no default route.
Default route cost	Metric for a default route.

Field	Description
Update output delay	RIP packet sending interval.
Output count	Maximum number of RIP packets that can be sent at each interval.
Current number of packets /Maximum number of packets	Number of RIP packets to be sent/maximum number of RIP packets that can be sent within a certain interval.

3.1.7. display rip route

Use **display rip route** to display routing information for a RIP process.

Syntax

display rip *process-id* **route** [*ip-address* { *mask-length* | *mask* } [**verbose**] | **peer** *ip-address* | **statistics**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies a RIP process by its ID in the range of 1 to 65535.

ip-address { *mask-length* | *mask* }: Displays route information for the specified IP address.

verbose: Displays all routing information for the specified destination IP address. If you do not specify this keyword, the command displays only information about optimal routes with the specified destination IP address.

peer *ip-address*: Displays route information learned from the specified neighbor.

statistics: Displays route statistics, including the total number of routes and number of routes from each neighbor.

Usage guidelines

If no optional parameters are specified, the **display rip** *process-id* **route** command displays all routing information for a RIP process.

Examples

Display all routing information for RIP process 1.

```
<Switch> display rip 1 route
 Route Flags: R - RIP, T - TRIP
              P - Permanent, A - Aging, S - Suppressed, G - Garbage-collect
              D - Direct, O - Optimal, F - Flush to RIB
```

```
------------------------------------------------------------------------------
 Peer 1.1.1.1 on Vlan-interface10
      Destination/Mask        Nexthop          Cost    Tag     Flags   Sec
      3.0.0.0/8               1.1.1.1          1       0       RAOF    24
 Local route
      Destination/Mask        Nexthop          Cost    Tag     Flags   Sec
      4.4.4.4/32              0.0.0.0          0       0       RDOF    -
      1.1.1.0/24              0.0.0.0          0       0       RDOF    -
```

Display specified routing information for RIP process 1.

```
<Switch> display rip 1 route 3.0.0.0 8 verbose
 Route Flags: R - RIP, T - TRIP
              P - Permanent, A - Aging, S - Suppressed, G - Garbage-collect
              D - Direct, O - Optimal, F - Flush to RIB
------------------------------------------------------------------------------
 Peer 1.1.1.1 on Vlan-interface10
  Destination/Mask    OrigNexthop/RealNexthop          Cost  Tag    Flags Sec
  3.0.0.0/8           1.1.1.1/1.1.1.1                  1     0      RAOF  16
```

Table 3-4 Command output

Field	Description
Route Flags	• **R**—RIP route. • **P**—The route never ages out. • **A**—The route is aging. • **S**—The route is suppressed. • **G**—The route is in Garbage-collect state. • **D**—The route is a direct route. • **O**—The route is an optimal route. • **F**—The route has been flushed to the RIB.
Peer *X.X.X.X* on *interface-type interface-number*	Routing information learned from a neighbor on a RIP interface.
Local route	Locally generated direct routes.
Destination/Mask	Destination IP address and subnet mask.
Nexthop	Next hop of the route.
OrigNexthop/RealNexthop	If the route is from a directly connected neighbor, the original next hop is the real next hop. If the route is from an indirectly connected neighbor, the **RealNexthop** field displays the recursive next hop for the route. Otherwise, the field is blank.
Cost	Cost of the route.
Tag	Route tag.
Flags	Route state.
Sec	Remaining time of the timer corresponding to the route state.

Display routing statistics for RIP process 1.

```
<Switch> display rip 1 route statistics
 Peer                    Optimal/Aging       Optimal/Permanent       Garbage
 1.1.1.1                 1/1                 0/0                     0
 Local                   2/0                 0/0                     0
 Total                   3/1                 0/0                     0
```

Table 3-5 Command output

Field	Description
Peer	IP address of a neighbor.
Optimal	Total number of optimal routes.
Aging	Total number of aging routes.
Permanent	Total number of routes that never age out.
Garbage	Total number of routes in the Garbage-collection state.
Local	Total number of locally generated direct routes.
Total	Total number of routes learned from all RIP neighbors.

3.1.8. filter-policy export

Use **filter-policy export** to configure RIP to filter redistributed routes.

Use **undo filter-policy export** to remove the filtering.

Syntax

filter-policy { *ipv4-acl-number* | **prefix-list** *prefix-list-name* } **export** [*protocol* [*process-id*] | *interface-type interface-number*]

undo filter-policy export [*protocol* [*process-id*] | *interface-type interface-number*]

Default

RIP does not filter redistributed routes.

Views

RIP view

Predefined user roles

network-admin

Parameters

ipv4-acl-number: Specifies an IPv4 ACL by its number in the range of 2000 to 3999 to filter redistributed routes.

prefix-list *prefix-list-name*: Specifies an IP prefix list by its name, a case-sensitive string of 1 to 63 characters, to filter redistributed routes.

protocol: Filters routes redistributed from the specified routing protocol.

process-id: Specifies the process ID of the specified routing protocol, in the range of 1 to 65535. Specify a process ID when the routing protocol is **rip**, or **ospf**. If no process ID is specified, the default process ID is 1.

interface-type interface-number: Specifies an interface by its type and number.

Usage guidelines

You can configure only one filtering policy to filter routes redistributed from a routing protocol or an interface. Without any protocol or interface specified, the filtering policy applies globally. If you execute this command multiple times, the most recent configuration takes effect.

To remove the filtering policy configured for a protocol or an interface, use the **undo filter-policy export** command with the protocol or interface specified.

To reference an advanced ACL (with a number from 3000 to 3999) in the command, configure the ACL using one of the following methods:

- To deny/permit a route with the specified destination, use the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* command.
- To deny/permit a route with the specified destination and mask, use the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* **destination** *dest-addr dest-wildcard* command.

The **source** keyword specifies the destination address of a route and the **destination** keyword specifies the subnet mask of the route. For the mask configuration to take effect, specify a contiguous subnet mask.

Examples

Use basic ACL 2000 to filter redistributed routes.

```
<Switch> system-view
[Switch] acl basic 2000
[Switch-acl-ipv4-basic-2000] rule deny source 192.168.10.0 0.0.0.255
[Switch-acl-ipv4-basic-2000] quit
[Switch] rip 1
[Switch-rip-1] filter-policy 2000 export
```

Use IP prefix list **abc** to filter redistributed routes.

```
<Switch> system-view
[Switch] ip prefix-list abc index 10 permit 11.0.0.0 8
[Switch] rip 1
[Switch-rip-1] filter-policy prefix-list abc export
```

Configure advanced ACL 3000 to permit only route 113.0.0.0/16 to pass. Use ACL 3000 to filter redistributed routes.

```
<Switch> system-view
[Switch] acl advanced 3000
[Switch-acl-ipv4-adv-3000] rule 10 permit ip source 113.0.0.0 0 destination 255.255.0.0
0
```

```
[Switch-acl-ipv4-adv-3000] rule 100 deny ip
[Switch-acl-ipv4-adv-3000] quit
[Switch] rip 1
[Switch-rip-1] filter-policy 3000 export
```

Related commands

acl (*ACL and QoS Command Reference*)

import-route

ip prefix-list

3.1.9. filter-policy import

Use **filter-policy import** to configure RIP to filter received routes.

Use **undo filter-policy import** to remove the filtering.

Syntax

filter-policy { *ipv4-acl-number* | **gateway** *prefix-list-name* | **prefix-list** *prefix-list-name* [**gateway** *prefix-list-name*] } **import** [*interface-type interface-number*]

undo filter-policy import [*interface-type interface-number*]

Default

RIP does not filter received routes.

Views

RIP view

Predefined user roles

network-admin

Parameters

ipv4-acl-number: Specifies an IPv4 ACL by its number in the range of 2000 to 3999 to filter received routes.

prefix-list *prefix-list-name*: Specifies an IP prefix list by its name, a case-sensitive string of 1 to 63 characters, to filter received routes.

gateway *prefix-list-name*: Specifies an IP prefix list by its name, a case-sensitive string of 1 to 63 characters, to filter routes based on their next hops.

interface-type interface-number: Specifies an interface by its type and number.

Usage guidelines

You can configure only one filtering policy to filter routes received on an interface. Without any interface specified, the filtering policy applies globally. If you execute this command multiple times, the most recent configuration takes effect.

To remove the filtering policy configured for an interface, use the **undo filter-policy import** command with the interface specified.

To reference an advanced ACL (with a number from 3000 to 3999) in the command, configure the ACL using one of the following methods:

- To deny/permit a route with the specified destination, use the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* command
- To deny/permit a route with the specified destination and mask, use the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* **destination** *dest-addr dest-wildcard* command.

The **source** keyword specifies the destination address of a route and the **destination** keyword specifies the subnet mask of the route. For the mask configuration to take effect, specify a contiguous subnet mask.

Examples

Use basic ACL 2000 to filter received RIP routes.

```
<Switch> system-view
[Switch] acl basic 2000
[Switch-acl-ipv4-basic-2000] rule deny source 192.168.10.0 0.0.0.255
[Switch-acl-ipv4-basic-2000] quit
[Switch] rip 1
[Switch-rip-1] filter-policy 2000 import
```

Use IP prefix list **abc** to filter received RIP routes.

```
<Switch> system-view
[Switch] ip prefix-list abc index 10 permit 11.0.0.0 8
[Switch] rip 1
[Switch-rip-1] filter-policy prefix-list abc import
```

Configure advanced ACL 3000 to permit only route 113.0.0.0/16 to pass. Use ACL 3000 to filter received routes.

```
<Switch> system-view
[Switch] acl advanced 3000
[Switch-acl-ipv4-adv-3000] rule 10 permit ip source 113.0.0.0 0 destination 255.255.0.0
0
[Switch-acl-ipv4-adv-3000] rule 100 deny ip
[Switch-acl-ipv4-adv-3000] quit
[Switch] rip 1
[Switch-rip-1] filter-policy 3000 import
```

Related commands

acl (*ACL and QoS Command Reference*)

ip prefix-list

3.1.10. graceful-restart

Use **graceful-restart** to enable RIP GR.

Use **undo graceful-restart** to disable RIP GR.

Syntax

graceful-restart

undo graceful-restart

Default

RIP GR is disabled.

Views

RIP view

Predefined user roles

network-admin

Examples

Enable GR for RIP process 1.

```
<Switch> system-view
[Switch] rip 1
[Switch-rip-1] graceful-restart
```

3.1.11. host-route

Use **host-route** to enable host route reception.

Use **undo host-route** to disable host route reception.

Syntax

host-route

undo host-route

Default

RIP receives host routes.

Views

RIP view

Predefined user roles

network-admin

Usage guidelines

A router might receive many host routes from the same subnet. These routes are not helpful for routing and occupy a large number of resources. To solve this problem, use the **undo host-route** command to disable RIP from receiving host routes.

This command takes effect only for RIPv2 routes.

Examples

Disable RIP from receiving host routes.

```
<Switch> system-view
[Switch] rip 1
[Switch-rip-1] undo host-route
```

3.1.12. import-route

Use **import-route** to enable route redistribution from another routing protocol.

Use **undo import-route** to remove routes redistributed from another routing protocol.

Syntax

import-route bgp [**allow-ibgp**] [**cost** *cost-value* | **route-policy** *route-policy-name* | **tag** *tag*] *

undo import-route bgp

import-route { **direct** | **static** } [**cost** *cost-value* | **route-policy** *route-policy-name* | **tag** *tag*] *

undo import-route { **direct** | **static** }

import-route { **ospf** | **rip** } [*process-id* | **all-processes**] [**cost** *cost-value* | **route-policy** *route-policy-name* | **tag** *tag*] *

undo import-route { **ospf** | **rip** } [*process-id* | **all-processes**]

Default

RIP does not redistribute routes from any other routing protocol.

Views

RIP view

Predefined user roles

network-admin

Parameters

bgp: Redistributes BGP routes.

direct: Redistributes direct routes.

ospf: Redistributes OSPF routes.

rip: Redistributes RIP routes.

static: Redistributes static routes.

process-id: Specifies an OSPF, or RIP process by its ID in the range of 1 to 65535. The default is 1.

all-processes: Enables route redistribution from all OSPF or RIP processes.

allow-ibgp: Allows redistribution of IBGP routes. The **import-route bgp** command redistributes only EBGP routes. The **import-route bgp allow-ibgp** command additionally redistributes IBGP routes and might cause routing loops. Therefore, use it with caution.

cost *cost-value*: Specifies a cost for redistributed routes, in the range of 0 to 16. The default cost is 0.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters.

tag *tag*: Specifies a tag for marking redistributed routes, in the range of 0 to 65535. The default is 0.

Usage guidelines

This command redistributes only active routes. To view route state information, use the **display ip routing-table protocol** command.

The **undo import-route** { **ospf** | **rip** } **all-processes** command removes only the configuration made by the **import-route** { **ospf** | **rip** } **all-processes** command. It does not remove the configuration made by the **import-route** { **ospf** | **rip** } *process-id* command.

Examples

Redistribute static routes into RIP, and set the cost for redistributed routes to 4.

```
<Switch> system-view
[Switch] rip 1
[Switch-rip-1] import-route static cost 4
```

Related commands

default cost

3.1.13. maximum load-balancing

Use **maximum load-balancing** to set the maximum number of RIP equal-cost multi-path (ECMP) routes for load balancing.

Use **undo maximum load-balancing** to restore the default.

Syntax

maximum load-balancing *number*

undo maximum load-balancing

Default

8

Views

RIP view

Predefined user roles

network-admin

Parameters

number: Specifies the maximum number of RIP ECMP routes in the range of 1 to 8. Load balancing is not implemented when the value is 1.

Examples

Set the maximum number of RIP ECMP routes to 2.

```
<Switch> system-view
[Switch] rip
[Switch-rip-1] maximum load-balancing 2
```

Related commands

max-ecmp-num

3.1.14. network

Use **network** to enable RIP on an interface attached to a specified network.

Use **undo network** to disable RIP on an interface attached to a specified network.

Syntax

network *network-address* [*wildcard-mask*]

undo network *network-address*

Default

RIP is disabled on an interface.

Views

RIP view

Predefined user roles

network-admin

Parameters

network-address: Specifies a subnet address where an interface resides.

wildcard-mask: Specifies an IP address wildcard mask. A wildcard mask can be thought of as a subnet mask, with 1s and 0s inverted. For example, a wildcard mask of 255.255.255.0

corresponds to a subnet mask of 0.0.0.255. If you do not specify this argument, the command uses the natural mask.

Usage guidelines

RIP runs only on an interface attached to the specified network, which can be configured with a wildcard mask. An interface not on the specified network does not receive or send RIP routes, or advertise its direct routes.

For a single RIP process, the **network** 0.0.0.0 command can enable RIP on all interfaces. If multiple RIP processes exist, the command is not applicable.

If a physical interface is attached to multiple networks, you cannot advertise these networks in different RIP processes.

Examples

Enable RIP process 100 on the interface attached to the network 129.102.0.0.

```
<Switch> system-view
[Switch] rip 100
[Switch-rip-100] network 129.102.0.0
```

3.1.15. non-stop-routing

MEMO:

non-stop-routing command is supported from later software, including Version 7.2.16.

Use **non-stop-routing** to enable RIP NSR.

Use **undo non-stop-routing** to disable RIP NSR.

Syntax

non-stop-routing

undo non-stop-routing

Default

RIP NSR is disabled.

Views

RIP view

Predefined user roles

network-admin

Usage guidelines

RIP NSR enabled for a RIP process takes effect only on that process. As a best practice, enable RIP NSR for each process if multiple RIP processes exist.

The **non-stop-routing** command and the **graceful-restart** command are mutually exclusive.

Examples

Enable NSR for RIP process 1.

```
<Switch> system-view
[Switch] rip 1
[Switch-rip-1] non-stop-routing
```

3.1.16. output-delay

Use **output-delay** to set the rate at which an interface sends RIP packets.

Use **undo output-delay** to restore the default.

Syntax

output-delay *time* **count** *count*

undo output-delay

Default

An interface sends up to three RIP packets every 20 milliseconds.

Views

RIP view

Predefined user roles

network-admin

Parameters

time: Specifies the sending interval in the range of 10 to 100 milliseconds.

count: Specifies the maximum number of RIP packets sent at each interval, in the range of 1 to 30.

Examples

Configure all interfaces running RIP process 1 to send up to 10 RIP packets every 60 milliseconds.

```
<Switch> system-view
[Switch] rip 1
[Switch-rip-1] output-delay 60 count 10
```

3.1.17. peer

Use **peer** to specify a RIP neighbor in the NBMA network, where routing updates destined for the neighbor are only unicasts and not multicast or broadcast.

Use **undo peer** to remove a RIP neighbor.

Syntax

peer *ip-address*

undo peer *ip-address*

Default

RIP does not unicast updates to any neighbor.

Views

RIP view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the IP address of a RIP neighbor, in dotted decimal notation.

Usage guidelines

Do not use the **peer** *ip-address* command when the neighbor is directly connected. Otherwise, the neighbor might receive both unicast and multicast (or broadcast) messages with the same routing information.

This command must be executed together with the **undo validate-source-address** command, which disables source IP address check on inbound RIP routing updates.

Examples

Configure RIP to unicast updates to peer 202.38.165.1.

```
<Switch> system-view
[Switch] rip 1
[Switch-rip-1] peer 202.38.165.1
```

Related commands

validate-source-address

3.1.18. preference

Use **preference** to specify a preference for RIP routes.

Use **undo preference** to restore the default.

Syntax

preference { *preference* | **route-policy** *route-policy-name* } *

undo preference

Default

The preference of RIP routes is 100.

Views

RIP view

Predefined user roles

network-admin

Parameters

preference: Specifies a preference for RIP routes, in the range of 1 to 255. The smaller the value, the higher the preference.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters.

Usage guidelines

You can specify a routing policy by using the keyword **route-policy** to set a preference for matching RIP routes.

- The preference set by the routing policy applies to all matching RIP routes. The preference of other routes is set by the **preference** command.
- If no preference is set by the routing policy, the preference of all RIP routes is set by the **preference** command.

Examples

Set a preference of 120 for RIP routes.

```
<Switch> system-view
[Switch] rip 1
[Switch-rip-1] preference 120
```

3.1.19. reset rip process

Use **reset rip process** to reset a RIP process.

Syntax

reset rip *process-id* **process**

Views

User view

Predefined user roles

network-admin

Parameters

process-id: Specifies a RIP process by its ID in the range of 1 to 65535.

Usage guidelines

After executing the command, you are prompted to confirm the operation.

Examples

Reset RIP process 100.

```
<Switch> reset rip 100 process
Reset RIP process? [Y/N]:y
```

3.1.20. reset rip statistics

Use **reset rip statistics** to clear statistics for a RIP process.

Syntax

reset rip *process-id* **statistics**

Views

User view

Predefined user roles

network-admin

Parameters

process-id: Specifies a RIP process by its ID in the range of 1 to 65535.

Examples

Clear statistics for RIP process 100.

```
<Switch> reset rip 100 statistics
```

3.1.21. rip

Use **rip** to enable RIP and enter RIP view.

Use **undo rip** to disable RIP.

Syntax

rip [*process-id*] [**vpn-instance** *vpn-instance-name*]

undo rip [*process-id*]

Default

RIP is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

process-id: Specifies a RIP process by its ID in the range of 1 to 65535. The default is 1.

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the RIP process runs on the public network.

Usage guidelines

You must enable a RIP process before configuring global parameters for it. This restriction does not apply to configuring interface parameters.

If you disable a RIP process, the configured interface parameters become invalid.

Examples

Enable RIP process 1 and enter RIP view.

```
<Switch> system-view
[Switch] rip
[Switch-rip-1]
```

3.1.22. rip authentication-mode

Use **rip authentication-mode** to configure RIPv2 authentication.

Use **undo rip authentication-mode** to restore the default.

Syntax

rip authentication-mode { **md5** { **rfc2082** { **cipher** | **plain** } *string key-id* | **rfc2453** { **cipher** | **plain** } *string* } | **simple** { **cipher** | **plain** } *string* }

undo rip authentication-mode

Default

RIPv2 authentication is not configured.

Views

Interface view

Predefined user roles

network-admin

Parameters

md5: Specifies the MD5 authentication.

rfc2082: Uses the message format defined in RFC 2082.

cipher: Specifies a password in encrypted form.

plain: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 16 characters. Its encrypted form is a case-sensitive string of 33 to 53 characters.

key-id: Specifies the key ID in the range of 1 to 255.

rfc2453: Uses the message format defined in RFC 2453 (IETF standard).

simple: Specifies the simple authentication mode.

Usage guidelines

A newly configured key overwrites the old one, if any.

Although you can specify an authentication mode for RIPv1 in interface view, the configuration does not take effect because RIPv1 does not support authentication.

Examples

Configure MD5 authentication on VLAN-interface 10 and specify a plaintext key **rose** in the format defined in RFC 2453.

```
<Switch> system-view
[Switch] interface vlan-interface 10
[Switch-Vlan-interface10] rip version 2
[Switch-Vlan-interface10] rip authentication-mode md5 rfc2453 plain rose
```

Related commands

rip version

3.1.23. rip bfd enable

Use **rip bfd enable** to enable BFD for RIP on an interface.

Use **undo rip bfd enable** to restore the default.

Syntax

rip bfd enable

undo rip bfd enable

Default

BFD for RIP is disabled on an interface.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

RIP supports BFD echo-mode detection for a directly connected neighbor, and BFD control-mode detection for an indirectly neighbor.

BFD echo-mode detection only applies to a RIP neighbor one hop away.

Using the **undo peer** command does not delete the neighbor relationship immediately and cannot bring down the BFD session immediately.

Examples

Enable BFD for RIP on VLAN-interface 11.

```
<Switch> system-view
[Switch] interface vlan-interface 11
[Switch-Vlan-interface11] rip bfd enable
```

3.1.24. rip default-route

Use **rip default-route** to configure a RIP interface to advertise a default route with a specified metric.

Use **undo rip default-route** to disable a RIP interface from sending a default route.

Syntax

rip default-route { { **only** | **originate** } [**cost** *cost-value*] * | **no-originate** }

undo rip default-route

Default

A RIP interface advertises a default route if the RIP process that the interface runs is enabled to advertise a default route.

Views

Interface view

Predefined user roles

network-admin

Parameters

only: Advertises only a default route.

originate: Advertises both a default route and other routes.

cost-value: Specifies a cost for the default route, in the range of 1 to 15. The default is 1.

no-originate: Advertises only non-default routes.

Usage guidelines

An interface that is enabled to advertise a default route does not receive any default route from RIP neighbors.

Examples

Configure VLAN-interface 10 to advertise only a default route with a metric of 2.

```
<Switch> system-view
[Switch] interface vlan-interface 10
```

```
[Switch-Vlan-interface10] rip default-route only cost 2
```

Configure VLAN-interface 10 to advertise a default route with a metric of 2 and other routes.

```
<Switch> system-view
[Switch] interface vlan-interface 10
[Switch-Vlan-interface10] rip default-route originate cost 2
```

Related commands

default-route

3.1.25. rip input

Use **rip input** to enable an interface to receive RIP messages.

Use **undo rip input** to disable an interface from receiving RIP messages.

Syntax

rip input

undo rip input

Default

An interface is enabled to receive RIP messages.

Views

Interface view

Predefined user roles

network-admin

Examples

Disable VLAN-interface 10 from receiving RIP messages.

```
<Switch> system-view
[Switch] interface vlan-interface 10
[Switch-Vlan-interface10] undo rip input
```

3.1.26. rip metricin

Use **rip metricin** to configure an interface to add a metric to inbound routes.

Use **undo rip metricin** to restore the default.

Syntax

rip metricin [**route-policy** *route-policy-name*] *value*

undo rip metricin

Default

The additional metric of an inbound route is 0.

Views

Interface view

Predefined user roles

network-admin

Parameters

route-policy *route-policy-name*: Specifies a routing policy by its name, a case sensitive string of 1 to 63 characters. If you specify this option, the command adds an additional metric for the routes that match the routing policy.

value: Adds an additional metric to inbound routes, in the range of 0 to 16.

Usage guidelines

When a valid RIP route is received, the system adds a metric to it and then installs it into the routing table. The metric of the route received on the configured interface is then increased. If the sum of the additional metric and the original metric is greater than 16, the metric of the route will be 16.

If a routing policy is referenced with the **route-policy** keyword, the following operations can be performed:

- Routes matching the policy are added with the metric specified in the **apply cost** command configured in the policy. Routes not matching it are added with the metric specified in the **rip metricin** command. The **rip metricin** command does not support specifying the **+** or **–** keyword in the **apply cost** command to add or reduce a metric.
- If the **apply cost** command is not configured in the policy, all the inbound routes are added with the metric specified in the **rip metricin** command.

Examples

Configure VLAN-interface 10 to add a metric of 6 to the inbound route 1.0.0.0/8 and to add a metric of 2 to other inbound routes.

```
<Switch> system-view
[Switch] ip prefix-list 123 permit 1.0.0.0 8
[Switch] route-policy abc permit node 10
[Switch-route-policy-abc-10] if-match ip address prefix-list 123
[Switch-route-policy-abc-10] apply cost 6
[Switch-route-policy-abc-10] quit
[Switch] interface vlan-interface 10
[Switch-Vlan-interface10] rip metricin route-policy abc 2
```

Related commands

apply cost

3.1.27. rip metricout

Use **rip metricout** to configure an interface to add a metric to outbound routes.

Use **undo rip metricout** to restore the default.

Syntax

rip metricout [**route-policy** *route-policy-name*] *value*

undo rip metricout

Default

The additional metric for outbound routes is 1.

Views

Interface view

Predefined user roles

network-admin

Parameters

route-policy *route-policy-name*: Specifies a routing policy by its name, a case sensitive string of 1 to 63 characters. If you specify this option, the command adds an additional metric for the routes that match the routing policy.

value: Adds an additional metric to outbound routes, in the range of 1 to 16.

Usage guidelines

With the command configured on an interface, the metric of RIP routes sent on the interface will be increased.

If a routing policy is referenced with the **route-policy** keyword, the following operations can be performed:

- Routes matching the policy is added with the metric specified in the **apply cost** command configured in the policy. Routes not matching it are added with the metric specified in the **rip metricout** command. The **rip metricout** command does not support specifying the **+** or **–** keyword in the **apply cost** command to add or reduce a metric.
- If the **apply cost** command is not configured in the policy, all the outbound routes are added with the metric specified in the **rip metricout** command.

Examples

Configure VLAN-interface 10 to add a metric of 6 to the outbound route 1.0.0.0/8 and to add a metric of 2 to other outbound routes.

```
<Switch> system-view
[Switch] ip prefix-list 123 permit 1.0.0.0 8
[Switch] route-policy abc permit node 10
[Switch-route-policy-abc-10] if-match ip address prefix-list 123
```

```
[Switch-route-policy-abc-10] apply cost 6
[Switch-route-policy-abc-10] quit
[Switch] interface vlan-interface 10
[Switch-Vlan-interface10] rip metricout route-policy abc 2
```

Related commands

apply cost

3.1.28. rip mib-binding

Use **rip mib-binding** to bind a RIP process to MIB.

Use **undo rip mib-binding** to restore the default.

Syntax

rip mib-binding *process-id*

undo rip mib-binding

Default

MIB operation is bound to the RIP process with the smallest process ID.

Views

System view

Predefined user roles

network-admin

Parameters

process-id: Specifies a RIP process by its ID in the range of 1 to 65535.

Usage guidelines

If the specified process ID does not exist, the MIB binding configuration does not take effect.

Deleting a RIP process bound to MIB operation deletes the MIB binding configuration. After the RIP process is deleted, MIB operation is bound to the RIP process with the smallest process ID.

Examples

Bind RIP process 100 to MIB.

```
<Switch> system-view
[Switch] rip mib-binding 100
```

3.1.29. rip output

Use **rip output** to enable an interface to send RIP messages.

Use **undo rip output** to disable an interface from sending RIP messages.

Syntax

rip output

undo rip output

Default

An interface sends RIP messages.

Views

Interface view

Predefined user roles

network-admin

Examples

Disable VLAN-interface 10 from sending RIP messages.

```
<Switch> system-view
[Switch] interface vlan-interface 10
[Switch-Vlan-interface10] undo rip output
```

3.1.30. rip poison-reverse

Use **rip poison-reverse** to enable the poison reverse feature.

Use **undo rip poison-reverse** to disable the poison reverse feature.

Syntax

rip poison-reverse

undo rip poison-reverse

Default

The poison reverse feature is disabled.

Views

Interface view

Predefined user roles

network-admin

Examples

Enable the poison reverse feature on VLAN-interface 10.

```
<Switch> system-view
[Switch] interface vlan-interface 10
[Switch-Vlan-interface10] rip poison-reverse
```

3.1.31. rip split-horizon

Use **rip split-horizon** to enable the split horizon feature.

Use **undo rip split-horizon** to disable the split horizon feature.

Syntax

rip split-horizon

undo rip split-horizon

Default

The split horizon feature is enabled.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

- The split horizon feature prevents routing loops. If you want to disable the feature, make sure the operation is necessary.
- If both split horizon and poison reverse are enabled, only the poison reverse feature takes effect.

Examples

Enable the split horizon feature on VLAN-interface 10.

```
<Switch> system-view
[Switch] interface vlan-interface 10
[Switch-Vlan-interface10] rip split-horizon
```

3.1.32. rip summary-address

Use **rip summary-address** to configure a summary route on an interface.

Use **undo rip summary-address** to remove a summary route on an interface.

Syntax

rip summary-address *ip-address* { *mask-length* | *mask* }

undo rip summary-address *ip-address* { *mask-length* | *mask* }

Default

No summary route is configured on an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the destination IP address of the summary route.

mask-length: Specifies the subnet mask length of the summary route, in the range of 0 to 32.

mask: Specifies the subnet mask of the summary route, in dotted decimal notation.

Usage guidelines

This command takes effect only when automatic route summarization is disabled.

Examples

Configure a summary route on VLAN-interface 10.

```
<Switch> system-view
[Switch] interface vlan-interface 10
[Switch-Vlan-interface10] rip summary-address 10.0.0.0 255.255.255.0
```

Related commands

summary

3.1.33. rip version

Use **rip version** to specify a RIP version on an interface.

Use **undo rip version** to restore the default.

Syntax

rip version { **1** | **2** [**broadcast** | **multicast**] }

undo rip version

Default

No RIP version is configured on an interface. The interface can send RIPv1 broadcasts, and receive RIPv1 broadcasts and unicasts, and RIPv2 broadcasts, multicasts, and unicasts.

Views

Interface view

Predefined user roles

network-admin

Parameters

1: Specifies the RIP version as RIPv1.

2: Specifies the RIP version as RIPv2.

[**broadcast** | **multicast**]: Sends RIPv2 messages in broadcast mode or multicast mode (default).

Usage guidelines

If an interface has no RIP version configured, it uses the global RIP version. Otherwise, it uses the RIP version configured on it.

An interface running RIPv1 can perform the following operations:

- Sends RIPv1 broadcast messages.
- Receives RIPv1 broadcast and unicast messages.

An interface running RIPv2 in broadcast mode can perform the following operations:

- Sends RIPv2 broadcast messages.
- Receives RIPv1 broadcast and unicast messages, and RIPv2 broadcast, multicast, and unicast messages.

An interface running RIPv2 in multicast mode can perform the following operations:

- Sends RIPv2 multicast messages.
- Receives RIPv2 broadcast, multicast, and unicast messages.

Only a limited number of broadcasts can be received and processed by both RIPv1 and RIPv2. It is limited broadcast only. RIP packets for other broadcasts (local/direct) cannot be processed.

Examples

Configure RIPv2 in broadcast mode on VLAN-interface 10.

```
<Switch> system-view
[Switch] interface vlan-interface 10
[Switch-Vlan-interface10] rip version 2 broadcast
```

Related commands

version

3.1.34. silent-interface

Use **silent-interface** to disable interfaces from sending RIP messages. The interfaces can still receive RIP messages.

Use **undo silent-interface** to enable interfaces to send RIP messages.

Syntax

silent-interface { *interface-type interface-number* | **all** }

undo silent-interface { *interface-type interface-number* | **all** }

Default

All RIP interfaces can send RIP messages.

Views

RIP view

Predefined user roles

network-admin

Parameters

interface-type interface-number: Disables a specified interface from sending RIP messages.

all: Disables all interfaces from sending RIP messages.

Examples

Disable all VLAN interfaces from sending RIP messages except VLAN-interface 10.

```
<Switch> system-view
[Switch] rip 100
[Switch-rip-100] silent-interface all
[Switch-rip-100] undo silent-interface vlan-interface 10
[Switch-rip-100] network 131.108.0.0
```

3.1.35. summary

Use **summary** to enable automatic RIPv2 route summarization. Natural masks are used to advertise summary routes to reduce the size of routing tables.

Use **undo summary** to disable automatic RIPv2 route summarization to advertise all subnet routes.

Syntax

summary

undo summary

Default

Automatic RIPv2 route summarization is enabled.

Views

RIP view

Predefined user roles

network-admin

Usage guidelines

Automatic RIPv2 route summarization can reduce the routing table size to enhance the scalability and efficiency for large networks.

Examples

Disable automatic RIPv2 route summarization.

```
<Switch> system-view
[Switch] rip
[Switch-rip-1] undo summary
```

Related commands

rip summary-address

rip version

3.1.36. timers

Use **timers** to set RIP timers.

Use **undo timers** to restore the default.

Syntax

timers { **garbage-collect** *garbage-collect-value* | **suppress** *suppress-value* | **timeout** *timeout-value* | **update** *update-value* } *

undo timers { **garbage-collect** | **suppress** | **timeout** | **update** } *

Default

The garbage-collect timer is 120 seconds, the suppress timer is 120 seconds, the timeout timer is 180 seconds, and the update timer is 30 seconds.

Views

RIP view

Predefined user roles

network-admin

Parameters

garbage-collect-value: Specifies the garbage-collect timer in the range of 1 to 3600 seconds.

suppress-value: Specifies the suppress timer in the range of 0 to 3600 seconds.

timeout-value: Specifies the timeout timer in the range of 1 to 3600 seconds.

update-value: Specifies the update timer in the range of 1 to 3600 seconds.

Usage guidelines

RIP uses the following timers:

- **Update timer**—Specifies the interval between routing updates.
- **Timeout timer**—Specifies the route aging time. If no update for a route is received before the timer expires, RIP sets the metric of the route to 16.
- **Suppress timer**—Specifies how long a RIP route stays in suppressed state. When the metric of a route becomes 16, the route enters the suppressed state. If RIP receives an update for the route with a metric less than 16 from the same neighbor, RIP uses this route to replace the suppressed route.

- **Garbage-collect timer**—Specifies the interval from when the metric of a route becomes 16 to when it is deleted from the routing table. During the garbage-collect timer length, RIP advertises the route with a metric of 16. If no update is announced for that route before the garbage-collect timer expires, RIP deletes the route from the routing table.

As a best practice, do not change the default values of these timers.

The timer lengths must be consistent on all routers on the network.

The timeout timer must be greater than the update timer.

Examples

Set the update, timeout, suppress, and garbage-collect timers to 5, 15, 15, and 30 seconds.

```
<Switch> system-view
[Switch] rip 100
[Switch-rip-100] timers update 5 timeout 15 suppress 15 garbage-collect 30
```

3.1.37. validate-source-address

Use **validate-source-address** to enable source IP address check on inbound RIP routing updates.

Use **undo validate-source-address** to disable source IP address check on inbound RIP routing updates.

Syntax

validate-source-address

undo validate-source-address

Default

Source IP address check on inbound RIP routing updates is enabled.

Views

RIP view

Predefined user roles

network-admin

Examples

Disable source IP address check on inbound RIP routing updates.

```
<Switch> system-view
[Switch-rip] rip 100
[Switch-rip-100] undo validate-source-address
```

3.1.38. version

Use **version** to specify a global RIP version.

Use **undo version** to restore the default.

Syntax

version { **1** | **2** }

undo version

Default

No global RIP version is configured. An RIP interface can send RIPv1 broadcasts and receive RIPv1 broadcasts and unicasts, and RIPv2 broadcasts, multicasts, and unicasts.

Views

RIP view

Predefined user roles

network-admin

Parameters

1: Specifies the RIP version as RIPv1.

2: Specifies the RIP version as RIPv2. RIPv2 messages are multicast.

Usage guidelines

An interface prefers the RIP version configured on it over the global RIP version.

If no RIP version is specified for the interface and the global version is RIPv1, the interface uses RIPv1 and can perform the following operations:

- Send RIPv1 broadcasts.
- Receive RIPv1 broadcasts and unicasts.

If no RIP version is specified for the interface and the global version is RIPv2, the interface uses RIPv2 multicast mode and can perform the following operations:

- Send RIPv2 multicasts.
- Receive RIPv2 broadcasts, multicasts, and unicasts.

Examples

Specify the global RIP version as RIPv2.

```
<Switch> system-view
[Switch] rip 100
[Switch-rip-100] version 2
```

Related commands

rip version

Contents

A page of this section is **5-x-x**

4. OSPF commands ····· 4-1
4.1. OSPF commands ····· 4-1
4.1.1. abr-summary (OSPF area view) ····· 4-1
4.1.2. area (OSPF view) ····· 4-2
4.1.3. asbr-summary (OSPF view) ····· 4-2
4.1.4. authentication-mode ····· 4-4
4.1.5. bandwidth-reference (OSPF view) ····· 4-5
4.1.6. default (OSPF view) ····· 4-6
4.1.7. default-cost (OSPF area view) ····· 4-7
4.1.8. default-route-advertise (OSPF view) ····· 4-8
4.1.9. description (OSPF/OSPF area view) ····· 4-9
4.1.10. display ospf ····· 4-10
4.1.11. display ospf abr-asbr ····· 4-17
4.1.12. display ospf abr-summary ····· 4-18
4.1.13. display ospf asbr-summary ····· 4-21
4.1.14. display ospf event-log ····· 4-22
4.1.15. display ospf graceful-restart ····· 4-27
4.1.16. display ospf interface ····· 4-30
4.1.17. display ospf lsdb ····· 4-32
4.1.18. display ospf nexthop ····· 4-35
4.1.19. display ospf peer ····· 4-36
4.1.20. display ospf peer statistics ····· 4-39
4.1.21. display ospf request-queue ····· 4-40
4.1.22. display ospf retrans-queue ····· 4-42
4.1.23. display ospf routing ····· 4-43
4.1.24. display ospf statistics ····· 4-47
4.1.25. display ospf vlink ····· 4-51
4.1.26. display router id ····· 4-52
4.1.27. dscp ····· 4-53
4.1.28. enable link-local-signaling ····· 4-53
4.1.29. enable out-of-band-resynchronization ····· 4-54
4.1.30. event-log ····· 4-54
4.1.31. fast-reroute (OSPF view) ····· 4-55
4.1.32. filter (OSPF area view) ····· 4-56
4.1.33. filter-policy export (OSPF view) ····· 4-57
4.1.34. filter-policy import (OSPF view) ····· 4-58
4.1.35. graceful-restart (OSPF view) ····· 4-60
4.1.36. graceful-restart helper enable ····· 4-61
4.1.37. graceful-restart helper strict-lsa-checking ····· 4-62
4.1.38. graceful-restart interval (OSPF view) ····· 4-63
4.1.39. host-advertise ····· 4-63
4.1.40. import-route (OSPF view) ····· 4-64
4.1.41. log-peer-change ····· 4-66
4.1.42. lsa-arrival-interval ····· 4-67
4.1.43. lsa-generation-interval ····· 4-68
4.1.44. lsdb-overflow-interval ····· 4-69
4.1.45. lsdb-overflow-limit ····· 4-70
4.1.46. maximum load-balancing (OSPF view) ····· 4-70
4.1.47. non-stop-routing ····· 4-71
4.1.48. network (OSPF area view) ····· 4-72
4.1.49. nssa (OSPF area view) ····· 4-73
4.1.50. opaque-capability enable ····· 4-74

4.1.51. ospf ····· 4-74
4.1.52. ospf authentication-mode ····· 4-75
4.1.53. ospf bfd enable ····· 4-77
4.1.54. ospf cost (interface view) ····· 4-78
4.1.55. ospf dr-priority ····· 4-78
4.1.56. ospf mib-binding ····· 4-79
4.1.57. ospf mtu-enable ····· 4-80
4.1.58. ospf network-type ····· 4-81
4.1.59. ospf peer sub-address enable ····· 4-82
4.1.60. ospf timer dead ····· 4-83
4.1.61. ospf timer hello ····· 4-84
4.1.62. ospf timer poll ····· 4-85
4.1.63. ospf timer retransmit ····· 4-86
4.1.64. ospf trans-delay ····· 4-86
4.1.65. peer (OSPF view) ····· 4-87
4.1.66. preference (OSPF view) ····· 4-88
4.1.67. reset ospf event-log ····· 4-89
4.1.68. reset ospf process ····· 4-90
4.1.69. reset ospf redistribution ····· 4-91
4.1.70. reset ospf statistics ····· 4-91
4.1.71. rfc1583 compatible ····· 4-92
4.1.72. router id ····· 4-92
4.1.73. silent-interface (OSPF view) ····· 4-93
4.1.74. snmp-agent trap enable ospf ····· 4-94
4.1.75. spf-schedule-interval (OSPF view) ····· 4-96
4.1.76. stub (OSPF area view) ····· 4-97
4.1.77. stub-router (OSPF view) ····· 4-98
4.1.78. transmit-pacing ····· 4-99
4.1.79. vlink-peer (OSPF area view) ····· 4-99

4. OSPF commands

4.1. OSPF commands

4.1.1. abr-summary (OSPF area view)

Use **abr-summary** to configure route summarization on an ABR.

Use **undo abr-summary** to remove the configuration.

Syntax

abr-summary *ip-address* { *mask-length* | *mask* } [**advertise** | **not-advertise**] [**cost** *cost-value*]

undo abr-summary *ip-address* { *mask-length* | *mask* }

Default

Route summarization is not configured on an ABR.

Views

OSPF area view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the destination IP address of the summary route in dotted decimal notation.

mask-length: Specifies the mask length in the range of 0 to 32.

mask: Specifies the mask of the IP address, in dotted decimal notation.

advertise | **not-advertise**: Advertises the summary route or not. By default, the command advertises the summary route.

cost *cost-value*: Specifies the cost of the summary route, in the range of 1 to 16777215. The default cost is the largest cost value among routes that are summarized.

Usage guidelines

This command applies only to an ABR to summarize multiple contiguous networks into one network.

To enable ABR to advertise specific routes that have been summarized, use the **undo abr-summary** command.

Examples

Summarize networks 36.42.10.0/24 and 36.42.110.0/24 in Area 1 into 36.42.0.0/16.

```
<Switch> system-view
[Switch] ospf 100
[Switch-ospf-100] area 1
[Switch-ospf-100-area-0.0.0.1] network 36.42.10.0 0.0.0.255
[Switch-ospf-100-area-0.0.0.1] network 36.42.110.0 0.0.0.255
[Switch-ospf-100-area-0.0.0.1] abr-summary 36.42.0.0 255.255.0.0
```

4.1.2. area (OSPF view)

Use **area** to create an OSPF area and enter OSPF area view.

Use **undo area** to remove an OSPF area.

Syntax

area *area-id*

undo area *area-id*

Default

No OSPF areas exist.

Views

OSPF view

Predefined user roles

network-admin

Parameters

area-id: Specifies an area by its ID, an IP address or a decimal integer in the range of 0 to 4294967295 that is translated into the IP address format.

Examples

Create Area 0 and enter Area 0 view.

```
<Switch> system-view
[Switch] ospf 100
[Switch-ospf-100] area 0
[Switch-ospf-100-area-0.0.0.0]
```

4.1.3. asbr-summary (OSPF view)

Use **asbr-summary** to configure route summarization on an ASBR.

Use **undo asbr-summary** to remove the configuration.

Syntax

asbr-summary *ip-address* { *mask-length* | *mask* } [**cost** *cost-value* | **not-advertise** | **nssa-only** | **tag** *tag*] *

undo asbr-summary *ip-address* { *mask-length* | *mask* }

Default

Route summarization is not configured on an ASBR.

Views

OSPF view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the destination IP address of the summary route.

mask-length: Specifies the mask length in the range of 0 to 32.

mask: Specifies the mask in dotted decimal notation.

cost *cost-value*: Specifies the cost of the summary route, in the range of 1 to 16777214. If you do not specify this option, the largest cost among the summarized routes applies. If the routes in Type-5 LSAs translated from Type-7 LSAs are Type-2 external routes, the largest cost among the summarized routes plus 1 applies.

not-advertise: Disables advertising the summary route. If you do not specify this keyword, the command advertises the route.

nssa-only: Limits the route advertisement to the NSSA area by setting the P-bit of Type-7 LSAs to 0. By default, the P-bit of Type-7 LSAs is set to 1. If the ASBR is also an ABR and **FULL** state neighbors exist in the backbone area, the P-bit of Type-7 LSAs originated by the ASBR is set to 0. This keyword applies to the NSSA ASBR.

tag *tag*: Specifies a tag for the summary route, in the range of 0 to 4294967295. The default is 1. The tag can be used by a routing policy to control summary route advertisement.

Usage guidelines

An ASBR can summarize routes in the following LSAs:

- Type-5 LSAs.
- Type-7 LSAs in an NSSA area.
- Type-5 LSAs translated by the ASBR (also an ABR) from Type-7 LSAs in an NSSA area.

  If the ASBR (ABR) is not a translator, it cannot summarize routes in Type-5 LSAs translated from Type-7 LSAs.

To enable ASBR to advertise specific routes that have been summarized, use the **undo asbr-summary** command.

Examples

Summarize redistributed static routes into a single route, and specify a tag value of 2 and a cost of 100 for the summary route.

```
<Switch> system-view
[Switch] ip route-static 10.2.1.0 24 null 0
[Switch] ip route-static 10.2.2.0 24 null 0
[Switch] ospf 100
[Switch-ospf-100] import-route static
[Switch-ospf-100] asbr-summary 10.2.0.0 255.255.0.0 tag 2 cost 100
```

4.1.4. authentication-mode

Use **authentication-mode** to specify an authentication mode for an OSPF area.

Use **undo authentication-mode** to remove the configuration.

Syntax

For MD5/HMAC-MD5 authentication:

authentication-mode { **hmac-md5** | **md5** } *key-id* { **cipher** | **plain** } *string*

undo authentication-mode [{ **hmac-md5** | **md5** } *key-id*]

For simple authentication:

authentication-mode simple { **cipher** | **plain** } *string*

undo authentication-mode

Default

No authentication is performed for an area.

Views

OSPF area view

Predefined user roles

network-admin

Parameters

hmac-md5: Specifies the HMAC-MD5 authentication mode.

md5: Specifies the MD5 authentication mode.

simple: Specifies the simple authentication mode.

key-id: Specifies a key by its ID in the range of 0 to 255.

cipher: Specifies a key in encrypted form.

plain: Specifies a key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. This argument is case sensitive.

- In simple authentication mode, the plaintext form of the key is a string of 1 to 8 characters. The encrypted form of the key is a string of 33 to 41 characters.
- In MD5/HMAC-MD5 authentication mode, the plaintext form of the key is a string of 1 to 16 characters. The encrypted form of the key is a string of 33 to 53 characters.

Usage guidelines

To establish or maintain adjacencies, routers in the same area must have the same authentication mode and key.

If MD5 or HMAC-MD5 authentication is configured, you can configure multiple keys, each having a unique key ID and key string. As a best practice to minimize the risk of key compromise, use only one key for an area and delete the old key after key replacement.

To replace the key used for MD5 or HMAC-MD5 authentication in an area, you must configure the new key before removing the old key from each router. OSPF uses the key rollover mechanism to ensure that the routers can pass authentication before the replacement is complete across the area. After you configure a new key on a router, the router sends copies of the same packet, each authenticated by a different key, including the new key and the keys in use. This practice continues until the router detects that all its neighbors have the new key.

The authentication algorithm can only be MD5 or HMAC-MD5 and the ID of keys used for authentication can only be in the range of 0 to 255.

Examples

Configure OSPF Area 0 to use the MD5 authentication mode, and set the key ID to 15 and the key to **abc** in plaintext form.

```
<Switch> system-view
[Switch] ospf 100
[Switch-ospf-100] area 0
[Switch-ospf-100-area-0.0.0.0] authentication-mode md5 15 plain abc
```

Related commands

ospf authentication-mode

4.1.5. bandwidth-reference (OSPF view)

Use **bandwidth-reference** to set a reference bandwidth value for link cost calculation.

Use **undo bandwidth-reference** to restore the default value.

Syntax

bandwidth-reference *value*

undo bandwidth-reference

Default

The reference bandwidth value is 100 Mbps for link cost calculation.

Views

OSPF view

Predefined user roles

network-admin

Parameters

value: Specifies the reference bandwidth value for link cost calculation, in the range of 1 to 4294967 Mbps.

Usage guidelines

If no cost values are configured for links, OSPF calculates their cost values by using the following formula: Cost = Reference bandwidth value(100 Mbps) / Expected interface bandwidth(Mbps). If the calculated cost is greater than 65535, the value of 65535 is used. If the calculated cost is less than 1, the value of 1 is used.

Examples

Set the reference bandwidth value to 1000 Mbps.

```
<Switch> system-view
[Switch] ospf 100
[Switch-ospf-100] bandwidth-reference 1000
```

Related commands

ospf cost

4.1.6. default (OSPF view)

Use **default** to configure default parameters for redistributed routes.

Use **undo default** to remove the configuration.

Syntax

default { **cost** *cost-value* | **tag** *tag* | **type** *type* } *

undo default { **cost** | **tag** | **type** } *

Default

The cost is 1, the tag is 1, and the route type is 2.

Views

OSPF view

Predefined user roles

network-admin

Parameters

cost *cost-value*: Specifies a default cost for redistributed routes, in the range of 0 to 16777214.

tag *tag*: Specifies a tag for redistributed routes, in the range of 0 to 4294967295.

type *type*: Specifies a type for redistributed routes: 1 or 2.

Examples

Set the default cost, tag, and type to 10, 100, and 2 for redistributed external routes.

```
<Switch> system-view
[Switch] ospf 100
[Switch-ospf-100] default cost 10 tag 100 type 2
```

Related commands

import-route

4.1.7. default-cost (OSPF area view)

Use **default-cost** to set a cost for the default route advertised to the stub or NSSA area.

Use **undo default-cost** to restore the default value.

Syntax

default-cost *cost-value*

undo default-cost

Default

The cost is 1.

Views

OSPF area view

Predefined user roles

network-admin

Parameters

cost-value: Specifies a cost for the default route advertised to the Stub or NSSA area, in the range of 0 to 16777214.

Usage guidelines

This command takes effect only on the ABR of a stub area or the ABR or ASBR of an NSSA area.

Examples

Configure Area 1 as a stub area, and set the cost of the default route advertised to the stub area to 20.

```
<Switch> system-view
[Switch] ospf 100
```

```
[Switch-ospf-100] area 1
[Switch-ospf-100-area-0.0.0.1] stub
[Switch-ospf-100-area-0.0.0.1] default-cost 20
```

Related commands

nssa

stub

4.1.8. default-route-advertise (OSPF view)

Use **default-route-advertise** to redistribute a default route into the OSPF routing domain.

Use **undo default-route-advertise** to restore the default.

Syntax

default-route-advertise [**always** | **permit-calculate-other** | **cost** *cost-value* | **route-policy** *route-policy-name* | **type** *type*] *

default-route-advertise [**summary cost** *cost-value*]

undo default-route-advertise

Default

No default route is redistributed into the OSPF routing domain.

Views

OSPF view

Predefined user roles

network-admin

Parameters

always: Redistributes a default route in a Type-5 LSA into the OSPF routing domain regardless of whether a default route exists in the routing table. If you do not specify this keyword, the router redistributes a default route only when an active default route that does not belong to the current OSPF process exists in the IP routing table.

permit-calculate-other: Enables OSPF to calculate default routes received from other routers. If you do not specify this keyword, OSPF does not calculate default routes from other routers. If the router does not redistribute any default route in a Type-5 LSA into the OSPF routing domain, the router calculates default routes from other routers. It calculates these routes regardless of whether this keyword is specified.

cost *cost-value*: Specifies a cost for the default route, in the range of 0 to 16777214. If you do not specify this option, the default cost specified by the **default-cost** command applies.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters. When the routing policy is matched and one of the

following conditions is met, the command redistributes a default route in a Type-5 LSA into the OSPF routing domain:

- A default route exists in the routing table.
- The **always** keyword is specified.

The routing policy modifies values in the Type-5 LSA.

type *type*: Specifies a type for the Type-5 LSA: 1 or 2. If you do not specify this option, the default type for the Type-5 LSA specified by the **default type** command applies.

summary: Advertises the specified default route in a Type-3 LSA. This keyword is available only for VPNs.

Usage guidelines

This command redistributes a default route in a Type-5 LSA, which cannot be redistributed with the **import-route** command. If the local routing table has no default route, you must specify the **always** keyword for the command.

The **default-route-advertise summary cost** command is applicable only to VPNs. It enables a PE router to redistribute a default external route in a Type-3 LSA to CE routers.

Examples

Redistribute a default route into the OSPF routing domain, regardless of whether the default route exists in the local routing table.

```
<Switch> system-view
[Switch] ospf 100
[Switch-ospf-100] default-route-advertise always
```

Related commands

default

import-route

4.1.9. description (OSPF/OSPF area view)

Use **description** to configure a description for an OSPF process or area.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

No description is configured for an OSPF process or area.

Views

OSPF view

OSPF area view

Predefined user roles

network-admin

Parameters

text: Specifies a description, a case-sensitive string of 1 to 80 characters.

Usage guidelines

The description specified by this command is used to identify an OSPF process or area.

Examples

Describe OSPF process 100 as **abc**.

```
<Switch> system-view
[Switch] ospf 100
[Switch-ospf-100] description abc
```

Describe OSPF Area 0 as **bone area**.

```
<Switch> system-view
[Switch] ospf 100
[Switch-ospf-100] area 0
[Switch-ospf-100-area-0.0.0.0] description bone area
```

4.1.10. display ospf

Use **display ospf** to display OSPF process information.

Syntax

display ospf [*process-id*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays information about all OSPF processes.

verbose: Displays detailed OSPF process information. If you do not specify this keyword, the command displays brief OSPF process information.

Examples

Display detailed OSPF process information.

```
<Switch> display ospf verbose
```

```
          OSPF Process 1 with Router ID 192.168.1.2
                  OSPF Protocol Information

RouterID: 192.168.1.2      Router type:  NSSA
Route tag: 0
Multi-VPN-Instance is not enabled
Ext-community type: domain ID 0x105, route type 0x8000, router ID 0x8001
Domain ID: 0.0.0.0:23
Opaque capable
Originating router-LSAs with maximum metric
   Condition: On startup for 600 seconds, State: Inactive
   Advertise stub links with maximum metric in router-LSAs
   Advertise summary-LSAs with metric 16711680
   Advertise external-LSAs with metric 16711680
ISPF is enabled
SPF-schedule-interval: 5 50 200
LSA generation interval: 5
LSA arrival interval: 1000
Transmit pacing: Interval: 20 Count: 3
Default ASE parameters: Metric: 1 Tag: 1 Type: 2
Route preference: 10
ASE route preference: 150
SPF computation count: 22
RFC 1583 compatible
Graceful restart interval: 120
SNMP trap rate limit interval: 2  Count: 300
This process is currently bound to MIB
Area count: 1   NSSA area count: 1
Normal areas with up interfaces: 0
NSSA areas with up interfaces: 1
Up interfaces: 1
ExChange/Loading neighbors: 0
Full neighbors:3
Calculation trigger type: Full
Current calculation type: SPF calculation
Current calculation phase: Calculation area topology
Process reset state: N/A
Current reset type: N/A
Next reset type: N/A
Reset prepare message replied: -/-/-/-
Reset process message replied: -/-/-/-
Reset phase of module:
  M-N/A, P-N/A, L-N/A, C-N/A, R-N/A


Area: 0.0.0.1          (MPLS TE  not enabled)
Authtype: None    Area flag: NSSA
7/5 translator state: Disabled
```

```
7/5 translate stability timer interval: 0
SPF scheduled count: 5
ExChange/Loading neighbors: 0
Up interfaces: 1

Interface: 192.168.1.2 (Vlan-interface10)
Cost: 1       State: DR        Type: Broadcast    MTU: 1500
Priority: 1
Designated router: 192.168.1.2
Backup designated router: 192.168.1.1
Timers: Hello 10 , Dead 40 , Poll  40 , Retransmit 5 , Transmit Delay 1
FRR backup: Enabled
Enabled by network configuration
Packet size: 1000
```

Table 4-1 Command output

Field	Description
OSPF Process 1 with Router ID 192.168.1.2	OSPF process ID and OSPF router ID.
RouterID	Router ID.
Router type	Router type: • ABR. • ASBR. • NSSA. • Null.
Route tag	Tag of redistributed routes.
Multi-VPN-Instance is not enabled	The OSPF process does not support multi-VPN-instance.
Ext-community type	OSPF extended community attribute type codes: • **domain ID**—Domain ID code. • **router type**—Router type code. • **router ID**—Router ID code.
Domain ID	OSPF domain ID (primary ID).
Opaque capable	Opaque LSA advertisement and reception capability is enabled.
Originating router-LSAs with maximum metric	The maximum cost value for router LSAs (excluding stub links) is used.
Condition	Status of the stub router: • Always. • On startup while BGP is converging. • On startup while BGP is converging for *xxx* seconds, where *xxx* is specified by the user. • On startup for *xxx* seconds, where *xxx* is specified by the user.
State	Whether the stub router is active.
SPF-schedule-interval	Interval for SPF calculations.

Field	Description
LSA generation interval	LSA generation interval.
LSA arrival interval	LSA arrival interval.
Transmit pacing	LSU packet transmit rate of the interface: • **Interval**—LSU transmit interval of the interface. • **Count**—Maximum number of LSU packets sent at each interval.
Default ASE parameters	Default ASE parameters: **Metric**, **Tag**, and **Type**.
Route preference	Internal route preference.
ASE route preference	External route preference.
SPF computation count	SPF computation count of the OSPF process.
RFC1583 compatible	Compatible with RFC 1583.
Graceful restart interval	GR interval.
SNMP trap rate limit interval	SNMP notification sending interval.
Count	Number of sent SNMP notifications.
ExChange/Loading neighbors	Neighbors in ExChange/Loading state.
Full neighbors	Neighbors in Full state.
Calculation trigger type	Route calculation trigger type: • **Full**—Calculation of all routes is triggered. • **Area topology change**—Topology change in an area. • **Intra router change**—Incremental intra-area route change. • **ASBR change**—Incremental ASBR route change. • **7to5 translator**—Type-7-to-Type-5 LSA translator role change. • **Full IP prefix**—Calculation of all IP prefixes is triggered. • **Full intra AS**—Calculation of all intra-AS prefixes is triggered. • **Inc intra AS**—Calculation of incremental intra-AS prefixes is triggered. • **Full inter AS**—Calculation of all AS-external prefixes is triggered. • **Inc inter AS**—Calculation of incremental AS-external prefixes is triggered. • **N/A**—Route calculation is not triggered.
Current calculation type	Current route calculation type: • SPF calculation. • **Intra router calculation**—Intra-area route calculation. • **ASBR calculation**—Inter-area ASBR route calculation. • **Inc intra router**—Incremental intra-area route calculation. • **Inc ASBR calculation**—Incremental

Field	Description
	inter-area ASBR route calculation. • **7to5 translator**—Type-7-to-Type-5 LSA calculation. • **Full intra AS**—Calculation of all intra-AS prefixes. • **Inc intra AS**—Calculation of incremental intra-AS prefixes. • **Full inter AS**—Calculation of all AS-external prefixes. • **Inc inter AS**—Calculation of incremental AS-external prefixes. • **Forward address**—Forwarding address calculation. • **N/A**—Route calculation is not triggered.
Current calculation phase	Current route calculation phase: • **Calculation area topology**—Calculating area topology. • **Calculation router**—Calculating routes on routers. • **Calculation intra AS**—Calculating intra-AS routes. • **7to5 translator**—Calculating Type-7-to-Type-5 LSAs. • **Forward address**—Calculating forwarding addresses. • **Calculation inter AS**—Calculating AS-external routes. • **Calculation end**—Ending phase of calculation. • **N/A**—Route calculation is not triggered.
Process reset state	Process reset state: • **N/A**—The process is not reset. • **Under reset**—The process is in the reset progress. • **Under RIB smooth**—The process is synchronizing the RIB.
Current reset type	Current process reset type: • **N/A**—The process is not reset. • **Normal**—Normal reset. • **GR quit**—Normal reset when GR quits abnormally. • **Delete**—Delete OSPF process. • **VPN delete**—Delete VPN.
Next reset type	Next process reset type: • **N/A**—The process is not reset. • **Normal**—Normal reset. • **GR quit**—Normal reset when GR quits abnormally. • **Delete**—Delete OSPF process.
Reset prepare message replied	Modules that reply reset prepare messages: • **P**—Neighbor maintenance module.

Field	Description
	• **L**—LSDB synchronization module. • **C**—Route calculation module. • **R**—Route redistribution module.
Reset process message replied	Modules that reply reset process messages: • **P**—Neighbor maintenance module. • **L**—LSDB synchronization module. • **C**—Route calculation module. • **R**—Route redistribution module.

Reset phase of module	Reset phase of each module:
	• Main control module:
	  ○ **N/A**—Not reset.
	  ○ Delete area.
	  ○ Delete process.
	• Neighbor maintenance (P) module:
	  ○ **N/A**—Not reset.
	  ○ Delete neighbor.
	  ○ Delete interface.
	  ○ **Delete vlink**—Delete virtual link.
	• LSDB synchronization (L) module:
	  ○ **N/A**—Not reset.
	  ○ Stop timer.
	  ○ **Delete ASE**—Delete all ASE LSAs.
	  ○ **Delete ASE maps**—Delete ASE LSA maps.
	  ○ Clear process data.
	  ○ **Delete area LSA**—Delete LSAs and maps from an area.
	  ○ **Delete area interface**—Delete interfaces from an area.
	  ○ **Delete process**—Delete process-related resources.
	  ○ **Restart**—Restart process-related resources.
	• Route calculation (C) module:
	  ○ **N/A**—Not reset.
	  ○ **Delete topology**—Delete area topology.
	  ○ **Delete router**—Delete routes of routers.
	  ○ **Delete intra AS**—Delete intra-AS routes
	  ○ **Delete inter AS**—Delete AS-external routes.
	  ○ **Delete forward address**—Delete forwarding address list.
	  ○ **Delete advertise**—Delete advertising router list.
	• Route redistribution (R) module:
	  ○ **N/A**—Not reset.
	  ○ **Delete ABR summary**—Delete summary routes of the ABR.
	  ○ **Delete ASBR summary**—Delete summary routes of the ASBR.
	  ○ **Delete import**—Delete redistributed routes.

Field	Description
Area	Area ID in the IP address format.
MPLS TE not enabled	This field is not supported in the current software version. Whether MPLS TE is enabled for the OSPF area.
Authtype	Authentication type of the area: • **None**—No authentication. • **Simple**—Simple authentication. • **MD5**—MD5 authentication. • **Keychain**—Keychain authentication.
Area flag	Type of the area: • Normal. • Stub. • StubNoSummary (totally stub area). • NSSA. • NSSANoSummary (totally NSSA area).
7/5 translator state	State of the translator that translates Type-7 LSAs to Type-5 LSAs: • **Enabled**—The translator is specified through commands. • **Elected**—The translator is designated through election. • **Disabled**—The device is not a translator.
7/5 translate stability timer interval	Stability interval for Type-7 LSA-to-Type-5 LSA translation.
SPF scheduled Count	SPF calculation count in the OSPF area.
Interface	Interface in the area.
Cost	Interface cost.
State	Interface state.
Type	Interface network type.
MTU	Interface MTU.
Priority	Router priority.
Timers	OSPF timers: • **Hello**—Interval for sending hello packets. • **Dead**—Interval within which the neighbor is down. • **Poll**—Interval for sending hello packets. • **Retransmit**—Interval for retransmitting LSAs.
FRR backup	Whether Loop Free Alternate (LFA) calculation is enabled on an interface.
Simple authentication enabled	Simple authentication is enabled.
Keychain authentication enabled, name is *xx*	Keychain authentication is enabled. The name of the keychain is *xx*.
MD5 authentication enabled	MD5/HMAC-MD5 authentication is enabled.
The last key is *xx*	The most recent MD5/HMAC-MD5 authentication

Field	Description
	key ID is *xx*.
The rollover is in progress, *xx* neighbor(s) left	Key rollover for MD5/HMAC-MD5 authentication is in progress. The number of neighbors that have not completed rollover is *xx*.
Packet size	Maximum length of OSPF packets that can be sent by the interface.

4.1.11. display ospf abr-asbr

Use **display ospf abr-asbr** to display routes to the ABR or ASBR.

Syntax

display ospf [*process-id*] **abr-asbr** [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays routes to the ABR and ASBR for all OSPF processes.

verbose: Displays detailed information. If you do not specify this keyword, the command displays brief information.

Usage guidelines

If you use this command on routers in a stub area, the commands displays no ASBR information.

Examples

Display brief information about routes to the ABR or ASBR.

```
<Switch> display ospf abr-asbr

          OSPF Process 1 with Router ID 192.168.1.2
                  Routing Table to ABR and ASBR


                 Topology base (MTID 0)
 Type        Destination       Area        Cost  Nexthop         RtType
 Inter       3.3.3.3           0.0.0.0     3124  10.1.1.2        ASBR
 Intra       2.2.2.2           0.0.0.0     1562  10.1.1.2        ABR
```

Display detailed information about routes to the ABR or ASBR.

```
<Switch> display ospf abr-asbr verbose

          OSPF Process 10 with Router ID 101.1.1.11
                  Routing Table to ABR and ASBR

                Topology base (MTID 0)

 Destination: 1.1.1.1            RtType      : ASBR
 Area       : 0.0.0.1            Type        : Intra
 Nexthop    : 150.0.1.12         BkNexthop   : 0.0.0.0
 Interface  : Vlan10             BkInterface: N/A
 Cost       : 1000
```

Table 4-2 Command output

Field	Description
Type	Type of the route to the ABR or ASBR: • **Intra**—Intra-area route. • **Inter**—Inter-area route.
Topology	This field is not supported in the current software version. Topology name. The topology name for base topology is **base**.
MTID	This field is not supported in the current software version. Topology ID. The value of 0 indicates the base topology.
Destination	Router ID of an ABR or ASBR.
Area	ID of the area of the next hop.
Cost	Cost from the router to the ABR or ASBR.
Nexthop	Next hop address.
BkNexthop	Backup next hop address.
RtType	Router type: ABR or ASBR.
Interface	Output interface.
BkInterface	Backup output interface.

4.1.12. display ospf abr-summary

Use **display ospf abr-summary** to display ABR summary route information.

Syntax

display ospf [*process-id*] [**area** *area-id*] **abr-summary** [*ip-address* { *mask-length* | *mask* }] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays information about ABR summary routes for all OSPF processes.

area *area-id*: Specifies an OSPF area by its ID. The area ID is an IP address or a decimal integer in the range of 0 to 4294967295 that is translated into the IP address format. If you do not specify this option, the command displays information about ABR summary routes for all OSPF areas.

ip-address: Specifies a summary route by its IP address.

mask-length: Specifies the mask length in the range of 0 to 32.

mask: Specifies the mask in dotted decimal notation.

verbose: Displays detailed ABR summary route information. If you do not specify this keyword, the command displays brief ABR summary route information.

Usage guidelines

If you do not specify an IP address, this command displays information about all summary routes on the ABR.

Examples

Display brief information about summary routes on the ABR.

```
<Switch> display ospf abr-summary

          OSPF Process 1 with Router ID 2.2.2.2
                  ABR Summary Addresses

                Topology base (MTID 0)
                        Area: 0.0.0.1
 Total summary address count: 1
 Net             Mask            Status        Count      Cost
 100.0.0.0       255.0.0.0       Advertise     1          (Not Configured)
```

Table 4-3 Command output

Field	Description
Topology	This field is not supported in the current software version. Topology name. The topology name for base

Field	Description
	topology is **base**.
MTID	This field is not supported in the current software version. Topology ID. The value of 0 indicates the base topology.
Area	Area to which the summary routes belong.
Total summary address count	Total number of summary routes.
Net	Address of the summary route.
Mask	Mask of the summary route address.
Status	Advertisement status of the summary route: **Advertise** or **Non-Advertise**.
Count	Number of summarized routes.
Cost	Cost of the summary route.

Display detailed information about summary routes on the ABR.

```
<Switch> display ospf abr-summary verbose

          OSPF Process 1 with Router ID 2.2.2.2
                  ABR Summary Addresses

                Topology base (MTID 0)
                        Area: 0.0.0.1
 Total summary address count: 1

 Net          : 100.0.0.0
 Mask         : 255.0.0.0
 Status       : Advertise
 Cost         : (Not Configured)
 Routes count: 1
   Destination            NetMask                Metric
   100.1.1.0              255.255.255.0          1000
```

Table 4-4 Command output

Field	Description
Topology	This field is not supported in the current software version. Topology name. The topology name for base topology is **base**.
MTID	This field is not supported in the current software version. Topology ID. The value of 0 indicates the base topology.
Destination	Destination address of a summarized route.
NetMask	Network mask of a summarized route.

Field	Description
Metric	Metric of a summarized route.

4.1.13. display ospf asbr-summary

Use **display ospf asbr-summary** to display ASBR summary route information.

Syntax

display ospf [*process-id*] **asbr-summary** [*ip-address* { *mask-length* | *mask* }]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays information about ASBR summary routes for all OSPF processes.

ip-address: Specifies an IP address in dotted decimal notation.

mask-length: Specifies the mask length in the range of 0 to 32.

mask: Specifies the mask in dotted decimal notation.

Usage guidelines

If you do not specify an IP address, this command displays information about all ASBR summary routes.

Examples

Display ASBR summary route information in OSPF process 1.

```
<Switch> display ospf 1 asbr-summary

          OSPF Process 1 with Router ID 2.2.2.2
                  Summary Addresses


                Topology base (MTID 0)
 Total summary address count: 1

                  Summary Address

 Net         : 30.1.0.0
```

```
Mask         : 255.255.0.0
Tag          : 20
Status       : Advertise
Cost         : 10 (Configured)
Route count : 2

Destination     Net mask        Proto      Process   Type     Metric

30.1.2.0        255.255.255.0   OSPF       2         2        1
30.1.1.0        255.255.255.0   OSPF       2         2        1
```

Table 4-5 Command output

Field	Description
Topology	This field is not supported in the current software version. Topology name. The topology name for base topology is **base**.
MTID	This field is not supported in the current software version. Topology ID. The value of 0 indicates the base topology.
Total summary address count	Total number of summary routes.
Net	Address of the summary route.
Mask	Mask of the summary route address.
Tag	Tag of the summary route.
Status	Advertisement status of the summary route.
Cost	Cost of the summary route.
Route count	Number of summarized routes.
Destination	Destination address of a summarized route.
Net mask	Network mask of a summarized route.
Proto	Routing protocol from which the route was redistributed.
Process	Process ID of the routing protocol from which the route was redistributed.
Type	Type of a summarized route.
Metric	Metric of a summarized route.

4.1.14. display ospf event-log

Use **display ospf event-log** to display OSPF log information.

Syntax

display ospf [*process-id*] **event-log** { **lsa-flush** | **peer** | **spf** }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays OSPF log information for all processes.

lsa-flush: Specifies LSA aging log information.

peer: Specifies neighbor log information.

spf: Specifies route calculation log information.

Usage guidelines

Route calculation logs show the number of routes newly installed in the IP routing table.

Neighbor logs include information about the following events:

- The OSPF neighbor state goes down.
- The OSPF neighbor state goes backward because the local end receives BadLSReq, SeqNumberMismatch, and 1-Way events.

Examples

Display OSPF LSA aging log information for all processes.

```
<Switch> display ospf event-log lsa-flush

          OSPF Process 1 with Router ID 1.1.1.1
                  LSA Flush Log

 Date: 2013-09-22 Time: 14:47:33 Received MaxAge LSA from 10.1.1.1
 Type: 1   LS ID: 2.2.2.2         AdvRtr: 2.2.2.2           Seq#: 80000001

 Date: 2013-09-22 Time: 14:47:33 Flushed MaxAge LSA by the self
 Type: 1   LS ID: 1.1.1.1         AdvRtr: 1.1.1.1           Seq#: 80000001

 Date: 2013-09-22 Time: 14:47:33 Received MaxAge LSA from 10.1.2.2
 Type: 1   LS ID: 2.2.2.2         AdvRtr: 2.2.2.2           Seq#: 80000001

 Date: 2013-09-22 Time: 14:47:33 Flushed MaxAge LSA by the self
 Type: 1   LS ID: 1.1.1.1         AdvRtr: 1.1.1.1           Seq#: 80000001
```

Table 4-6 Command output

Field	Description
Date/Time	Time when the device receives an LSA that has reached the maximum age.

Field	Description
Received MaxAge LSA from *X.X.X.X*	The device received an LSA that has reached the maximum age from *X.X.X.X*.
Flushed MaxAge LSA by the self	The device flushed the LSA that has reached the maximum age.
Type	LSA type.
LS ID	LSA link state ID.
AdvRtr	Advertising router.
Seq#	LSA sequence number.

Display OSPF route calculation log information for all processes.

```
<Switch> display ospf event-log spf

          OSPF Process 1 with Router ID 1.1.1.2
                  SPF Log

                Topology base (MTID 0)

Date       Time     Duration   Intra Inter External Reason
2012-06-27 15:28:26 0.95       1     1     10000    Intra-area LSA
2012-06-27 15:28:23 0.2        0     0     0        Area 0 full neighbor
2012-06-27 15:28:19 0          0     0     0        Intra-area LSA
2012-06-27 15:28:19 0          0     0     0        external LSA
2012-06-27 15:28:19 0.3        0     0     0        Intra-area LSA
2012-06-27 15:28:12 0          1     0     0        Intra-area LSA
2012-06-27 15:28:11 0          0     0     0        Routing policy
2012-06-27 15:28:11 0          0     0     0        Intra-area LSA
```

Table 4-7 Command output

Field	Description
Topology	This field is not supported in the current software version. Topology name. The topology name for base topology is **base**.
MTID	This field is not supported in the current software version. Topology ID. The value of 0 indicates the base topology.
Date/Time	Time when the route calculation starts.
Duration	Duration of the route calculation, in seconds.
Intra	Number of intra-area routes newly installed in the IP routing table.
Inter	Number of inter-area routes newly installed in the IP routing table.
External	Number of external routes newly installed in the IP routing table.
Reason	Reasons why the route calculation is performed: • **Intra-area LSA**—Intra-area LSA changes. • **Inter-area LSA**—Inter-area LSA changes.

Field	Description
	• **External LSA**—External LSA changes. • **Configuration**—Configuration changes. • **Area 0 full neighbor**—Number of **FULL**-state neighbors in Area 0 changes. • **Area 0 up interface**—Number of interfaces in up state in Area 0 changes. • **LSDB overflow state**—Overflow status changes. • **AS number**—AS number changes. • **ABR summarization**—ABR summarization changes. • **GR end**—GR ends. • **Routing policy**—Routing policy changes. • **Intra-area tunnel**—Intra-area tunnel changes. • **Others**—Other reasons.

Display OSPF neighbor log information for OSPF process 1.

```
<Switch> display ospf 1 event-log peer

          OSPF Process 1 with Router ID 1.1.1.1
                 Neighbors Log

Date       Time     Local Address   Remote Address  Router ID       Reason
2012-12-31 12:35:45 197.168.1.1     197.168.1.2     2.2.2.2         IntPhyChange
2012-12-31 12:35:19 197.168.1.1     197.168.1.2     2.2.2.2         ConfNssaArea
2012-12-31 12:34:59 197.168.1.1     197.168.1.2     2.2.2.2         SilentInt
```

Table 4-8 Command output

Field	Description
Date/Time	Time when the neighbor state changes.
Local Address	Local address of the neighbor relationship.
Remote Address	Peer address of the neighbor relationship.
Router ID	Neighbor router ID.
Reason	Reasons for neighbor state changes: • **ResetConnect**—The connection is lost due to insufficient memory. • **IntChange**—The interface parameter has changed. • **VlinkChange**—The virtual link parameter has changed. • **ResetOspf**—The OSPF process is reset. • **UndoOspf**—The OSPF process is deleted. • **UndoArea**—The OSPF area is deleted. • **UndoNetwork**—The interface is disabled. • **SilentInt**—The interface is configured as a silent interface. • **IntLogChange**—The logical attribute of the interface has changed. • **IntPhyChange**—The physical attribute of the interface has changed. • **IntVliChange**—The virtual link attribute of the interface has changed.

Field	Description
	• **VlinkDown**—The virtual link goes down. • **DeadExpired**—The dead timer expires. • **ConfStubArea**—The interface is configured with stub area parameters. • **ConfNssaArea**—The interface is configured with NSSA area parameters. • **AuthChange**—The authentication type has changed. • **OpaqueChange**—The Opaque capability has changed. • **Retrans**—Excessive retransmissions. • **LLSChange**—The LLS capability has changed. • **OOBChange**—The OOB capability has changed. • **GRChange**—The GR capability has changed. • **BFDDown**—The interface is shut down by BFD. • **BadLSReq**—The interface receives BadLSReq events. • **SeqMismatch**—The interface receives SeqNumberMismatch events. • **1-Way**—The interface receives 1-Way events. • **LocalNoLSA**—The requested LSA does not exist. • **SameLSAReq**—The received LSA is in the local request queue. • **OldLSAReq**—The received LSA has a larger aging time than the requested LSA in the local request queue. • **DdTimerOut**—Receives a DD packet after the hello timer expires. • **EAChange**—The External Attribute bit has changed. • **RecvNoDupPkt**—Receives a non-duplicate DD packet in loading or full status. • **EbitChange**—The E bit has changed. • **MSbitChange**—The MS bit has changed. • **IbitChange**—The I bit has changed. • **MSeqNumError**—The primary router receives an unexpected serial number from the secondary router. • **SSeqNumError**—The secondary router receives an unexpected serial number from the primary router. • **RecvOpqIntf**—A DD packet that contains a type 9 LSA is received when the opaque LSA reception and advertisement capability is disabled. • **RecvOpqArea**—A DD packet that contains a type 10 LSA is received when the opaque LSA reception and advertisement capability is disabled. • **RecvOpqAs**—A DD packet that contains a type 11 LSA is received when the opaque LSA reception and advertisement capability is disabled. • **RecvNSSA**—A DD packet that contains a type 7 LSA is received in a non-NSSA area. • **InvalidLSA**—A DD packet that contains an invalid LSA is received. • **RecvASE**—A DD packet that contains a type 5 LSA is received on a virtual link or in a stub area.

Related commands

`reset ospf event-log`

4.1.15. display ospf graceful-restart

Use **display ospf graceful-restart** to display GR information.

Syntax

display ospf [*process-id*] **graceful-restart** [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays GR information for all processes.

verbose: Displays detailed GR information. If you do not specify this keyword, the command displays brief GR information.

Examples

Display detailed GR information.

```
<Switch> display ospf graceful-restart verbose

          OSPF Process 1 with Router ID 1.1.1.1
              Graceful Restart information

Graceful Restart capability     : Enable(IETF)
Graceful Restart support        : Planned and un-planned,Partial
Helper capability                 : Enable(IETF)
Helper support                  : Planned and un-planned(IETF),Strict LSA check
Current GR state                : Normal
Graceful Restart period         : 40 seconds
Number of neighbors under Helper: 0
Number of restarting neighbors  : 0
Last exit reason:
  Restarter  : None
  Helper     : None

Area: 0.0.0.0
Authtype: None Area flag: Normal
Area up Interface count: 2

Interface: 40.4.0.1 (Vlan-interface40)
Restarter state: Normal  State: P-2-P     Type: PTP
Last exit reason:
```

```
  Restarter  : None
  Helper     : None
Neighbor count of this interface: 1
Number of neighbors under Helper: 0
Neighbor        IP address      GR state     Last Helper exit reason
3.3.3.3         40.4.0.3        Normal       None

Virtual-link Neighbor-ID  -> 4.4.4.4, Neighbor-State: Full
Restarter state: Normal
Interface: 20.2.0.1 (Vlink)
Transit Area: 0.0.0.1
Last exit reason:
  Restarter  : None
  Helper     : None
Neighbor        IP address      GR state     Last Helper exit reason
4.4.4.4         20.2.0.4        Normal       Reset neighbor
```

Table 4-9 Command output

Field	Description
OSPF Process 1 with Router ID 1.1.1.1 Graceful Restart information	GR information for OSPF process 1 with router ID 1.1.1.1.
Graceful Restart capability	Whether GR is enabled: • **Enable(IETF)**—IETF GR is enabled. • **Enable(Nonstandard)**—Non-IETF GR is enabled. • **Disable**—GR is disabled.
Graceful Restart support	GR modes that the process supports (displayed only when GR is enabled): • **Planned and un-planned**—Supports both planned and unplanned GR. • **Planned only**—Supports only planned GR. • **Partial**—Supports partial GR. • **Global**—Supports global GR.
Helper capability	Helper capability that the process supports: • **Enable (IETF)**—Supports IETF GR helper capability. • **Enable (Nonstandard)**—Supports non-IETF GR helper capability. • **Enable (IETF and nonstandard)**—Supports both IETF GR helper capability and non-IETF GR helper capability. • **Disable**—Does not support GR helper capability.
Helper support	Policies that the helper supports (displayed only when GR helper is enabled): • **Strict lsa check**—The helper supports strict LSA checking. • **Planned and un-planned**—The helper supports planned and unplanned GR.

Field	Description
	• **Planned only**—The helper supports only planned GR.
Current GR state	GR state: • **Normal**—GR is not in progress or has completed. • **Under GR**—GR is in process. • **Under Helper**—The process is acting as GR helper.
Last exit reason	Last exit reason: • **Restarter**—Reason that the restarter exited most recently. • **Helper**—Reason that the helper exited most recently.
Area	Area ID in IP address format.
Authtype	Authentication type of the area: • **None**—No authentication. • **Simple**—Simple authentication. • **MD5**—MD5 authentication. • **Keychain**—Keychain authentication.
Area flag	Type of the area: • Normal. • Stub. • StubNoSummary (totally stub area). • NSSA. • NSSANoSummary (totally NSSA area).
Area up Interface count	Number of up interfaces in the area.
Interface	Interface in the area.
Restarter state	Restarter state on the interface.
State	Interface state.
Type	Interface network type.
Neighbor count of this interface	Neighbors of an interface.
Neighbor	Neighbor router ID.
IP address	Neighbor IP address.
GR state	Neighbor GR state: • **Normal**—GR is not in progress or has completed. • **Under GR**—GR is in process. • **Under Helper**—The process is acting as GR helper.
Last Helper exit reason	Reason that the helper exited most recently.
Virtual-link Neighbor-ID	Router ID of the virtual link's neighbor.
Neighbor-State	Neighbor state: Down, Init, 2-Way, ExStart, Exchange, Loading, and Full.
Interface	Output interface of the virtual link.

4.1.16. display ospf interface

Use **display ospf interface** to display OSPF interface information.

Syntax

display ospf [*process-id*] **interface** [*interface-type interface-number* | **verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies an OSPF process ID in the range of 1 to 65535. If you do not specify this argument, the command displays the OSPF interface information for all OSPF processes.

interface-type interface-number: Specifies an interface by its type and number.

verbose: Displays detailed OSPF information for all interfaces.

Usage guidelines

If you do not specify the *interface-type interface-number* argument or the **verbose** keyword, this command displays OSPF brief information for all interfaces.

Examples

Display all OSPF interface brief information.

```
<Switch> display ospf interface

          OSPF Process 1 with Router ID 192.168.1.1
                  Interfaces

 Area: 0.0.0.0
 IP Address      Type         State    Cost  Pri   DR              BDR
 192.168.1.1     PTP          P-2-P    1562  1     0.0.0.0         0.0.0.0

 Area: 0.0.0.1
 IP Address      Type         State    Cost  Pri   DR              BDR
 172.16.0.1      Broadcast    DR       1     1     172.16.0.1      0.0.0.0
```

Table 4-10 Command output

Field	Description
Area	Area ID of the interface.
IP Address	Interface IP address (regardless of whether TE is enabled or not).

Field	Description
Type	Interface network type: PTP (P2P), PTMP (P2MP), Broadcast, or NBMA.
State	Interface state: • **DOWN**—No protocol traffic can be sent or received on the interface. • **Loopback**—The interface is in loopback state and it cannot forward traffic. • **Waiting**—The interface starts sending and receiving Hello packets. The router is trying to determine the identity of the (Backup) designated router for the network. • **P-2-P**—The interface will send Hello packets at the hello interval, and try to establish an adjacency with the neighbor. • **DR**—The router is the designated router on the network. • **BDR**—The router is the backup designated router on the network. • **DROther**—The router is a DR Other router on the attached network.
Cost	Interface cost.
Pri	Router priority.
DR	DR on the interface's network segment.
BDR	BDR on the interface's network segment.

Display detailed information about VLAN-interface 10.

```
<Switch> display ospf interface vlan-interface 10


          OSPF Process 1 with Router ID 192.168.1.1
                  Interfaces

 Area: 0.0.0.0

 Interface: 172.16.0.1 (Vlan-interface10)
 Cost: 1       State: DR        Type: Broadcast    MTU: 1500
 Priority: 1
 Designated router: 172.16.0.1
 Backup designated router: 0.0.0.0
 Timers: Hello 10, Dead 40, Poll  40, Retransmit 5, Transmit Delay 1
 FRR backup: Enabled
 Primary path detection mode: BFD ctrl
 Enabled by interface configuration (including secondary IP addresses)
 BFD: echo
 MD5 authentication enabled.
    The last key is 3.
    The rollover is in progress, 2 neighbor(s) left.
 LDP state: No-LDP
 LDP sync state: Achieved
 Packet size: 1000
```

Table 4-11 Command output

Field	Description
Interface	Information about the interface, such as the IP address.
Timers	OSPF timers (in seconds): **Hello**, **Dead**, **Poll**, and **Retransmit**.
Transmit Delay	LSA transmission delay on the interface, in seconds.
FRR backup	Whether LFA calculation is enabled on an interface.
Primary path detection mode	Primary link detection mode: • **BFD ctrl**—BFD control packet mode. • **BFD echo**—BFD echo packet mode.
Enabled by interface configuration (including secondary IP addresses)	OSPF is enabled on the interface (including secondary IP addresses).
BFD	BFD session mode enabled on the interface: • **ctrl**—BFD control packet mode. • **echo**—BFD echo packet mode.
Simple authentication enabled	Simple authentication is enabled.
Keychain authentication enabled, name is *xx*	Keychain authentication is enabled. The name of the keychain is *xx*.
MD5 authentication enabled	MD5/HMAC-MD5 authentication is enabled.
The last key is *xx*	The most recent MD5/HMAC-MD5 authentication key ID is *xx*.
The rollover is in progress, *xx* neighbor(s) left.	Key rollover for MD5/HMAC-MD5 authentication is in progress. The number of neighbors that have not completed rollover is *xx*.
LDP state	LDP state: • **Init**—Initialization state. LDP has not been delivered. • **No-LDP**—LDP is not configured. • **Not ready**—LDP sessions have not been established. • **Ready**—LDP sessions have been established.
LDP sync state	LDP IGP synchronization state: • **Init**—Initialization state. • **Achieved**—LDP has been synchronized. • **Max cost**—OSPF advertises the maximum cost in LSAs.
Packet size	Maximum length of OSPF packets that can be sent by the interface.

4.1.17. display ospf lsdb

Use **display ospf lsdb** to display OSPF LSDB information.

Syntax

display ospf [*process-id*] **lsdb** [**brief** | **originate-router** *advertising-router-id* | **self-originate**]

display ospf [*process-id*] **lsdb** { **opaque-as** | **ase** } [*link-state-id*] [**originate-router** *advertising-router-id* | **self-originate**]

display ospf [*process-id*] [**area** *area-id*] **lsdb** { **asbr** | **network** | **nssa** | **opaque-area** | **opaque-link** | **router** | **summary** } [*link-state-id*] [**originate-router** *advertising-router-id* | **self-originate**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays LSDB information for all OSPF processes.

area *area-id*: Specifies an OSPF area by its ID. The area ID is an IP address or a decimal integer in the range of 0 to 4294967295 that is translated into the IP address format. If you do not specify this option, the command displays LSDB information for all OSPF areas.

brief: Displays brief LSDB information.

asbr: Displays Type-4 LSA (ASBR Summary LSA) information in the LSDB.

ase: Displays Type-5 LSA (AS External LSA) information in the LSDB.

network: Displays Type-2 LSA (Network LSA) information in the LSDB.

nssa: Displays Type-7 LSA (NSSA External LSA) information in the LSDB.

opaque-area: Displays Type-10 LSA (Opaque-area LSA) information in the LSDB.

opaque-as: Displays Type-11 LSA (Opaque-AS LSA) information in the LSDB.

opaque-link: Displays Type-9 LSA (Opaque-link LSA) information in the LSDB.

router: Displays Type-1 LSA (Router LSA) information in the LSDB.

summary: Displays Type-3 LSA (Network Summary LSA) information in the LSDB.

link-state-id: Specifies a link state ID in the IP address format.

originate-router *advertising-router-id*: Specifies an advertising router by its ID.

self-originate: Displays information about self-originated LSAs.

Examples

Display OSPF LSDB information.

```
<Switch> display ospf lsdb
         OSPF Process 1 with Router ID 192.168.0.1
                 Link State Database
```

```
                        Area: 0.0.0.0
 Type       LinkState ID    AdvRouter          Age  Len   Sequence   Metric
 Router     192.168.0.2     192.168.0.2        474  36    80000004   0
 Router     192.168.0.1     192.168.0.1        21   36    80000009   0
 Network    192.168.0.1     192.168.0.1        321  32    80000003   0
 Sum-Net    192.168.1.0     192.168.0.1        321  28    80000002   1
 Sum-Net    192.168.2.0     192.168.0.2        474  28    80000002   1
                        Area: 0.0.0.1
 Type       LinkState ID    AdvRouter          Age  Len   Sequence   Metric
 Router     192.168.0.1     192.168.0.1        21   36    80000005   0
 Sum-Net    192.168.2.0     192.168.0.1        321  28    80000002   2
 Sum-Net    192.168.0.0     192.168.0.1        321  28    80000002   1
                        Type 9 Opaque (Link-Local Scope) Database
 Flags: * -Vlink interface LSA
 Type       LinkState ID    AdvRouter          Age  Len   Sequence   Interfaces
*Opq-Link   3.0.0.0         7.2.2.1            8    14    80000001   10.1.1.2
*Opq-Link   3.0.0.0         7.2.2.2            8    14    80000001   20.1.1.2
```

Table 4-12 Command output

Field	Description
Area	LSDB information for the area.
Type	LSA type.
LinkState ID	Link state ID.
AdvRouter	Advertising router.
Age	Age of the LSA.
Len	Length of the LSA.
Sequence	Sequence number of the LSA.
Metric	Cost of the LSA.
*Opq-Link	Opaque LSA generated by a virtual link.

Display Type-2 LSA (Network LSA) information in the LSDB.

```
<Switch> display ospf 1 lsdb network

          OSPF Process 1 with Router ID 192.168.1.1
                  Link State Database

                        Area: 0.0.0.0

    Type      : Network
    LS ID     : 192.168.0.2
    Adv Rtr   : 192.168.2.1
    LS age    : 922
    Len       : 32
    Options   :  E
    Seq#      : 80000003
```

```
Checksum    : 0x8d1b
Net mask  : 255.255.255.0
   Attached router    192.168.1.1
   Attached router    192.168.2.1

                      Area: 0.0.0.1

Type      : Network
LS ID     : 192.168.1.2
Adv Rtr   : 192.168.1.2
LS age    : 782
Len       : 32
Options   :  NP
Seq#      : 80000003
Checksum    : 0x2a77
Net mask  : 255.255.255.0
   Attached router    192.168.1.1
   Attached router    192.168.1.2
```

Table 4-13 Command output

Field	Description
Type	LSA type.
LS ID	DR IP address.
Adv Rtr	Router that advertised the LSA.
LS age	LSA age time.
Len	LSA length.
Options	LSA options: • **O**—Opaque LSA advertisement capability. • **E**—AS External LSA reception capability. • **EA**—External extended LSA reception capability. • **DC**—On-demand link support. • **N**—NSSA external LSA support. • **P**—Capability of an NSSA ABR to translate Type-7 LSAs into Type-5 LSAs.
Seq#	LSA sequence number.
Checksum	LSA checksum.
Net mask	Network mask.
Attached router	ID of the router that established adjacency with the DR, and ID of the DR itself.

4.1.18. display ospf nexthop

Use **display ospf nexthop** to display OSPF next hop information.

Syntax

display ospf [*process-id*] **nexthop**

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays next hop information for all OSPF processes.

Examples

Display OSPF next hop information.

```
<Switch> display ospf nexthop

          OSPF Process 1 with Router ID 1.1.1.2
                  Neighbor Nexthop Information

 NbrID           Nexthop         Interface               RefCount   Status
 192.168.12.1    0.0.0.0         Vlan10                  4          Valid
 192.168.12.2    192.168.12.2    Vlan10                  3          Valid
 192.168.12.1    0.0.0.0         Loop100                 1          Valid
```

Table 4-14 Command output

Field	Description
NbrID	Neighbor router ID.
Nexthop	Next hop address.
Interface	Output interface.
RefCount	Reference count (routes that use the next hop).
Status	Next hop status: valid or invalid.

4.1.19. display ospf peer

Use **display ospf peer** to display information about OSPF neighbors.

Syntax

display ospf [*process-id*] **peer** [**verbose**] [*interface-type interface-number*] [*neighbor-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies an OSPF process by ID in the range of 1 to 65535. If you do not specify this argument, the command displays OSPF neighbor information for all OSPF processes.

verbose: Displays detailed neighbor information. If you do not specify this keyword, the command displays brief OSPF neighbor information.

interface-type interface-number: Specifies an interface by its type and number. If you do not specify this argument, the command displays neighbor information for all interfaces.

neighbor-id: Specifies a neighbor router ID. If you do not specify this argument, the command displays all neighbor information.

Examples

Display detailed OSPF neighbor information.

```
<Switch> display ospf peer verbose

          OSPF Process 1 with Router ID 1.1.1.1
                  Neighbors

 Area 0.0.0.0 interface 1.1.1.1(Vlan-interface100)'s neighbors
 Router ID: 1.1.1.2          Address: 1.1.1.2          GR state: Normal
   State: Full  Mode: Nbr is master  Priority: 1
   DR: 1.1.1.2  BDR: 1.1.1.1  MTU: 0
   Options is 0x02 (-|-|-|-|-|-|E|-)
   Dead timer due in 33  sec
   Neighbor is up for 02:03:35
   Authentication sequence: [ 0 ]
   Neighbor state change count: 6
   BFD status: Disabled


 Last Neighbor Down Event:
 Router ID: 22.22.22.22
 Local Address: 11.11.11.11
 Remote Address: 22.22.22.22
 Time: Apr  9 03:18:19 2014
 Reason: Ospf_ifachange
```

Table 4-15 Command output

Field	Description
Area *areaID* interface *IPAddress*(*InterfaceName*)'s neighbors	Neighbor information for the interface in the specified area:

Field	Description
	• **areaID**—Area to which the neighbor belongs. • **IPAddress**—Interface IP address. • **InterfaceName**—Interface name.
Router ID	Neighbor router ID.
Address	Neighbor router address.
GR state	GR state: • Normal. • Restarter. • Complete. • Helper.
State	Neighbor state: • **Down**—Initial state of a neighbor conversation. • **Init**—The router has received a Hello packet from the neighbor. However, the router has not established bidirectional communication with the neighbor. The router did not appear in the neighbor's hello packet. • **Attempt**—Available only in an NBMA network. In this state, the OSPF router has not received any information from a neighbor for a period. The router can send Hello packets at a longer interval to keep the neighbor relationship. • **2-Way**—Communication between the two routers is bidirectional. The local router appears in the neighbor's Hello packet. • **Exstart**—The goal of this state is to decide which router is the master, and to decide upon the initial Database Description (DD) sequence number. • **Exchange**—The router is sending DD packets to the neighbor, describing its entire link-state database. • **Loading**—The router sends LSRs packets to the neighbor, requesting more recent LSAs. • **Full**—The neighboring routers are fully adjacent.
Mode	Neighbor mode for LSDB synchronization.
Priority	Neighboring router priority.
DR	DR on the interface's network segment.
BDR	BDR on the interface's network segment.
MTU	Interface MTU.
Options	LSA options: • **O**—Opaque LSA advertisement capability. • **E**—AS External LSA reception capability. • **EA**—External extended LSA reception capability. • **DC**—On-demand link support. • **N**—NSSA external LSA support. • **P**—Capability of an NSSA ABR to translate

Field	Description
	Type-7 LSAs into Type-5 LSAs.
Dead timer due in 33 sec	This dead timer will expire in 33 seconds.
Neighbor is up for 02:03:35	The neighbor has been up for 02:03:35.
Authentication sequence	Authentication sequence number.
Neighbor state change count	Count of neighbor state changes.
BFD status	BFD status: • Disabled. • Enabled (Control mode). • Enabled (Echo mode).
Last Neighbor Down Event	The most recent neighbor down event.
Time	Time when the neighbor went down.
Reason	Reason for the neighbor down event.

Display brief OSPF neighbor information.

```
<Switch> display ospf peer

          OSPF Process 1 with Router ID 1.1.1.1
               Neighbor Brief Information

 Area: 0.0.0.0
 Router ID       Address         Pri Dead-Time  State             Interface
 1.1.1.2         1.1.1.2         1   40         Full/DR           Vlan10
```

Table 4-16 Command output

Field	Description
Area	Neighbor area.
Router ID	Neighbor router ID.
Address	Neighbor interface address.
Pri	Neighboring router priority.
Dead-Time	Dead interval remained.
Interface	Interface connected to the neighbor.
State	Neighbor state: Down, Init, Attempt, 2-Way, Exstart, Exchange, Loading, or Full.

4.1.20. display ospf peer statistics

Use **display ospf peer statistics** to display OSPF neighbor statistics.

Syntax

display ospf [*process-id*] **peer statistics**

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays OSPF neighbor statistics for all OSPF processes.

Examples

Display OSPF neighbor statistics.

```
<Switch> display ospf peer statistics
          OSPF Process 1 with Router ID 10.3.1.1
                    Neighbor Statistics
  Area ID          Down Attempt Init 2-Way ExStart Exchange Loading Full Total
  0.0.0.0          0    0       0    0     0       0        0       1    1
  0.0.0.2          0    0       0    0     0       0        0       1    1
  Total            0    0       0    0     0       0        0       2    2
```

Table 4-17 Command output

Field	Description
Area ID	The state statistics for all the routers in the area to which the router belongs is displayed.
Down	Number of neighboring routers in Down state in the same area.
Attempt	Number of neighboring routers in Attempt state in the same area.
Init	Number of neighboring routers in Init state in the same area.
2-Way	Number of neighboring routers in 2-Way state in the same area.
ExStart	Number of neighboring routers in ExStart state in the same area.
Exchange	Number of neighboring routers in Exchange state in the same area.
Loading	Number of neighboring routers in Loading state in the same area.
Full	Number of neighboring routers in Full state in the same area.
Total	Total number of neighbors in the same state: Down, Attempt, Init, 2-Way, ExStart, Exchange, Loading, or Full.

4.1.21. display ospf request-queue

Use **display ospf request-queue** to display OSPF request queue information.

Syntax

display ospf [*process-id*] **request-queue** [*interface-type interface-number*] [*neighbor-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays the OSPF request queue information for all OSPF processes.

interface-type interface-number: Specifies an interface by its type and number. If you do not specify this argument, the command displays the OSPF request queue information for all interfaces.

neighbor-id: Specifies a neighbor's router ID. If you do not specify this argument, the command displays the OSPF request queue information for all OSPF neighbors.

Examples

Display OSPF request queue information.

```
<Switch> display ospf request-queue

          OSPF Process 100 with Router ID 192.168.1.59
                  Link State Request List

  The Router's Neighbor is Router ID 2.2.2.2         Address 10.1.1.2
  Interface 10.1.1.1         Area 0.0.0.0
  Request list:
       Type       LinkState ID      AdvRouter         Sequence   Age
       Router     2.2.2.2           1.1.1.1           80000004   1
       Network    192.168.0.1       1.1.1.1           80000003   1
       Sum-Net    192.168.1.0       1.1.1.1           80000002   2
```

Table 4-18 Command output

Field	Description
The Router's Neighbor is Router ID	Neighbor router ID.
Address	Neighbor interface IP address.
Interface	Local interface IP address.
Area	Area ID.
Request list	Request list information.
Type	LSA type.
LinkState ID	Link state ID.
AdvRouter	Advertising router.

Field	Description
Sequence	LSA sequence number.
Age	LSA age.

4.1.22. display ospf retrans-queue

Use **display ospf retrans-queue** to display retransmission queue information.

Syntax

display ospf [*process-id*] **retrans-queue** [*interface-type interface-number*] [*neighbor-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays retransmission queue information for all OSPF processes.

interface-type interface-number: Specifies an interface by its type and number. If you do not specify this argument, the command displays retransmission queue information for all interfaces.

neighbor-id: Specifies a neighbor's router ID. If you do not specify this argument, the command displays retransmission queue information for all neighbors.

Examples

Display OSPF retransmission queue information.

```
<Switch> display ospf retrans-queue

          OSPF Process 100 with Router ID 192.168.1.59
                  Link State Retransmission List

  The Router's Neighbor is Router ID 2.2.2.2         Address 10.1.1.2
  Interface 10.1.1.1         Area 0.0.0.0
  Retransmit list:
       Type       LinkState ID      AdvRouter         Sequence   Age
       Router     2.2.2.2           2.2.2.2           80000004   1
       Network    12.18.0.1         2.2.2.2           80000003   1
       Sum-Net    12.18.1.0         2.2.2.2           80000002   2
```

Table 4-19 Command output

Field	Description
The Router's Neighbor is Router ID	Neighbor router ID.
Address	Neighbor interface IP address.
Interface	Interface address of the router.
Area	Area ID.
Retrans List	Retransmission list.
Type	LSA type.
LinkState ID	Link state ID.
AdvRouter	Advertising router.
Sequence	LSA sequence number.
Age	LSA age.

4.1.23. display ospf routing

Use **display ospf routing** to display OSPF routing information.

Syntax

display ospf [*process-id*] **routing** [*ip-address* { *mask-length* | *mask* }] [**interface** *interface-type interface-number*] [**nexthop** *nexthop-address*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays the routing information for all OSPF processes.

ip-address: Specifies a destination IP address.

mask-length: Specifies mask length in the range of 0 to 32.

mask: Specifies the mask in dotted decimal notation.

interface *interface-type interface-number*: Displays routes passing the specified output interface. If you do not specify this option, the command displays OSPF routing information for all interfaces.

nexthop *nexthop-address*: Displays routes passing the specified next hop. If you do not specify this option, the command displays all OSPF routing information.

verbose: Displays detailed OSPF routing information. If you do not specify this keyword, the command displays brief OSPF routing information.

Examples

Display OSPF routing information.

```
<Switch> display ospf routing

          OSPF Process 1 with Router ID 192.168.1.2
                   Routing Table

                Topology base (MTID 0)

 Routing for network
 Destination        Cost  Type       NextHop         AdvRouter      Area
 192.168.1.0/24     1562  Stub       192.168.1.2     192.168.1.2    0.0.0.0
 172.16.0.0/16      1563  Inter      192.168.1.1     192.168.1.1    0.0.0.0

 Total nets: 2
 Intra area: 1  Inter area: 1  ASE: 0  NSSA: 0

                Topology red (MTID 41)

 Routing for network
 Destination         Cost    Type    NextHop         AdvRouter       Area
 36.1.1.0/24         1       Transit 0.0.0.0         192.168.1.3     0.0.0.1

 Total nets: 1
 Intra area: 1  Inter area: 0  ASE: 0  NSSA: 0
```

Table 4-20 Command output

Field	Description
Topology	This field is not supported in the current software version. Topology name. The topology name for base topology is **base**.
MTID	This field is not supported in the current software version. Topology ID. The value of 0 indicates the base topology.
Destination	Destination network.
Cost	Cost to destination.
Type	Route type: intra-area, transit, stub, inter-area, Type-1 external, and Type-2 external.
NextHop	Next hop address.
AdvRouter	Advertising router.
Area	Area ID.

Field	Description
Total nets	Total networks.
Intra area	Total intra-area routes.
Inter area	Total inter-area routes.
ASE	Total ASE routes.
NSSA	Total NSSA routes.

Display detailed OSPF routing information.

```
<Switch> display ospf routing verbose

          OSPF Process 2 with Router ID 192.168.1.112
                   Routing Table

                Topology base (MTID 0)

 Routing for network

 Destination: 192.168.1.0/24
    Priority: Low                    Type: Stub
   AdvRouter: 192.168.1.2            Area: 0.0.0.0
  SubProtoID: 0x1              Preference: 10
     NextHop: 192.168.1.2       BkNextHop: N/A
      IfType: Broadcast          BkIfType: N/A
   Interface: Vlan100         BkInterface: N/A
       NibID: 0x1300000c           Status: Normal
        Cost: 1562

 Destination: 172.16.0.0/16
    Priority: Low                    Type: Inter
   AdvRouter: 192.168.1.1            Area: 0.0.0.0
  SubProtoID: 0x1              Preference: 10
     NextHop: 192.168.1.1       BkNextHop: N/A
      IfType: Broadcast          BkIfType: N/A
   Interface: Vlan101         BkInterface: N/A
       NibID: 0x1300000c           Status: Normal
        Cost: 1563               SpfCost: 65535

 Total nets: 2
 Intra area: 2  Inter area: 0  ASE: 0  NSSA: 0

                Topology red (MTID 41)

 Routing for network

 Destination: 36.1.1.0/24
    Priority: Low                    Type: Transit
```

```
  AdvRouter: 192.168.1.3              Area: 0.0.0.1
 SubProtoID: 0x1                Preference: 10
    NextHop: 0.0.0.0             BkNextHop: N/A
     IfType: Broadcast             BkIfType: N/A
  Interface: Vlan102           BkInterface: N/A
      NibID: 0x13000001             Status: Direct
       Cost: 1

Total nets: 1
Intra area: 1  Inter area: 0  ASE: 0  NSSA: 0
```

Table 4-21 Command output

Field	Description
Topology	This field is not supported in the current software version. Topology name. The topology name for base topology is **base**.
MTID	This field is not supported in the current software version. Topology ID. The value of 0 indicates the base topology.
Priority	Prefix priority: critical, high, medium, and low.
Type	Route type: intra-area, transit, stub, inter-area, Type-1 external, and Type-2 external.
AdvRouter	Advertising router.
Area	Area ID.
SubProtoID	Sub protocol ID.
Preference	OSPF route preference.
NextHop	Primary next hop IP address.
BkNextHop	Backup next hop IP address.
IfType	Type of the network to which the primary next hop belongs.
BkIfType	Type of the network to which the backup next hop belongs.
Interface	Output interface.
BkInterface	Backup output interface.
NibID	Next hop ID.
Status	Route status: • **Local**—The route is on the local end and is not sent to the route management module. • **Invalid**—The next hop is invalid. • **Stale**—The next hop is stale. • **Normal**—The route is available. • **Delete**—The route is deleted. • **Host-Adv**—The route is a host route. • **Rely**—The route is a recursive route.
Cost	Cost to destination.
SpfCost	SPF cost.

4.1.24. display ospf statistics

Use **display ospf statistics** to display OSPF statistics.

Syntax

display ospf [*process-id*] **statistics** [**error** | **packet** [*interface-type interface-number*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays OSPF statistics for all OSPF processes.

error: Displays error statistics. If you do not specify this keyword, the command displays OSPF packet, LSA, and route statistics.

packet: Displays OSPF packet statistics.

interface-type interface-number: Specifies an interface by its type and number. If you do not specify this argument, the command displays statistics for all interfaces.

Examples

Display OSPF statistics.

```
<Switch> display ospf statistics

          OSPF Process 1 with Router ID 2.2.2.2
                  Statistics


 I/O statistics
  Type                    Input     Output
  Hello                   61        122
  DB Description          2          3
  Link-State Req          1          1
  Link-State Update       3          3
  Link-State Ack          3          2

 LSAs originated by this router
  Router  : 4
  Network : 0
  Sum-Net : 0
  Sum-Asbr: 0
```

```
 External: 0
 NSSA    : 0
 Opq-Link: 0
 Opq-Area: 0
 Opq-As  : 0

LSAs originated: 4  LSAs received: 7

Routing table:
  Intra area: 2  Inter area: 3  ASE/NSSA: 0
```

Table 4-22 Command output

Field	Description
I/O statistics	Statistics about input/output packets and LSAs.
Type	OSPF packet type.
Input	Packets received.
Output	Packets sent.
Hello	Hell packet.
DB Description	Database Description packet.
Link-State Req	Link-State Request packet.
Link-State Update	Link-State Update packet.
Link-State Ack	Link-State Acknowledge packet.
LSAs originated by this router	LSAs originated by this router.
Router	Number of Type-1 LSAs originated.
Network	Number of Type-2 LSAs originated.
Sum-Net	Number of Type-3 LSAs originated.
Sum-Asbr	Number of Type-4 LSAs originated.
External	Number of Type-5 LSAs originated.
NSSA	Number of Type-7 LSAs originated.
Opq-Link	Number of Type-9 LSAs originated.
Opq-Area	Number of Type-10 LSAs originated.
Opq-As	Number of Type-11 LSAs originated.
LSA originated	Number of LSAs originated.
LSA received	Number of LSAs received.
Routing table	Routing table information.
Intra area	Number of intra-area routes.
Inter area	Number of inter-area routes.
ASE	Number of ASE routes.

Display OSPF error statistics.

```
<Switch> display ospf statistics error

          OSPF Process 1 with Router ID 192.168.1.112
                  OSPF Packet Error Statistics

0          : Router ID confusion         0          : Bad packet
0          : Bad version                 0          : Bad checksum
0          : Bad area ID                 0          : Drop on unnumbered link
0          : Bad virtual link            0          : Bad authentication type
0          : Bad authentication key      0          : Packet too small
0          : Neighbor state low          0          : Transmit error
0          : Interface down              0          : Unknown neighbor
0          : HELLO: Netmask mismatch     0          : HELLO: Hello-time mismatch
0          : HELLO: Dead-time mismatch   0          : HELLO: Ebit option mismatch
0          : HELLO: Mbit option mismatch 0          : DD: MTU option mismatch
0          : DD: Unknown LSA type        0          : DD: Ebit option mismatch
0          : ACK: Bad ack                0          : ACK: Unknown LSA type
0          : REQ: Empty request          0          : REQ: Bad request
0          : UPD: LSA checksum bad       0          : UPD: Unknown LSA type
0          : UPD: Less recent LSA
```

Table 4-23 Command output

Field	Description
Router ID confusion	Packets with duplicate router ID.
Bad packet	Packets illegal.
Bad version	Packets with wrong version.
Bad checksum	Packets with wrong checksum.
Bad area ID	Packets with invalid area ID.
Drop on unnumbered link	Packets dropped on the unnumbered interface.
Bad virtual link	Packets on wrong virtual links.
Bad authentication type	Packets with invalid authentication type.
Bad authentication key	Packets with invalid authentication key.
Packet too small	Packets too small in length.
Neighbor state low	Packets received in low neighbor state.
Transmit error	Packets with error when being transmitted.
Interface down	Shutdown times of the interface.
Unknown neighbor	Packets received from unknown neighbors.
HELLO: Netmask mismatch	Hello packets with mismatched mask.
HELLO: Hello-time mismatch	Hello packets with mismatched hello timer.
HELLO: Dead-time mismatch	Hello packets with mismatched dead timer.
HELLO: Ebit option mismatch	Hello packets with mismatched E-bit in the option field.

Field	Description
HELLO: Mbit option mismatch	Hello packets with mismatched M-bit in the option field.
DD: MTU option mismatch	DD packets with mismatched MTU.
DD: Unknown LSA type	DD packets with unknown LSA type.
DD: Ebit option mismatch	DD packets with mismatched E-bit in the option field.
ACK: Bad ack	Bad LSAck packets for LSU packets.
ACK: Unknown LSA type	LSAck packets with unknown LSA type.
REQ: Empty request	LSR packets with no request information.
REQ: Bad request	Bad LSR packets.
UPD: LSA checksum bad	LSU packets with wrong LSA checksum.
UPD: Unknown LSA type	LSU packets with unknown LSA type.
UPD: Less recent LSA	LSU packets without the most recent LSA.

Display OSPF packet statistics for all processes and interfaces.

```
<Switch> display ospf statistics packet

          OSPF Process 100 with Router ID 192.168.1.59
                  Packet Statistics

 Waiting to send packet count: 0
         Hello       DD          LSR         LSU         ACK         Total
 Input : 489         6           2           44          40          581
 Output: 492         8           2           45          40          587

 Area: 0.0.0.1
 Interface: 20.1.1.1 (Vlan-interface100)
         DD          LSR         LSU         ACK         Total
 Input : 0           0           0           0           0
 Output: 0           0           0           0           0

 Interface: 100.1.1.1 (Vlan-interface100)
         DD          LSR         LSU         ACK         Total
 Input : 3           1           22          16          42
 Output: 2           1           19          20          42
```

Table 4-24 Command output

Field	Description
Waiting to send packet count	Number of packets waiting to be sent.
Total	Total number of packets.
Input	Number of received packets.
Output	Number of sent packets.

Field	Description
Area	Area ID.
Interface	Interface address and interface name.

Related commands

reset ospf statistics

4.1.25. display ospf vlink

Use **display ospf vlink** to display OSPF virtual link information.

Syntax

display ospf [*process-id*] **vlink**

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays the OSPF virtual link information for all OSPF processes.

Examples

Display OSPF virtual link information.

```
<Switch> display ospf vlink


          OSPF Process 1 with Router ID 3.3.3.3
                  Virtual Links

 Virtual-link Neighbor-ID  -> 2.2.2.2, Neighbor-State: Full
 Interface: 10.1.2.1 (Vlan-interface100)
 Cost: 1562  State: P-2-P  Type: Virtual
 Transit Area: 0.0.0.1
 Timers: Hello 10 , Dead 40 , Retransmit 5 , Transmit Delay 1
 MD5 authentication enabled.
    The last key is 3.
    The rollover is in progress, 2 neighbor(s) left.
```

Table 4-25 Command output

Field	Description
Virtual-link Neighbor-ID	ID of the neighbor on the virtual link.
Neighbor-State	Neighbor state: Down, Init, 2-Way, ExStart, Exchange, Loading, Full.
Interface	IP address and name of the local interface on the virtual link.
Cost	Interface route cost.
State	Interface state.
Type	Virtual link.
Transit Area	Transit area ID.
Timers	Values of timers (in seconds): **Hello**, **Dead**, and **Retransmit**.
Transmit Delay	LSA transmission delay on the interface, in seconds.
Simple authentication enabled	Simple authentication is enabled.
Keychain authentication enabled, name is *xx*	Keychain authentication is enabled. The name of the keychain is *xx*.
MD5 authentication enabled	MD5/HMAC-MD5 authentication is enabled.
The last key is *xx*	The most recent MD5 authentication key ID is *xx*.
The rollover is in progress, *xx* neighbor(s) left	Key rollover for MD5/HMAC-MD5 authentication is in progress. The number of neighbors that have not completed rollover is *xx*.

4.1.26. display router id

Use **display router id** to display the global router ID.

Syntax

display router id

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display the global router ID.

```
<Switch> display router id
         Configured router ID is 1.1.1.1
```

4.1.27. dscp

Use **dscp** to set the DSCP value for outgoing OSPF packets.

Use **undo dscp** to restore the default.

Syntax

dscp *dscp-value*

undo dscp

Default

The DSCP value for outgoing OSPF packets is 48.

Views

OSPF view

Predefined user roles

network-admin

Parameters

dscp-value: Specifies the DSCP value in the range of 0 to 63 for outgoing OSPF packets.

Examples

Set the DSCP value for outgoing OSPF packets to 63 in OSPF process 1.

```
<Switch> system-view
[Switch] ospf 1
[Switch-ospf-1] dscp 63
```

4.1.28. enable link-local-signaling

Use **enable link-local-signaling** to enable the OSPF link-local signaling (LLS) capability.

Use **undo enable link-local-signaling** to disable the OSPF LLS capability.

Syntax

enable link-local-signaling

undo enable link-local-signaling

Default

OSPF link-local signaling capability is disabled.

Views

OSPF view

Predefined user roles

network-admin

Examples

Enable link-local signaling for OSPF process 1.

```
<Switch> system-view
[Switch] ospf 1
[Switch-ospf-1] enable link-local-signaling
```

4.1.29. enable out-of-band-resynchronization

Use **enable out-of-band-resynchronization** to enable the OSPF out-of-band resynchronization (OOB-Resynch) capability.

Use **undo enable out-of-band-resynchronization** to disable the OSPF out-of-band resynchronization capability.

Syntax

enable out-of-band-resynchronization

undo enable out-of-band-resynchronization

Default

The OSPF out-of-band resynchronization capability is disabled.

Views

OSPF view

Predefined user roles

network-admin

Usage guidelines

Before you configure this command, enable the link-local signaling capability.

Examples

Enable the out-of-band resynchronization capability for OSPF process 1.

```
<Switch> system-view
[Switch] ospf 1
[Switch-ospf-1] enable link-local-signaling
[Switch-ospf-1] enable out-of-band-resynchronization
```

Related commands

enable link-local-signaling

4.1.30. event-log

Use **event-log** to set the number of OSPF logs.

Use **undo event-log** to remove the configuration.

Syntax

event-log { **lsa-flush** | **peer** | **spf** } **size** *count*

undo event-log { **lsa-flush** | **peer** | **spf** } **size**

Default

The device can generate a maximum of 10 logs for each type, including route calculation logs, LSA aging logs, and neighbor logs.

Views

OSPF view

Predefined user roles

network-admin

Parameters

lsa-flush: Specifies the number of LSA aging logs.

peer: Specifies the number of neighbor logs.

spf: Specifies the number of route calculation logs.

size *count*: Specifies the number of OSPF logs, in the range of 0 to 65535.

Examples

Set the number of route calculation logs to 50 in OSPF process 100.

```
<Switch> system-view
[Switch] ospf 100
[Switch-ospf-100] event-log spf size 50
```

4.1.31. fast-reroute (OSPF view)

Use **fast-reroute** to configure OSPF FRR.

Use **undo fast-reroute** to restore the default.

Syntax

fast-reroute { **lfa** [**abr-only**] | **route-policy** *route-policy-name* }

undo fast-reroute

Default

OSPF FRR is disabled.

Views

OSPF view

Predefined user roles

network-admin

Parameters

lfa: Uses the LFA algorithm to calculate a backup next hop for all routes.

abr-only: Uses the next hop of the route to the ABR as the backup next hop.

route-policy *route-policy-name*: Uses a routing policy to designate a backup next hop. The *route-policy-name* argument is a case-sensitive string of 1 to 63 characters.

Usage guidelines

Do not use the **fast-reroute lfa** command together with the **vlink-peer** command.

Examples

Enable FRR to calculate a backup next hop for all routes by using LFA algorithm in OSPF process 1.

```
<Switch> system-view
[Switch] ospf 1
[Switch-ospf-1] fast-reroute lfa
```

4.1.32. filter (OSPF area view)

Use **filter** to configure OSPF to filter inbound/outbound Type-3 LSAs on an ABR.

Use **undo filter** to disable Type-3 LSA filtering.

Syntax

filter { *ipv4-acl-number* | **prefix-list** *prefix-list-name* | **route-policy** *route-policy-name* } { **export** | **import** }

undo filter { **export** | **import** }

Default

Type-3 LSAs are not filtered.

Views

OSPF area view

Predefined user roles

network-admin

Parameters

ipv4-acl-number: Specifies an IPv4 ACL by its number in the range of 2000 to 3999 to filter inbound/outbound Type-3 LSAs.

prefix-list-name: Specifies an IP prefix list by its name, a case-sensitive string of 1 to 63 characters, to filter inbound/outbound Type-3 LSAs.

route-policy-name: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters, to filter inbound/outbound Type-3 LSAs.

export: Filters Type-3 LSAs advertised to other areas.

import: Filters Type-3 LSAs advertised into the local area.

Usage guidelines

This command applies only to an ABR.

Examples

Use IP prefix list **my-prefix-list** to filter inbound Type-3 LSAs. Use basic ACL 2000 to filter outbound Type-3 LSAs in OSPF Area 1.

```
<Switch> system-view
[Switch] ospf 100
[Switch-ospf-100] area 1
[Switch-ospf-100-area-0.0.0.1] filter prefix-list my-prefix-list import
[Switch-ospf-100-area-0.0.0.1] filter 2000 export
```

4.1.33. filter-policy export (OSPF view)

Use **filter-policy export** to configure OSPF to filter redistributed routes.

Use **undo filter-policy export** to remove the configuration.

Syntax

filter-policy { *ipv4-acl-number* | **prefix-list** *prefix-list-name* } **export** [*protocol* [*process-id*]]

undo filter-policy export [*protocol* [*process-id*]]

Default

OSPF does not filter redistributed routes.

Views

OSPF view

Predefined user roles

network-admin

Parameters

ipv4-acl-number: Specifies an IPv4 ACL by its number in the range of 2000 to 3999 to filter redistributed routes by destination address.

prefix-list-name: Specifies an IP prefix list by its name, a case-sensitive string of 1 to 63 characters, to filter redistributed routes by destination address.

protocol: Filters routes redistributed from the specified routing protocol. If you do not specify this argument, the command filters all redistributed routes.

process-id: Specifies a process by its ID in the range of 1 to 65535. This argument is available only when the *protocol* argument is **rip**, or **ospf**.

Usage guidelines

To use an advanced ACL (with a number from 3000 to 3999) in the command, configure the ACL using one of the following methods:

- To deny/permit a route with the specified destination, use the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* command.
- To deny/permit a route with the specified destination and mask, use the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* **destination** *dest-addr dest-wildcard* command.

The **source** keyword specifies the destination address of a route and the **destination** keyword specifies the subnet mask of the destination address. For the mask configuration to take effect, specify a contiguous subnet mask.

Examples

Configure OSPF process 100 to filter redistributed routes by using basic ACL 2000.

```
<Switch> system-view
[Switch] acl basic 2000
[Switch-acl-ipv4-basic-2000] rule deny source 192.168.10.0 0.0.0.255
[Switch-acl-ipv4-basic-2000] quit
[Switch] ospf 100
[Switch-ospf-100] filter-policy 2000 export
```

Configure advanced ACL 3000 to permit only route 113.0.0.0/16. Configure OSPF process 100 to filter redistributed routes by using advanced ACL 3000.

```
<Switch> system-view
[Switch] acl advanced 3000
[Switch-acl-ipv4-adv-3000] rule 10 permit ip source 113.0.0.0 0 destination 255.255.0.0
0
[Switch-acl-ipv4-adv-3000] rule 100 deny ip
[Switch-acl-ipv4-adv-3000] quit
[Switch] ospf 100
[Switch-ospf-100] filter-policy 3000 export
```

Related commands

import-route

4.1.34. filter-policy import (OSPF view)

Use **filter-policy import** to configure OSPF to filter routes calculated using received LSAs.

Use **undo filter-policy import** to restore the default.

Syntax

filter-policy { *ipv4-acl-number* [**gateway** *prefix-list-name*] | **gateway** *prefix-list-name* | **prefix-list** *prefix-list-name* [**gateway** *prefix-list-name*] | **route-policy** *route-policy-name* } **import**

undo filter-policy import

Default

OSPF does not filter routes calculated using received LSAs.

Views

OSPF view

Predefined user roles

network-admin

Parameters

ipv4-acl-number: Specifies an IPv4 ACL by its number in the range of 2000 to 3999 to filter received routes by destination.

gateway *prefix-list-name*: Specifies an IP prefix list by its name, a case-sensitive string of 1 to 63 characters, to filter received routes by next hop.

prefix-list *prefix-list-name*: Specifies an IP prefix list by its name, a case-sensitive string of 1 to 63 characters, to filter received routes by destination.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters, to filter received routes.

Usage guidelines

To use an advanced ACL (with a number from 3000 to 3999) in the command or in the specified routing policy, configure the ACL in one of the following ways:

- To deny/permit a route with the specified destination, use the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* command.
- To deny/permit a route with the specified destination and mask, use the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* **destination** *dest-addr dest-wildcard* command.

The **source** keyword specifies the destination address of a route and the **destination** keyword specifies the subnet mask of the destination address. For the mask configuration to take effect, specify a contiguous subnet mask.

Examples

Use basic ACL 2000 to filter received routes.

```
<Switch> system-view
[Switch] acl basic 2000
[Switch-acl-ipv4-basic-2000] rule deny source 192.168.10.0 0.0.0.255
[Switch-acl-ipv4-basic-2000] quit
```

```
[Switch] ospf 100
[Switch-ospf-100] filter-policy 2000 import
```

Configure advanced ACL 3000 to permit only route 113.0.0.0/16. Use ACL 3000 to filter received routes.

```
<Switch> system-view
[Switch] acl advanced 3000
[Switch-acl-ipv4-adv-3000] rule 10 permit ip source 113.0.0.0 0 destination 255.255.0.0
0
[Switch-acl-ipv4-adv-3000] rule 100 deny ip
[Switch-acl-ipv4-adv-3000] quit
[Switch] ospf 100
[Switch-ospf-100] filter-policy 3000 import
```

4.1.35. graceful-restart (OSPF view)

Use **graceful-restart** to enable OSPF GR.

Use **undo graceful-restart** to disable OSPF GR.

Syntax

graceful-restart [**ietf** | **nonstandard**] [**global** | **planned-only**] *

undo graceful-restart

Default

OSPF GR is disabled.

Views

OSPF view

Predefined user roles

network-admin

Parameters

ietf: Enables IETF GR.

nonstandard: Enables non-IETF GR.

global: Enables global GR. In global GR mode, a GR process can be completed only when all GR helpers exist. A GR process fails if a GR helper fails (for example, the interface connected to the GR helper goes down). If you do not specify this keyword, the command enables partial GR. In partial GR mode, a GR process can be completed if a GR helper exists.

planned-only: Enables only planned GR. If you do not specify this keyword, the command enables both planned GR and unplanned GR.

Usage guidelines

GR includes planned GR and unplanned GR.

- **Planned GR**—Manually restarts OSPF by using the **reset ospf process** command or performs an active/standby process switchover by using the **placement reoptimize** command. Before OSPF restart or active/standby switchover, the GR restarter sends Grace-LSAs to GR helpers.
- **Unplanned GR**—OSPF restarts or an active/standby switchover occurs because of device failure. Before OSPF restart or active/standby switchover, the GR restarter does not send Grace-LSAs to GR helpers.

Before enabling IETF GR for OSPF, enable Opaque LSA advertisement and reception with the **opaque-capability enable** command.

Before enabling non-IETF GR for OSPF, enable OSPF LLS with the **enable link-local-signaling** command and OOB-Resynch with the **enable out-of-band-resynchronization** command.

If you do not specify the **nonstandard** or **ietf** keyword, this command enables non-IETF GR for OSPF.

Examples

Enable IETF GR for OSPF process 1.

```
<Switch> system-view
[Switch] ospf 1
[Switch-ospf-1] opaque-capability enable
[Switch-ospf-1] graceful-restart ietf
```

Enable non-IETF GR for OSPF process 1.

```
<Switch> system-view
[Switch] ospf 1
[Switch-ospf-1] enable link-local-signaling
[Switch-ospf-1] enable out-of-band-resynchronization
[Switch-ospf-1] graceful-restart nonstandard
```

Related commands

enable link-local-signaling

enable out-of-band-resynchronization

opaque-capability enable

4.1.36. graceful-restart helper enable

Use **graceful-restart helper enable** to enable OSPF GR helper capability.

Use **undo graceful-restart helper enable** to disable OSPF GR helper capability.

Syntax

graceful-restart helper enable [**planned-only**]

undo graceful-restart helper enable

Default

OSPF GR helper capability is enabled.

Views

OSPF view

Predefined user roles

network-admin

Parameters

planned-only: Enables only planned GR for the GR helper. If you do not specify this keyword, the command enables both planned GR and unplanned GR for the GR helper.

Usage guidelines

The **planned-only** keyword is available only for the IETF GR helper.

Examples

Enable GR helper capability for OSPF process 1.

```
<Switch> system-view
[Switch] ospf 1
[Switch-ospf-1] graceful-restart helper enable
```

4.1.37. graceful-restart helper strict-lsa-checking

Use **graceful-restart helper strict-lsa-checking** to enable strict LSA checking capability for GR helper.

Use **undo graceful-restart helper strict-lsa-checking** to disable strict LSA checking capability for GR helper.

Syntax

graceful-restart helper strict-lsa-checking

undo graceful-restart helper strict-lsa-checking

Default

Strict LSA checking capability for GR helper is disabled.

Views

OSPF view

Predefined user roles

network-admin

Usage guidelines

When an LSA change on the GR helper is detected, the GR helper device exits the GR helper mode.

Examples

Enable strict LSA checking capability for GR helper in OSPF process 1.

```
<Switch> system-view
[Switch] ospf 1
[Switch-ospf-1] graceful-restart helper strict-lsa-checking
```

4.1.38. graceful-restart interval (OSPF view)

Use **graceful-restart interval** to set the GR interval.

Use **undo graceful-restart interval** to restore the default.

Syntax

graceful-restart interval *interval*

undo graceful-restart interval

Default

The GR interval is 120 seconds.

Views

OSPF view

Predefined user roles

network-admin

Parameters

interval: Specifies the GR interval in the range of 40 to 1800 seconds.

Usage guidelines

For GR restart to succeed, the value of the GR restart interval cannot be smaller than the maximum OSPF neighbor dead time of all the OSPF interfaces.

Examples

Set the GR interval for OSPF process 1 to 100 seconds.

```
<Switch> system-view
[Switch] ospf 1
[Switch-ospf-1] graceful-restart interval 100
```

Related commands

ospf timer dead

4.1.39. host-advertise

Use **host-advertise** to advertise a host route.

Use **undo host-advertise** to remove a host route.

Syntax

host-advertise *ip-address cost-value*

undo host-advertise *ip-address*

Default

No host route is advertised.

Views

OSPF area view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the IP address of a host.

cost-value: Specifies a cost for the route, in the range of 1 to 65535.

Examples

Advertise host route 1.1.1.1 with a cost of 100.

```
<Switch> system-view
[Switch] ospf 100
[Switch-ospf-100] area 0
[Switch-ospf-100-area-0.0.0.0] host-advertise 1.1.1.1 100
```

4.1.40. import-route (OSPF view)

Use **import-route** to redistribute AS-external routes from another routing protocol.

Use **undo import-route** to disable route redistribution from another routing protocol.

Syntax

import-route bgp [**allow-ibgp**] [**cost** *cost-value* | **nssa-only** | **route-policy** *route-policy-name* | **tag** *tag* | **type** *type*] *

undo import-route bgp

import-route { **direct** | **static** } [**cost** *cost-value* | **nssa-only** | **route-policy** *route-policy-name* | **tag** *tag* | **type** *type*] *

undo import-route { **direct** | **static** }

import-route { **ospf** | **rip** } [*process-id* | **all-processes**] [**allow-direct** | **cost** *cost-value* | **nssa-only** | **route-policy** *route-policy-name* | **tag** *tag* | **type** *type*] *

undo import-route { **ospf** | **rip** } [*process-id* | **all-processes**]

Default

OSPF does not redistribute AS-external routes from any other routing protocol.

Views

OSPF view

Predefined user roles

network-admin

Parameters

bgp: Redistributes BGP routes.

direct: Redistributes direct routes.

ospf: Redistributes OSPF routes.

rip: Redistributes RIP routes.

static: Redistributes static routes.

process-id: Specifies a process by its ID in the range of 1 to 65535. The default is 1.

all-processes: Redistributes routes from all the processes of the specified routing protocol.

allow-ibgp: Redistributes IBGP routes. The **import-route bgp** command redistributes only EBGP routes. Because the **import-route bgp allow-ibgp** command redistributes both EBGP and IBGP routes and might cause routing loops, use it with caution.

allow-direct: Redistributes the networks of the local interfaces enabled with the specified routing protocol. If you do not specify this keyword, the networks of the local interfaces are not redistributed. If you specify both the **allow-direct** keyword and the **route-policy** *route-policy-name* option, make sure the **if-match** rule defined in the routing policy does not conflict with the **allow-direct** keyword. For example, if you specify the **allow-direct** keyword, do not configure the **if-match route-type** rule for the routing policy. Otherwise, the **allow-direct** keyword does not take effect.

cost *cost-value*: Specifies a route cost in the range of 0 to 16777214. The default is 1.

nssa-only: Limits the route advertisement to the NSSA area by setting the P-bit of Type-7 LSAs to 0. If you do not specify this keyword, the P-bit of Type-7 LSAs is set to 1. If the router acts as both an ASBR and an ABR and **FULL** state neighbors exist in the backbone area, the P-bit is set to 0. This keyword applies to NSSA routers.

route-policy *route-policy-name*: Specifies a routing policy to filter redistributed routes. The *route-policy-name* argument is a case-sensitive string of 1 to 63 characters.

tag *tag*: Specifies a tag for external LSAs, in the range of 0 to 4294967295. The default is 1.

type *type*: Specifies a cost type, 1 or 2. The default is 2.

Usage guidelines

This command redistributes routes destined for other ASs from another protocol. AS external routes include the following types:

- **Type-1 external routes**—Have high credibility. The cost of Type-1 external routes is comparable with the cost of OSPF internal routes. The cost of a Type-1 external route equals the cost from the router to the ASBR plus the cost from the ASBR to the external route's destination.
- **Type-2 external routes**—Have low credibility. OSPF considers the cost from the ASBR to the destination of a Type-2 external route is much bigger than the cost from the ASBR to an OSPF internal router. The cost of a Type-2 external route equals the cost from the ASBR to the Type-2 external route's destination.

The **import-route** command redistributes only active routes. To display information about active routes, use the **display ip routing-table protocol** command. The **import-route** command cannot redistribute default external routes.

The **import-route nssa-only** command redistributes AS-external routes in Type-7 LSAs only into the NSSA area.

The **undo import-route** { **ospf** | **rip** } **all-processes** command removes only the configuration made by the **import-route** { **ospf** | **rip** } **all-processes** command, instead of the configuration made by the **import-route** { **ospf** | **rip** } *process-id* command.

Examples

Redistribute routes from RIP process 40 and specify the type, tag, and cost as 2, 33, and 50 for redistributed routes.

```
<Switch> system-view
[Switch] ospf 100
[Switch-ospf-100] import-route rip 40 type 2 tag 33 cost 50
```

Related commands

default-route-advertise (OSPF view)

4.1.41. log-peer-change

Use **log-peer-change** to enable logging for OSPF neighbor state changes.

Use **undo log-peer-change** to disable logging for OSPF neighbor state changes.

Syntax

log-peer-change

undo log-peer-change

Default

Logging for OSPF neighbor state changes is enabled.

Views

OSPF view

Predefined user roles

network-admin

Usage guidelines

This command enables output of OSPF neighbor state changes to the information center. The information center processes the logs according to user-defined output rules (whether and where to output logs). For more information about the information center, see *Network Management and Monitoring Configuration Guide*.

Examples

Disable logging for neighbor state changes for OSPF process 100.

```
<Switch> system-view
[Switch] ospf 100
[Switch-ospf-100] undo log-peer-change
```

4.1.42. lsa-arrival-interval

Use **lsa-arrival-interval** to set the LSA arrival interval.

Use **undo lsa-arrival-interval** to restore the default.

Syntax

lsa-arrival-interval *interval*

undo lsa-arrival-interval

Default

The LSA arrival interval is 1000 milliseconds.

Views

OSPF view

Predefined user roles

network-admin

Parameters

interval: Specifies the LSA arrival interval in the range of 0 to 60000 milliseconds.

Usage guidelines

If an LSA that has the same LSA type, LS ID, and originating router ID as the previous LSA is received within the interval, OSPF discards the LSA. This feature helps avoid overuse of system resources due to frequent network changes.

As a best practice, set the interval with the **lsa-arrival-interval** command to be smaller than or equal to the minimum interval set with the **lsa-generation-interval** command.

Examples

Set the LSA arrival interval to 200 milliseconds.

```
<Switch> system-view
[Switch] ospf 100
[Switch-ospf-100] lsa-arrival-interval 200
```

Related commands

lsa-generation-interval

4.1.43. lsa-generation-interval

Use **lsa-generation-interval** to set the OSPF LSA generation interval.

Use **undo lsa-generation-interval** to restore the default.

Syntax

lsa-generation-interval *maximum-interval* [*minimum-interval* [*incremental-interval*]]

undo lsa-generation-interval

Default

The maximum interval is 5 seconds, the minimum interval is 50 milliseconds, and the incremental interval is 200 milliseconds.

Views

OSPF view

Predefined user roles

network-admin

Parameters

maximum-interval: Specifies the maximum LSA generation interval in the range of 1 to 60 seconds.

minimum-interval: Specifies the minimum LSA generation interval in the range of 10 to 60000 milliseconds.

incremental-interval: Specifies the LSA generation incremental interval in the range of 10 to 60000 milliseconds.

Usage guidelines

When network changes are infrequent, LSAs are generated at the minimum interval. If network changes become frequent, the LSA generation interval is incremented by the incremental interval × 2^{n-2} for each generation until the maximum interval is reached. The value n is the number of generation times.

The minimum interval and the incremental interval cannot be greater than the maximum interval.

Examples

Set the maximum LSA generation interval to 2 seconds, minimum interval to 100 milliseconds, and incremental interval to 100 milliseconds.

```
<Switch> system-view
[Switch] ospf 100
[Switch-ospf-100] lsa-generation-interval 2 100 100
```

Related commands

lsa-arrival-interval

4.1.44. lsdb-overflow-interval

Use **lsdb-overflow-interval** to set the interval that OSPF exits overflow state.

Use **undo lsdb-overflow-interval** to restore the default.

Syntax

lsdb-overflow-interval *interval*

undo lsdb-overflow-interval

Default

The OSPF exit overflow interval is 300 seconds.

Views

OSPF view

Predefined user roles

network-admin

Parameters

interval: Specifies the interval that OSPF exits overflow state, in the range of 0 to 2147483647 seconds.

Usage guidelines

When the number of LSAs in the LSDB exceeds the upper limit, the LSDB is in an overflow state. In this state, OSPF does not receive any external LSAs and deletes the external LSAs generated by itself to save system resources.

You can configure the interval that OSPF exits overflow state. An interval of 0 indicates that the timer is not started and OSPF does not exit overflow state.

Examples

Set the OSPF exit overflow interval to 10 seconds.

```
<Switch> system-view
[Switch] ospf 100
[Switch-ospf-100] lsdb-overflow-interval 10
```

4.1.45. lsdb-overflow-limit

Use **lsdb-overflow-limit** to set the upper limit of external LSAs in the LSDB.

Use **undo lsdb-overflow-limit** to restore the default.

Syntax

lsdb-overflow-limit *number*

undo lsdb-overflow-limit

Default

The number of external LSAs is not limited.

Views

OSPF view

Predefined user roles

network-admin

Parameters

number: Specifies the upper limit of external LSAs in the LSDB, in the range of 1 to 1000000.

Examples

Set the upper limit of external LSAs to 400000.

```
<Switch> system-view
[Switch] ospf 100
[Switch-ospf-100] lsdb-overflow-limit 400000
```

4.1.46. maximum load-balancing (OSPF view)

Use **maximum load-balancing** to set the maximum number of equal-cost multi-path (ECMP) routes for load balancing.

Use **undo maximum load-balancing** to restore the default.

Syntax

maximum load-balancing *number*

undo maximum load-balancing

Default

8

Views

OSPF view

Predefined user roles

network-admin

Parameters

number: Specifies the maximum number of ECMP routes in the range of 1 to 8. No ECMP load balancing is available when the number is set to 1.

Examples

Set the maximum number of ECMP routes to 2.

```
<Switch> system-view
[Switch] ospf 100
[Switch-ospf-100] maximum load-balancing 2
```

Related commands

max-ecmp-num

4.1.47. non-stop-routing

> 🕮 **MEMO:**
>
> **non-stop-routing** command is supported from later software, including Version 7.2.16.

Use **non-stop-routing** to enable OSPF NSR.

Use **undo non-stop-routing** to disable OSPF NSR.

Syntax

non-stop-routing

undo non-stop-routing

Default

OSPF NSR is disabled.

Views

OSPF view

Predefined user roles

network-admin

Usage guidelines

This command takes effect only for the current process. As a best practice, enable OSPF NSR for each process if multiple OSPF processes exist.

OSPF NSR and OSPF GR are mutually exclusive. Do not configure the **non-stop-routing** command and the **graceful-restart** command at the same time.

Examples

Enable NSR for OSPF process 100.

```
<Switch> system-view
[Switch] ospf 100
```

```
[Switch-ospf-100] non-stop-routing
```

4.1.48. network (OSPF area view)

Use **network** to enable OSPF on the interface attached to the specified network in the area.

Use **undo network** to disable OSPF for the interface attached to the specified network in the area.

Syntax

network *ip-address wildcard-mask*

undo network *ip-address wildcard-mask*

Default

OSPF is not enabled for any interface.

Views

OSPF area view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the IP address of a network.

wildcard-mask: Specifies the wildcard mask of the IP address. For example, the wildcard mask of mask 255.0.0.0 is 0.255.255.255.

Usage guidelines

This command enables OSPF on the interface attached to the specified network. The interface's primary IP address must be in the specified network. If only the interface's secondary IP address is in the network, the interface cannot run OSPF.

Examples

Specify the interface whose primary IP address is on network 131.108.20.0/24 to run OSPF in Area 2.

```
<Switch> system-view
[Switch] ospf 100
[Switch-ospf-100] area 2
[Switch-ospf-100-area-0.0.0.2] network 131.108.20.0 0.0.0.255
```

Related commands

ospf

4.1.49. nssa (OSPF area view)

Use **nssa** to configure an area as an NSSA area.

Use **undo nssa** to restore the default.

Syntax

nssa [**default-route-advertise** * | **no-import-route** | **no-summary** | **translate-always** | **translator-stability-interval** *value*] *

undo nssa [**default-route-advertise** * | **no-import-route** | **no-summary** | **translate-always** | **translator-stability-interval**] *

Default

No area is configured as an NSSA area.

Views

OSPF area view

Predefined user roles

network-admin

Parameters

default-route-advertise: Used on an NSSA ABR or an ASBR only. With this keyword, an NSSA ABR redistributes a default route in a Type-7 LSA into the NSSA area. The ABR redistributes a default route regardless of whether a default route exists in the routing table. With this keyword, an ASBR redistributes a default route in a Type-7 LSA only when the default route exists in the routing table.

no-import-route: Used on an NSSA ABR to control the **import-route** command to not redistribute routes into the NSSA area.

no-summary: Used only on an ABR to advertise a default route in a Type-3 summary LSA into the NSSA area and to not advertise other summary LSAs into the area. The area is a totally NSSA area.

translate-always: Always translates Type-7 LSAs to Type-5 LSAs. This keyword takes effect only on an NSSA ABR.

translator-stability-interval *value*: Specifies the stability interval of the translator. During the interval, the translator can maintain its translating capability after another device becomes the new translator. The *value* argument is the stability interval in the range of 0 to 900 seconds and defaults to 0. A value of 0 means the translator does not maintain its translating capability when a new translator arises.

Usage guidelines

All routers attached to an NSSA area must be configured with the **nssa** command in area view.

If you specify the **translate-ignore-checking-backbone** keyword for an ABR, you must also specify the keyword for other ABRs in the NSSA area. This ensures that a translator can be elected among the ABRs.

Examples

Configure Area 1 as an NSSA area.

```
<Switch> system-view
[Switch] ospf 100
[Switch-ospf-100] area 1
[Switch-ospf-100-area-0.0.0.1] nssa
```

Related commands

default-cost (OSPF area view)

4.1.50. opaque-capability enable

Use **opaque-capability enable** to enable opaque LSA advertisement and reception.

Use **undo opaque-capability** to disable opaque LSA advertisement and reception.

Syntax

opaque-capability enable

undo opaque-capability

Default

The feature is enabled.

Views

OSPF view

Predefined user roles

network-admin

Usage guidelines

After the opaque LSA advertisement and reception capability is enabled, OSPF can receive and advertise Type-9, Type-10, and Type-11 opaque LSAs.

Examples

Disable opaque LSA advertisement and reception.

```
<Switch> system-view
[Switch] ospf 100
[Switch-ospf-100] undo opaque-capability
```

4.1.51. ospf

Use **ospf** to enable OSPF and enter OSPF view.

Use **undo ospf** to disable OSPF.

Syntax

ospf [*process-id* | **router-id** *router-id* | **vpn-instance** *vpn-instance-name*] *

undo ospf [*process-id*]

Default

OSPF is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535.

router-id *router-id*: Specifies an OSPF router ID in dotted decimal notation.

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the OSPF process runs on the public network.

Usage guidelines

You can enable multiple OSPF processes on a router and specify different router IDs for them.

Enable an OSPF process before performing other tasks.

For correct OSPF neighbor relationship establishment, do not bind an OSPF-enabled VLAN interface to an OpenFlow instance.

Examples

Enable OSPF process 100 and specify router ID 10.10.10.1.

```
<Switch> system-view
[Switch] ospf 100 router-id 10.10.10.1
[Switch-ospf-100]
```

4.1.52. ospf authentication-mode

Use **ospf authentication-mode** to set the authentication mode and key on an interface.

Use **undo ospf authentication-mode** to remove specified configuration.

Syntax

For MD5/HMAC-MD5 authentication:

ospf authentication-mode { **hmac-md5** | **md5** } *key-id* { **cipher** | **plain** } *string*

undo ospf authentication-mode { **hmac-md5** | **md5** } *key-id*

For simple authentication:

ospf authentication-mode simple { **cipher** | **plain** } *string*

undo ospf authentication-mode simple

Default

No authentication is performed for an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

hmac-md5: Specifies HMAC-MD5 authentication.

md5: Specifies MD5 authentication.

simple: Specifies simple authentication.

key-id: Specifies a key by its ID in the range of 1 to 255.

cipher: Specifies a key in encrypted form.

plain: Specifies a key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. This argument is case sensitive.

- In simple authentication mode, the plaintext form of the key is a string of 1 to 8 characters. The encrypted form of the key is a string of 33 to 41 characters.
- In MD5/HMAC-MD5 authentication mode, the plaintext form of the key is a string of 1 to 16 characters. The encrypted form of the key is a string of 33 to 53 characters.

Usage guidelines

To establish or maintain adjacencies, interfaces attached to the same network segment must have the same authentication mode and key.

If MD5 or HMAC-MD5 authentication is configured, you can configure multiple keys, each having a unique key ID and key string. To minimize the risk of key compromise, use only one key for an interface and delete the old key after key replacement.

To replace the key used for MD5 or HMAC-MD5 authentication on an interface, you must configure the new key before removing the old key from each router. OSPF uses the key rollover mechanism to ensure that the routers can pass authentication before the replacement is complete on the interface. After you configure a new key on a router, the router sends copies of

the same packet, each authenticated by a different key, including the new key and the keys in use. This practice continues until the router detects that all its neighbors have the new key.

The authentication algorithm can only be MD5 or HMAC-MD5 and the ID of keys used for authentication can only be in the range of 0 to 255.

Examples

On VLAN-interface 10, enable MD5 authentication, and set the interface key ID to 15 and the key to **123456** in plaintext form.

```
<Switch> system-view
[Switch] interface vlan-interface 10
[Switch-Vlan-interface10] ospf authentication-mode md5 15 plain 123456
```

On VLAN-interface 10, enable simple authentication, and set the key to **123456** in plaintext form.

```
<Switch> system-view
[Switch] interface vlan-interface 10
[Switch-Vlan-interface10] ospf authentication-mode simple plain 123456
```

Related commands

authentication-mode

4.1.53. ospf bfd enable

Use **ospf bfd enable** to enable BFD on an OSPF interface.

Use **undo ospf bfd enable** to disable BFD on an OSPF interface.

Syntax

ospf bfd enable [**echo**]

undo ospf bfd enable

Default

BFD for OSPF is disabled.

Views

Interface view

Predefined user roles

network-admin

Parameters

echo: Enables BFD single-hop echo detection. If you do not specify this keyword, the command enables BFD bidirectional control detection.

Examples

Enable BFD for OSPF on VLAN-interface 11.

```
<Switch> system-view
```

```
[Switch] ospf
[Switch-ospf-1] area 0
[Switch-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.255.255
[Switch] interface vlan-interface 11
[Switch-Vlan-interface11] ospf bfd enable
```

4.1.54. ospf cost (interface view)

Use **ospf cost** to set an OSPF cost for an interface.

Use **undo ospf cost** to restore the default.

Syntax

ospf cost *cost-value*

undo ospf cost

Default

An interface computes its OSPF cost according to the interface bandwidth. For a loopback interface, the cost is 0.

Views

Interface view

Predefined user roles

network-admin

Parameters

cost-value: Specifies an OSPF cost in the range of 0 to 65535 for a loopback interface, and in the range of 1 to 65535 for other interfaces.

Usage guidelines

If you do not execute this command, the interface automatically computes its OSPF cost.

Examples

Set the OSPF cost on VLAN-interface 10 to 65.

```
<Switch> system-view
[Switch] interface vlan-interface 10
[Switch-Vlan-interface10] ospf cost 65
```

Related commands

bandwidth-reference

4.1.55. ospf dr-priority

Use **ospf dr-priority** to set the router priority for DR/BDR election on an interface.

Use **undo ospf dr-priority** to restore the default value.

Syntax

ospf dr-priority *priority*

undo ospf dr-priority

Default

The router priority is 1.

Views

Interface view

Predefined user roles

network-admin

Parameters

priority: Specifies the router priority for the interface, in the range of 0 to 255.

Usage guidelines

The greater the value, the higher the priority for DR/BDR election. If a device has a priority of 0, it will not be elected as a DR or BDR.

Examples

Set the router priority on VLAN-interface 10 to 8.

```
<Switch> system-view
[Switch] interface vlan-interface 10
[Switch-Vlan-interface10] ospf dr-priority 8
```

4.1.56. ospf mib-binding

Use **ospf mib-binding** to bind an OSPF process to the public MIB.

Use **undo ospf mib-binding** to restore the default.

Syntax

ospf mib-binding *process-id*

undo ospf mib-binding

Default

The public MIB is bound to the OSPF process with the smallest process ID.

Views

System view

Predefined user roles

network-admin

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535.

Usage guidelines

To access information or data about an OSPF process in **RFC4750-OSPF.MIB**, use this command. To access information or data about an OSPF process in a private MIB for the device, you do not need to use this command. You can access information or data about all OSPF processes in the private MIBs.

If the specified process ID does not exist, a notification is displayed to report that the MIB binding configuration has failed.

Deleting an OSPF process that has been bound to the public MIB unbinds the OSPF process from the MIB, and re-binds the MIB to the OSPF process with the smallest process ID.

Examples

Bind OSPF process 100 to the public MIB.

```
<Switch> system-view
[Switch] ospf mib-binding 100
```

4.1.57. ospf mtu-enable

Use **ospf mtu-enable** to enable an interface to add the interface MTU into DD packets.

Use **undo ospf mtu-enable** to restore the default.

Syntax

ospf mtu-enable

undo ospf mtu-enable

Default

The MTU in DD packets is 0.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

After a virtual link is established through a Virtual-Template or Tunnel, two devices on the link from different vendors might have different MTU values. To make them consistent, restore the interfaces' MTU to the default value 0.

After you configure this command, the interface checks whether the MTU in a received DD packet is greater than its own MTU. If yes, the interface discards the packet.

Examples

Enable VLAN-interface 10 to add the interface MTU value into DD packets.

```
<Switch> system-view
```

```
[Switch] interface vlan-interface 10
[Switch-Vlan-interface10] ospf mtu-enable
```

4.1.58. ospf network-type

Use **ospf network-type** to specify the network type for an interface.

Use **undo ospf network-type** to restore the default.

Syntax

ospf network-type { **broadcast** | **nbma** | **p2mp** [**unicast**] | **p2p** }

undo ospf network-type

Default

The network type of an interface is broadcast.

Views

Interface view

Predefined user roles

network-admin

Parameters

broadcast: Specifies the network type as broadcast.

nbma: Specifies the network type as NBMA.

p2mp: Specifies the network type as P2MP.

unicast: Specifies the P2MP interface to unicast OSPF packets. By default, a P2MP interface multicasts OSPF packets.

p2p: Specifies the network type as P2P.

Usage guidelines

If a router on a broadcast network does not support multicast, configure the network type for the connected interfaces as NBMA.

When the network type of an interface is NBMA or P2MP unicast, you must use the **peer** command to specify the neighbor.

If only two routers run OSPF on a network, you can configure the network type for the connected interfaces as P2P.

When the network type of an interface is P2MP unicast, all OSPF packets are unicast by the interface.

Examples

Specify the OSPF network type for VLAN-interface 10 as NBMA.

```
<Switch> system-view
```

```
[Switch] interface vlan-interface 10
[Switch-Vlan-interface10] ospf network-type nbma
```

Related commands

ospf dr-priority

4.1.59. ospf peer sub-address enable

Use **ospf peer sub-address enable** to enable OSPF to establish neighbor relationships through the secondary IP addresses of an interface.

Use **undo ospf peer sub-address enable** to disable OSPF from establishing neighbor relationships through the secondary IP addresses of an interface.

Syntax

ospf peer sub-address enable [*ip-address*]

undo ospf peer sub-address enable

Default

OSPF cannot establish neighbor relationships through the secondary IP addresses of an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

ip-address: Specifies a secondary IP address of the interface in dotted decimal notation.

Usage guidelines

By default, OSPF uses the primary IP address of an interface to establish neighbor relationships.

You can execute this command to enable OSPF to establish neighbor relationships through both the primary and secondary IP addresses of an interface.

When you execute this command without specifying the *ip-address* argument, follow these guidelines:

- If you have advertised only the primary address of the interface in an area of an OSPF process, OSPF uses only the primary address to establish neighbor relationships. For OSPF to establish neighbor relationships through the secondary IP addresses, you must also advertise the secondary IP addresses in the same area of the same OSPF process.
- If the interface does not have a primary address but has multiple secondary addresses, OSPF uses the lowest secondary address to establish neighbor relationships. For OSPF to

establish neighbor relationships through the other secondary addresses, you must advertise these addresses in the same area of the same OSPF process.

When a customer-side device accesses the OSPF network through both M-LAG member devices in an M-LAG system, the M-LAG member devices provide Layer 3 gateway services. The gateway interfaces (such as VLAN interfaces) on different M-LAG member devices might have the same IP address and the same MAC address. In this case, the M-LAG member devices cannot establish OSPF neighbor relationships with the customer-side device. To resolve this issue, perform the following tasks:

1. Configure different M-LAG virtual IPv4 addresses for the gateway interfaces on different M-LAG member devices.
2. Execute the **ospf peer sub-address enable** *ip-address* command on each M-LAG member device, and set the ip-address argument to the M-LAG virtual IPv4 address of the gateway interface.

When you use the **ospf peer sub-address enable** *ip-address* command on an interface, follow these guidelines:

- After you use this command, OSPF uses only the specified address to establish neighbor relationships.
- To ensure successful OSPF neighbor relationship establishment, configure the specified address as the secondary address or the M-LAG virtual IPv4 address for the interface.
- If you execute this command multiple times, the most recent configuration takes effect.

After you execute the **ospf peer sub-address enable** command on a P2P OSPF interface, the device automatically checks the local and remote interface IP addresses before neighbor establishment. If the IP addresses belong to different networks, they cannot establish a neighbor relationship.

Examples

On interface VLAN-interface 10, enable OSPF to establish neighbor relationships through the secondary IP addresses of the interface.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospf peer sub-address enable
```

4.1.60. ospf timer dead

Use **ospf timer dead** to set the neighbor dead interval.

Use **undo ospf timer dead** to restore the default.

Syntax

ospf timer dead *seconds*

undo ospf timer dead

Default

The dead interval is 40 seconds for broadcast and P2P interfaces. The dead interval is 120 seconds for P2MP and NBMA interfaces.

Views

Interface view

Predefined user roles

network-admin

Parameters

seconds: Specifies the dead interval in the range of 1 to 2147483647 seconds.

Usage guidelines

If an interface receives no hello packet from a neighbor within the dead interval, the interface considers the neighbor down.

The dead interval on an interface is a minimum of four times the hello interval. Routers attached to the same segment must have the same dead interval.

Examples

Set the dead interval for VLAN-interface 10 to 60 seconds.

```
<Switch> system-view
[Switch] interface vlan-interface 10
[Switch-Vlan-interface10] ospf timer dead 60
```

Related commands

ospf timer hello

4.1.61. ospf timer hello

Use **ospf timer hello** to set the hello interval on an interface.

Use **undo ospf timer hello** to restore the default.

Syntax

ospf timer hello *seconds*

undo ospf timer hello

Default

The hello interval is 10 seconds for P2P and broadcast interfaces, and is 30 seconds for P2MP and NBMA interfaces.

Views

Interface view

Predefined user roles

network-admin

Parameters

seconds: Specifies the hello interval in the range of 1 to 65535 seconds.

Usage guidelines

The shorter the hello interval, the faster the topology converges, and the more resources are consumed. Make sure the hello interval on two neighboring interfaces is the same.

Examples

Set the hello interval on VLAN-interface to 20 seconds.

```
<Switch> system-view
[Switch] interface vlan-interface 10
[Switch-Vlan-interface10] ospf timer hello 20
```

Related commands

ospf timer dead

4.1.62. ospf timer poll

Use **ospf timer poll** to set the poll interval on an NBMA interface.

Use **undo ospf timer poll** to restore the default.

Syntax

ospf timer poll *seconds*

undo ospf timer poll

Default

The poll interval is 120 seconds on an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

seconds: Specifies the poll interval in the range of 1 to 2147483647 seconds.

Usage guidelines

When an NBMA interface finds its neighbor is down, it sends hello packets at the poll interval.

The poll interval must be a minimum of four times the hello interval.

Examples

Set the poll timer interval on VLAN-interface 10 to 130 seconds.

```
<Switch> system-view
[Switch] interface vlan-interface 10
[Switch-Vlan-interface10] ospf timer poll 130
```

Related commands

ospf timer hello

4.1.63. ospf timer retransmit

Use **ospf timer retransmit** to set the LSA retransmission interval on an interface.

Use **undo ospf timer retransmit** to restore the default.

Syntax

ospf timer retransmit *seconds*

undo ospf timer retransmit

Default

The LSA retransmission interval is 5 seconds on an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

seconds: Specifies the LSA retransmission interval in the range of 1 to 3600 seconds.

Usage guidelines

After sending an LSA, an interface waits for an acknowledgment packet. If the interface receives no acknowledgment within the retransmission interval, it retransmits the LSA.

To avoid unnecessary retransmissions, set an appropriate retransmission interval. For example, you can set a large retransmission interval value on a low-speed link.

Examples

Set the LSA retransmission interval to 8 seconds on VLAN-interface 10.

```
<Switch> system-view
[Switch] interface vlan-interface 10
[Switch-Vlan-interface10] ospf timer retransmit 8
```

4.1.64. ospf trans-delay

Use **ospf trans-delay** to set the LSA transmission delay on an interface.

Use **undo ospf trans-delay** to restore the default.

Syntax

ospf trans-delay *seconds*

undo ospf trans-delay

Default

The LSA transmission delay is 1 second.

Views

Interface view

Predefined user roles

network-admin

Parameters

seconds: Specifies the LSA transmission delay in the range of 1 to 3600 seconds.

Usage guidelines

Each LSA in the LSDB has an age that is incremented by 1 every second, but the age does not change during transmission. Adding a transmission delay into the age time is important in low speed networks.

Examples

Set the LSA transmission delay to 3 seconds on VLAN-interface 10.

```
<Switch> system-view
[Switch] interface vlan-interface 10
[Switch-Vlan-interface10] ospf trans-delay 3
```

4.1.65. peer (OSPF view)

Use **peer** to specify a neighbor in an NBMA or P2MP network.

Use **undo peer** to remove a neighbor in an NBMA or P2MP network.

Syntax

peer *ip-address* [**cost** *cost-value* | **dr-priority** *priority*]

undo peer *ip-address*

Default

No neighbor is specified.

Views

OSPF view

Predefined user roles

network-admin

Parameters

ip-address: Specifies a neighbor by its IP address.

cost *cost-value*: Specifies the cost to reach the neighbor, in the range of 1 to 65535.

dr-priority *priority*: Specifies the DR priority for the neighbor, in the range of 0 to 255. The default neighbor DR priority is 1.

Usage guidelines

In an NBMA or P2MP network, OSPF packets are sent in unicast, so you must use this command to specify neighbors.

The cost set with the **peer** command applies only to P2MP neighbors. If no cost is specified, the cost to the neighbor equals the local interface's cost.

A router uses the priority set with the **peer** command to determine whether to send a hello packet to the neighbor rather than for DR election. The DR priority set with the **ospf dr-priority** command is used for DR election.

Examples

Specify the neighbor 1.1.1.1.

```
<Switch> system-view
[Switch] ospf 100
[Switch-ospf-100] peer 1.1.1.1
```

Related commands

ospf dr-priority

4.1.66. preference (OSPF view)

Use **preference** to set a preference for OSPF.

Use **undo preference** to remove the configuration.

Syntax

preference [**ase**] { *preference* | **route-policy** *route-policy-name* } *

undo preference [**ase**]

Default

The preference is 10 for OSPF internal routes and 150 for OSPF external routes (ASE routes).

Views

OSPF view

Predefined user roles

network-admin

Parameters

ase: Specifies a preference for OSPF external routes. If you do not specify this keyword, the command sets a preference for OSPF internal routes.

preference: Specifies the preference value in the range of 1 to 255. A smaller value represents a higher preference.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters, to set a preference for the specified routes.

Usage guidelines

If multiple routing protocols find routes to the same destination, the router uses the route found by the protocol with the highest preference.

When the **route-policy** *route-policy-name* option is specified, the following preferences take effect:

- For routes matching the routing policy, the preference set in the routing policy takes effect.
- For other routes, the preference set with the **preference** command takes effect.

Examples

Set a preference of 200 for OSPF external routes.

```
<Switch> system-view
[Switch] ospf 100
[Switch-ospf-100] preference ase 200
```

Set a preference of 100 for OSPF internal routes matching the specified routing policy, and set a preference of 150 for other routes.

```
<Switch> system-view
[Switch] ip prefix-list test index 10 permit 100.1.1.0 24
[Switch] route-policy pre permit node 10
[Switch-route-policy-pre-10] if-match ip address prefix-list test
[Switch-route-policy-pre-10] apply preference 100
[Switch-route-policy-pre-10] quit
[Switch] ospf 100
[Switch-ospf-100] preference route-policy pre 150
```

4.1.67. reset ospf event-log

Use **reset ospf event-log** to clear OSPF log information.

Syntax

reset ospf [*process-id*] **event-log** [**lsa-flush** | **peer** | **spf**]

Views

User view

Predefined user roles

network-admin

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535. If you do not specify this argument, the command clears OSPF log information for all OSPF processes.

lsa-flush: Clears LSA aging log information.

peer: Clears neighbor log information.

spf: Clears route calculation log information.

Usage guidelines

If you do not specify a log type, this command clears all log information.

Examples

Clear OSPF route calculation log information for all OSPF processes.

```
<Switch> reset ospf event-log spf
```

Related commands

display ospf event-log

4.1.68. reset ospf process

Use **reset ospf process** to restart all OSPF processes or a specified process.

Syntax

reset ospf [*process-id*] **process** [**graceful-restart**]

Views

User view

Predefined user roles

network-admin

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535. If you do not specify a process, this command restarts all OSPF processes.

graceful-restart: Resets the OSPF process by using GR.

Usage guidelines

The **reset ospf process** command performs the following actions:

- Clears all invalid LSAs without waiting for their timeouts.
- Makes a newly configured router ID take effect.
- Starts a new DR/BDR election.
- Keeps previous OSPF configurations.

The system prompts you to select whether to restart OSPF process upon execution of this command.

Examples

Restart all OSPF processes.

```
<Switch> reset ospf process
Reset OSPF process? [Y/N]:y
```

4.1.69. reset ospf redistribution

Use **reset ospf redistribution** to restart route redistribution.

Syntax

reset ospf [*process-id*] **redistribution**

Views

User view

Predefined user roles

network-admin

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535. If you do not specify a process, this command restarts route redistribution for all OSPF processes.

Examples

Restart route redistribution.

```
<Switch> reset ospf redistribution
```

4.1.70. reset ospf statistics

Use **reset ospf statistics** to clear OSPF statistics.

Syntax

reset ospf [*process-id*] **statistics**

Views

User view

Predefined user roles

network-admin

Parameters

process-id: Clears the statistics for an OSPF process specified by its ID in the range of 1 to 65535.

Examples

Clear OSPF statistics for all processes.

```
<Switch> reset ospf statistics
```

Related commands

display ospf statistics

4.1.71. rfc1583 compatible

Use **rfc1583 compatible** to enable compatibility with RFC 1583.

Use **undo rfc1583 compatible** to disable compatibility with RFC 1583.

Syntax

rfc1583 compatible

undo rfc1583 compatible

Default

Compatibility with RFC 1583 is enabled.

Views

OSPF view

Predefined user roles

network-admin

Usage guidelines

RFC 1583 specifies a different method than RFC 2328 for selecting the optimal route to a destination in another AS. When multiple routes are available to the ASBR, OSPF selects the optimal route by using the following procedure:

1. Selects the route with the highest preference.
   - If RFC 2328 is compatible with RFC 1583, all these routes have equal preference.
   - If RFC 2328 is not compatible with RFC 1583, the intra-area route in a non-backbone area is preferred to reduce the burden of the backbone area. The inter-area route and intra-area route in the backbone area have equal preference.
2. Selects the route with lower cost if two routes have equal preference.
3. Selects the route with larger originating area ID if two routes have equal cost.

To avoid routing loops, set identical RFC 1583-compatibility on all routers in a routing domain.

Examples

Disable compatibility with RFC 1583.

```
<Switch> system-view
[Switch] ospf 100
[Switch-ospf-100] undo rfc1583 compatible
```

4.1.72. router id

Use **router id** to configure a global router ID.

Use **undo router id** to restore the default.

Syntax

router id *router-id*

undo router id

Default

No global router ID is configured.

Views

System view

Predefined user roles

network-admin

Parameters

router-id: Specifies the router ID, in the format of an IPv4 address.

Usage guidelines

OSPF uses a router ID to identify a device. If no router ID is specified, the global router ID is used.

If no global router ID is configured, the highest loopback interface IP address is used as the router ID. If no loopback interface IP address is available, the highest physical interface IP address is used, regardless of the interface status (up or down).

During an active/standby process switchover, the new active process checks whether the previously backed up router ID is valid. If not, the process selects a new router ID.

A new router ID is selected only when the interface IP address used as the router ID is removed or changed. Other events will not trigger a router ID re-selection. For example, router ID re-selection is not triggered in the following situations:

- The interface goes down.
- You change the router ID to the address of a loopback interface after a physical interface address is selected as the router ID.
- A higher interface IP address is configured as the router ID.

After a router ID is changed, you must use the **reset** command to enable it.

Examples

Configure a global router ID as 1.1.1.1.

```
<Switch> system-view
[Switch] router id 1.1.1.1
```

4.1.73. silent-interface (OSPF view)

Use **silent-interface** to disable an interface or all interfaces from receiving and sending OSPF packets.

Use **undo silent-interface** to remove the configuration.

Syntax

silent-interface { *interface-type interface-number* | **all** }

undo silent-interface { *interface-type interface-number* | **all** }

Default

An interface can receive and send OSPF packets.

Views

OSPF view

Predefined user roles

network-admin

Parameters

interface-type interface-number: Specifies an interface by its type and number.

all: Specifies all interfaces.

Usage guidelines

To disable a network from receiving and sending OSPF routes, use the command on the interface connected to the network.

Examples

Disable VLAN-interface 10 from receiving and sending OSPF packets.

```
<Switch> system-view
[Switch] ospf 100
[Switch-ospf-100] silent-interface vlan-interface 10
```

4.1.74. snmp-agent trap enable ospf

Use **snmp-agent trap enable ospf** to enable SNMP notifications for OSPF.

Use **undo snmp-agent trap enable ospf** to disable SNMP notifications for OSPF.

Syntax

snmp-agent trap enable ospf [**authentication-failure** | **bad-packet** | **config-error** | **grhelper-status-change** | **grrestarter-status-change** | **if-state-change** | **lsa-maxage** | **lsa-originate** | **lsdb-approaching-overflow** | **lsdb-overflow** | **neighbor-state-change** | **nssatranslator-status-change** | **retransmit** | **virt-authentication-failure** | **virt-bad-packet** | **virt-config-error** | **virt-retransmit** | **virtgrhelper-status-change** | **virtif-state-change** | **virtneighbor-state-change**] *

undo snmp-agent trap enable ospf [**authentication-failure** | **bad-packet** | **config-error** | **grhelper-status-change** | **grrestarter-status-change** | **if-state-change** | **lsa-maxage** | **lsa-originate** |

lsdb-approaching-overflow | **lsdb-overflow** | **neighbor-state-change** | **nssatranslator-status-change** | **retransmit** | **virt-authentication-failure** | **virt-bad-packet** | **virt-config-error** | **virt-retransmit** | **virtgrhelper-status-change** | **virtif-state-change** | **virtneighbor-state-change**] *

Default

SNMP notifications for OSPF are enabled.

Views

System view

Predefined user roles

network-admin

Parameters

authentication-failure: Specifies notifications about authentication failures on an interface.

bad-packet: Specifies notifications about error messages received on an interface.

config-error: Specifies notifications about error configuration of an interface.

grhelper-status-change: Specifies notifications about GR helper state change.

grrestarter-status-change: Specifies notifications about GR restarter state change.

if-state-change: Specifies notifications about interface state change.

lsa-maxage: Specifies LSA max age notifications.

lsa-originate: Specifies notifications about locally generated LSAs.

lsdb-approaching-overflow: Specifies notifications about approaching LSDB overflows.

lsdb-overflow: Specifies LSDB overflow notifications.

neighbor-state-change: Specifies notifications about neighbor state change.

nssatranslator-status-change: Specifies notifications about NSSA translator state change.

retransmit: Specifies notifications about packets that are received and forwarded on an interface.

virt-authentication-failure: Specifies notifications about authentication failures on a virtual interface.

virt-bad-packet: Specifies notifications about error messages received on a virtual interface.

virt-config-error: Specifies notifications about error configuration of a virtual interface.

virt-retransmit: Specifies notifications about packets that are received and forwarded on a virtual interface.

virtgrhelper-status-change: Specifies notifications about neighbor GR helper state changes of a virtual interface.

virtif-state-change: Specifies notifications about virtual interface state change.

virtneighbor-state-change: Specifies notifications about the neighbor state change of a virtual interface.

Examples

Disable SNMP notifications for OSPF.

```
<Switch> system-view
[Switch] undo snmp-agent trap enable ospf
```

4.1.75. spf-schedule-interval (OSPF view)

Use **spf-schedule-interval** to set the OSPF SPF calculation interval.

Use **undo spf-schedule-interval** to restore the default.

Syntax

spf-schedule-interval *maximum-interval* [*minimum-interval* [*incremental-interval*]]

undo spf-schedule-interval

Default

The maximum calculation interval is 5 seconds, the minimum interval is 50 milliseconds, and the incremental interval is 200 milliseconds.

Views

OSPF view

Predefined user roles

network-admin

Parameters

maximum-interval: Specifies the maximum OSPF SPF calculation interval in the range of 1 to 60 seconds.

minimum-interval: Specifies the minimum OSPF SPF calculation interval in the range of 10 to 60000 milliseconds.

incremental-interval: Specifies the incremental OSPF SPF calculation interval in the range of 10 to 60000 milliseconds.

Usage guidelines

Based on the LSDB, an OSPF router uses SPF to calculate a shortest path tree with itself as the root. OSPF uses the shortest path tree to determine the next hop to a destination. By adjusting the SPF calculation interval, you can prevent overconsumption of bandwidth and router resources due to frequent topology changes.

For a stable network, the minimum interval is used. If network changes become frequent, the SPF calculation interval is incremented by the incremental interval × 2^{n-2} for each calculation until the maximum interval is reached. The value n is the number of calculation times.

The minimum interval and the incremental interval cannot be greater than the maximum interval.

Examples

Set the maximum SPF calculation interval to 10 seconds, minimum interval to 500 milliseconds, and incremental interval to 300 milliseconds.

```
<Switch> system-view
[Switch] ospf 100
[Switch-ospf-100] spf-schedule-interval 10 500 300
```

4.1.76. stub (OSPF area view)

Use **stub** to configure an area as a stub area.

Use **undo stub** to restore the default.

Syntax

stub [**default-route-advertise-always** | **no-summary**] *

undo stub

Default

No area is a stub area.

Views

OSPF area view

Predefined user roles

network-admin

Parameters

default-route-advertise-always: Enables the ABR to advertise a default route in a Type-3 LSA into the stub area regardless of whether **FULL**-state neighbors exist in the backbone area. If you do not specify this keyword, the ABR advertises a default route in a Type-3 LSA into the stub area only when a minimum of one **FULL**-state neighbor exists in the backbone area.

no-summary: Enables the ABR to advertise only a default route in a Type-3 LSA into the stub area without advertising any other Type-3 LSAs. The area is a totally stub area.

Usage guidelines

To configure an area as a stub area, use the **stub** command on all routers attached to the area.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure Area 1 as a stub area.

```
<Switch> system-view
[Switch] ospf 100
[Switch-ospf-100] area 1
[Switch-ospf-100-area-0.0.0.1] stub
```

Related commands

default-cost (OSPF area view)

4.1.77. stub-router (OSPF view)

Use **stub-router** to configure a router as a stub router.

Use **undo stub-router** to restore the default.

Syntax

stub-router

undo stub-router

Default

The router is not configured as a stub router.

Views

OSPF view

Predefined user roles

network-admin

Usage guidelines

The router LSAs sent by the stub router over different links contain different link type values. A value of 3 represents a link to a stub network, and the cost of the link is not changed. A value of 1, 2, or 4 represents a point-to-point link, a link to a transit network, or a virtual link. The cost of these links is set to 65535. Neighbors on such links will not send packets to the stub router as long as they have a route with a smaller cost.

Examples

Configure a stub router.

```
<Switch> system-view
[Switch] ospf 100
[Switch-ospf-100] stub-router
```

4.1.78. transmit-pacing

Use **transmit-pacing** to set the LSU transmission interval and the maximum number of LSU packets that can be sent at each interval.

Use **undo transmit-pacing** to restore the default.

Syntax

transmit-pacing interval *interval* **count** *count*

undo transmit-pacing

Default

An OSPF interface sends a maximum of three LSU packets every 20 milliseconds.

Views

OSPF view

Predefined user roles

network-admin

Parameters

interval *interval*: Specifies an interval at which an interface sends LSU packets, in the range of 10 to 1000 milliseconds. If the router has multiple OSPF interfaces, increase this interval to reduce the total number of LSU packets sent by the router every second.

count *count*: Specifies the maximum number of LSU packets sent by an interface at each interval, in the range of 1 to 200. If the router has multiple OSPF interfaces, decrease the maximum number to reduce the total number of LSU packets sent by the router every second.

Examples

Configure all the interfaces running OSPF process 1 to send a maximum of 10 LSU packets every 30 milliseconds.

```
<Switch> system-view
[Switch] ospf 1
[Switch-ospf-1] transmit-pacing interval 30 count 10
```

4.1.79. vlink-peer (OSPF area view)

Use **vlink-peer** to configure a virtual link.

Use **undo vlink-peer** to remove a virtual link.

Syntax

vlink-peer *router-id* [**dead** *seconds* | **hello** *seconds* | { { **hmac-md5** | **md5** } *key-id* { **cipher** | **plain** } *string* | **simple** { **cipher** | **plain** } *string* } | **retransmit** *seconds* | **trans-delay** *seconds*] *

undo vlink-peer *router-id* [**dead** | **hello** | { **hmac-md5** | **md5** } *key-id* | **retransmit** | **simple** | **trans-delay**] *

Default

No virtual links exist.

Views

OSPF area view

Predefined user roles

network-admin

Parameters

router-id: Specifies the router ID of the neighbor on the virtual link.

dead *seconds*: Specifies the dead interval in the range of 1 to 32768 seconds. The default is 40. The dead interval must be identical with that on the virtual link neighbor, and a minimum of four times the hello interval.

hello *seconds*: Specifies the hello interval in the range of 1 to 8192 seconds. The default is 10. It must be identical with the hello interval on the virtual link neighbor.

hmac-md5: Specifies the HMAC-MD5 authentication mode.

md5: Specifies the MD5 authentication mode.

simple: Specifies the simple authentication mode.

key-id: Specifies the key ID for MD5 or HMAC-MD5 authentication, in the range of 1 to 255.

cipher: Specifies a key in encrypted form.

plain: Specifies a key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. This argument is case sensitive.

- In simple authentication mode, the plaintext form of the key is a string of 1 to 8 characters. The encrypted form of the key is a string of 33 to 41 characters.
- In MD5/HMAC-MD5 authentication mode, the plaintext form of the key is a string of 1 to 16 characters. The encrypted form of the key is a string of 33 to 53 characters.

retransmit *seconds*: Specifies the retransmission interval in the range of 1 to 3600 seconds. The default is 5.

trans-delay *seconds*: Specifies the transmission delay interval in the range of 1 to 3600 seconds. The default is 1.

Usage guidelines

As defined in RFC 2328, all non-backbone areas must maintain connectivity to the backbone. You can use the **vlink-peer** command to configure a virtual link to connect an area to the backbone.

When you configure this command, follow these guidelines:

- The smaller the hello interval is, the faster the network converges, and the more network resources are consumed.
- A retransmission interval that is too small can cause unnecessary retransmissions. A large value is appropriate for a low speed link.
- Specify an appropriate transmission delay with the **trans-delay** keyword.

You can specify either MD5/HMAC-MD5 authentication or simple authentication for a virtual link. For MD5/HMAC-MD5 authentication, you can configure multiple keys by executing this command multiple times, and each command must have a unique key ID and key string.

To modify the key of a virtual link, perform the following key rollover configurations:

1. Configure a new MD5/HMAC-MD5 authentication key for the virtual link on the local device. If the new key is not configured on the neighbor device, MD5/HMAC-MD5 authentication key rollover is triggered. During key rollover, OSPF sends multiple packets that contain both the new and old MD5/HMAC-MD5 authentication keys to ensure that the neighbor device can pass the authentication.
2. Configure the new MD5/HMAC-MD5 authentication key on the neighbor device. When the local device receives packets with the new key from the neighbor device, it exits MD5 key rollover.
3. Delete the old MD5/HMAC-MD5 authentication key from the local device and the neighbor. This step helps prevent attacks from devices that use the old key for communication and reduces system resources and bandwidth consumption caused by key rollover.

OSPF supports the MD5 and HMAC-MD5 authentication algorithms.

The ID of keys used for authentication can only be in the range of 0 to 255.

Examples

Configure a virtual link to the neighbor with router ID 1.1.1.1.

```
<Switch> system-view
[Switch] ospf 100
[Switch-ospf-100] area 2
[Switch-ospf-100-area-0.0.0.2] vlink-peer 1.1.1.1
```

Related commands

authentication-mode

display ospf vlink

Contents

A page of this section is **5-x-x**

5. BGP commands 5-1
5.1. BGP commands 5-1
5.1.1. additional-paths select-best 5-1
5.1.2. address-family ipv4 5-2
5.1.3. address-family ipv6 5-3
5.1.4. aggregate 5-3
5.1.5. balance 5-6
5.1.6. balance as-path-neglect 5-7
5.1.7. bestroute compare-med 5-8
5.1.8. bestroute med-confederation 5-9
5.1.9. bgp 5-10
5.1.10. compare-different-as-med 5-11
5.1.11. confederation id 5-12
5.1.12. confederation nonstandard 5-13
5.1.13. confederation peer-as 5-14
5.1.14. dampening 5-14
5.1.15. default local-preference 5-16
5.1.16. default med 5-17
5.1.17. default-route imported 5-18
5.1.18. display bgp group 5-19
5.1.19. display bgp network 5-22
5.1.20. display bgp paths 5-23
5.1.21. display bgp peer 5-24
5.1.22. display bgp routing-table dampened 5-32
5.1.23. display bgp routing-table flap-info 5-34
5.1.24. display bgp routing-table ipv4 unicast 5-37
5.1.25. display bgp routing-table ipv6 unicast 5-45
5.1.26. ebgp-interface-sensitive 5-51
5.1.27. filter-policy export 5-52
5.1.28. filter-policy import 5-55
5.1.29. graceful-restart 5-56
5.1.30. graceful-restart timer restart 5-57
5.1.31. graceful-restart timer wait-for-rib 5-58
5.1.32. group 5-59
5.1.33. import-route 5-60
5.1.34. ip vpn-instance (BGP instance view) 5-62
5.1.35. log-peer-change 5-64
5.1.36. network 5-65
5.1.37. non-stop-routing 5-66
5.1.38. network short-cut 5-67
5.1.39. peer additional-paths 5-68
5.1.40. peer advertise additional-paths best 5-70
5.1.41. peer advertise-community 5-71
5.1.42. peer advertise-ext-community 5-73
5.1.43. peer allow-as-loop 5-75
5.1.44. peer as-number (for a BGP peer group) 5-79
5.1.45. peer as-number (for a BGP peer) 5-80
5.1.46. peer as-path-acl 5-81
5.1.47. peer bfd 5-83
5.1.48. peer capability-advertise conventional 5-84
5.1.49. peer capability-advertise route-refresh 5-86
5.1.50. peer connect-interface 5-87

5.1.51. peer default-route-advertise ····· 5-89
5.1.52. peer description ····· 5-91
5.1.53. peer ebgp-max-hop ····· 5-92
5.1.54. peer enable ····· 5-93
5.1.55. peer fake-as ····· 5-95
5.1.56. peer filter-policy ····· 5-96
5.1.57. peer group ····· 5-98
5.1.58. peer ignore ····· 5-100
5.1.59. peer keep-all-routes ····· 5-102
5.1.60. peer log-change ····· 5-104
5.1.61. peer next-hop-local ····· 5-105
5.1.62. peer password ····· 5-107
5.1.63. peer preferred-value ····· 5-108
5.1.64. peer prefix-list ····· 5-110
5.1.65. peer public-as-only ····· 5-112
5.1.66. peer reflect-client ····· 5-113
5.1.67. peer route-limit ····· 5-115
5.1.68. peer route-policy ····· 5-117
5.1.69. peer route-update-interval ····· 5-119
5.1.70. peer source-address ····· 5-120
5.1.71. peer substitute-as ····· 5-122
5.1.72. peer timer ····· 5-124
5.1.73. preference ····· 5-125
5.1.74. reflect between-clients ····· 5-126
5.1.75. reflector cluster-id ····· 5-127
5.1.76. refresh bgp ····· 5-128
5.1.77. reset bgp ····· 5-130
5.1.78. reset bgp all ····· 5-132
5.1.79. reset bgp dampening ····· 5-132
5.1.80. reset bgp flap-info ····· 5-133
5.1.81. router id ····· 5-135
5.1.82. router-id (BGP instance view) ····· 5-136
5.1.83. router-id (BGP-VPN instance view) ····· 5-137
5.1.84. snmp-agent trap enable bgp ····· 5-138
5.1.85. summary automatic ····· 5-139
5.1.86. timer ····· 5-140

5. BGP commands

5.1. BGP commands

5.1.1. additional-paths select-best

Use **additional-paths select-best** to set the maximum total number of Add-Path optimal routes that can be advertised to all peers.

Use **undo additional-paths select-best** to restore the default.

Syntax

additional-paths select-best *best-number*

undo additional-paths select-best

Default

A maximum of one Add-Path optimal route can be advertised to all peers.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP IPv6 unicast address family view

BGP-VPN IPv6 unicast address family view

Predefined user roles

network-admin

Parameters

best-number: Specifies the maximum total number of Add-Path optimal routes that can be advertised to all peers, in the range of 2 to 32.

Usage guidelines

The number of optimal routes cannot exceed the maximum total number of Add-Path optimal routes that can be advertised to all peers.

Examples

In BGP IPv4 unicast address family view, set the maximum total number to 3 for Add-Path optimal routes that can be advertised to all peers.

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default] address-family ipv4 unicast
[Switch-bgp-default-ipv4] additional-paths select-best 3
```

Related commands

peer additional-paths

peer advertise additional-paths best

5.1.2. address-family ipv4

Use **address-family ipv4** to create the BGP IPv4 unicast address family, or BGP-VPN IPv4 unicast address family, and enter its view, or enter the view of the existing address family.

Use **undo address-family ipv4** to remove the BGP IPv4 unicast address family, or BGP-VPN IPv4 unicast address family, and all its configurations.

Syntax

address-family ipv4 [**unicast**]

undo address-family ipv4 [**unicast**]

Default

No BGP IPv4 unicast address family, or BGP-VPN IPv4 unicast address family exists.

Views

BGP instance view

BGP-VPN instance view

Predefined user roles

network-admin

Parameters

unicast: Specifies the IPv4 unicast address family. If this command is executed with the **unicast** keyword in BGP instance view, it places you into BGP IPv4 unicast address family view. If this command is executed with the **unicast** keyword in BGP-VPN instance view, it places you into BGP-VPN IPv4 unicast address family view.

Usage guidelines

Configurations made in BGP IPv4 unicast address family view apply only to the BGP IPv4 unicast routes and peers of the public network.

Configurations made in BGP-VPN IPv4 unicast address family view apply only to the BGP IPv4 unicast routes and peers of the specified VPN instance.

Examples

In BGP instance view, create the BGP IPv4 unicast address family and enter its view.

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default] address-family ipv4 unicast
[Switch-bgp-default-ipv4]
```

5.1.3. address-family ipv6

Use **address-family ipv6** to create the BGP IPv6 unicast address family, or BGP-VPN IPv6 unicast address family, and enter its view, or enter the view of the existing address family.

Use **undo address-family ipv6** to remove the BGP IPv6 unicast address family, or BGP-VPN IPv6 unicast address family, and all its configurations.

Syntax

address-family ipv6 [**unicast**]

undo address-family ipv6 [**unicast**]

Default

No BGP IPv6 unicast address family, or BGP-VPN IPv6 unicast address family exists.

Views

BGP instance view

BGP-VPN instance view

Predefined user roles

network-admin

Parameters

unicast: Specifies the IPv6 unicast address family. If this command is executed with the **unicast** keyword in BGP instance view, it places you into BGP IPv6 unicast address family view. If this command is executed with the **unicast** keyword in BGP-VPN instance view, it places you into BGP-VPN IPv6 unicast address family view.

Usage guidelines

Configurations made in BGP IPv6 unicast address family view apply only to the BGP IPv6 unicast routes and peers of the public network.

Configurations made in BGP-VPN IPv6 unicast address family view apply only to the BGP IPv6 unicast routes and peers of the specified VPN instance.

Examples

In BGP instance view, create the BGP IPv6 unicast address family and enter its view.

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default] address-family ipv6 unicast
[Switch-bgp-default-ipv6]
```

5.1.4. aggregate

Use **aggregate** to create a summary route in the BGP routing table.

Use **undo aggregate** to remove a summary route.

Syntax

In BGP IPv4 unicast address family view/BGP-VPN IPv4 unicast address family view:

aggregate *ipv4-address* { *mask-length* | *mask* } [**as-set** | **attribute-policy** *route-policy-name* | **detail-suppressed** | **origin-policy** *route-policy-name* | **suppress-policy** *route-policy-name*] *

undo aggregate ipv4-address { *mask-length* | *mask* }

In BGP IPv6 unicast address family view:

aggregate *ipv6-address prefix-length* [**as-set** | **attribute-policy** *route-policy-name* | **detail-suppressed** | **origin-policy** *route-policy-name* | **suppress-policy** *route-policy-name*] *

undo aggregate *ipv6-address prefix-length*

Default

No summary routes are configured.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP IPv6 unicast address family view

Predefined user roles

network-admin

Parameters

ipv4-address: Specifies an IPv4 summary address.

mask-length: Specifies a mask length for the IPv4 summary address, in the range of 0 to 32.

mask: Specifies a mask for the IPv4 summary address, in dotted decimal notation.

ipv6-address: Specifies an IPv6 summary address.

prefix-length: Specifies a prefix length for the IPv6 summary address, in the range of 0 to 128.

as-set: Enables the AS_PATH attribute of the summary route to contain the AS path information for all summarized routes. The AS_PATH attribute is of the AS_SET type that requires no sequence when arranging AS numbers. If you do not specify this keyword, the AS_PATH attribute of the summary route contains only the AS number of the local router.

attribute-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters, to set attributes for the summary route.

detail-suppressed: Advertises only the summary route. If you do not specify this keyword, BGP advertises both the summary route and the more specific routes.

origin-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters, to select routes to be summarized.

suppress-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters, to filter more specific routes to be advertised. Routes permitted by the specified routing policy are not advertised. Routes denied by the specified routing policy are advertised.

Usage guidelines

This command creates a summary route. If the BGP routing table has routes whose destination addresses fall within the specified network, the summary route is added to the BGP routing table. For example, if two routes 10.1.1.0/24 and 10.1.2.0/24 exist in the BGP routing table, configuring the **aggregate 10.1.0.0 16** command creates a summary route 10.1.0.0/16.

If the summarized routes have different ORIGIN attributes, the summary route selects the ORIGIN attribute in the sequence of INCOMPLETE, EGP, and IGP. For example, if the ORIGIN attributes of the summarized routes include INCOMPLETE and IGP, the ORIGIN attribute of the summary route is INCOMPLETE.

The COMMUNITY attribute of the summary route includes all the COMMUNITY (or extended community) attribute values if the routes have the following details:

- Summarized routes have different COMMUNITY (or extended community) attribute values.
- The summary route does not have the ATOMIC_AGGREGATE attribute.

Table 5-1 Functions of the keywords

Keywords	Function
as-set	Enables the summary route to carry the AS path information for all summarized routes. This feature can help avoid routing loops. However, if many routes are summarized and are changed frequently, do not specify this keyword. This configuration causes the summary route to flap with the more specific routes.
attribute-policy	Sets attributes except the AS-PATH attribute for the summary route. The **peer route-policy** command can achieve the same purpose. If you modify the AS_PATH attribute of the summary route through the routing policy specified by the **attribute-policy** keyword, you cannot specify the **as-set** keyword. Modifying the AS_PATH attribute of the summary route might cause routing loops.
detail-suppressed	Disables advertisement of all more specific routes. To disable advertisement of some more specific routes, use the **suppress-policy** keyword or the **peer filter-policy** command.
origin-policy	Summarizes only routes matching a routing policy. If the destination address of a route falls within the summary network but does not match the routing policy, the route is not summarized. It is not controlled by the **detail-suppressed** and **suppress-policy** keywords. There is no need to configure **apply** clauses for the routing policy applied by the **origin-policy** keyword because they do not

Keywords	Function
	take effect.
suppress-policy	Disables advertisement of some more specific routes filtered by a routing policy. The routing policy uses **if-match** clauses to filter routes. There is no need to configure **apply** clauses for the routing policy applied by the **suppress-policy** keyword because they do not take effect.

Examples

In BGP IPv4 unicast address family view, create summary route 1.1.0.0/16 in the BGP routing table.

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default] address-family ipv4 unicast
[Switch-bgp-default-ipv4] aggregate 1.1.0.0 255.255.0.0
```

Related commands

display bgp routing-table ipv4 unicast

display bgp routing-table ipv6 unicast

summary automatic

5.1.5. balance

Use **balance** to enable load balancing and set the maximum number of BGP ECMP routes for load balancing.

Use **undo balance** to disable load balancing.

Syntax

balance [**ebgp** | **eibgp** | **ibgp**] *number*

undo balance [**ebgp** | **eibgp** | **ibgp**]

Default

Load balancing is disabled.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP IPv6 unicast address family view

BGP-VPN IPv6 unicast address family view

Predefined user roles

network-admin

Parameters

ebgp: Enables load balancing over EBGP routes.

eibgp: Enables load balancing between EBGP and IBGP routes.

ibgp: Enables load balancing over IBGP routes.

number: Specifies the maximum number of BGP ECMP routes for load balancing, in the range of 1 to 8. When it is set to 1, load balancing is disabled.

Usage guidelines

Unlike IGP, BGP has no explicit metric for making load balancing decision. Instead, it implements load balancing by modifying route selection rules.

BGP uses the following load balancing criteria to determine load balanced routes:

- The routes have the same ORIGIN, LOCAL_PREF, and MED attributes.
- The routes meet the following requirements on the AS_PATH attribute:
  - If the **balance as-path-neglect** command is configured or only the **balance as-path-neglect** command is configured, the routes can have different AS_PATH attributes.
  - If the **balance as-path-neglect** is not configured, the routes must have the same AS_PATH attribute.

If you do not specify the **ibgp**, **eibgp**, or **ebgp** keyword, this command enables load balancing over EBGP routes and IBGP routes, but not between EBGP and IBGP routes.

After you execute the **balance eibgp** *number* command, the **balance** [**ebgp** | **ibgp**] *number* and **undo balance** [**ebgp** | **ibgp**] commands cannot be executed; and vice versa.

Examples

In BGP IPv4 unicast address family view, enable load balancing and set the maximum number of BGP ECMP routes used for load balancing to 2.

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default] address-family ipv4 unicast
[Switch-bgp-default-ipv4] balance 2
```

Related commands

balance as-path-neglect

max-ecmp-num

5.1.6. balance as-path-neglect

Use **balance as-path-neglect** to enable BGP to ignore the AS_PATH attribute when it implements load balancing.

Use **undo balance as-path-neglect** to restore the default.

Syntax

balance as-path-neglect

undo balance as-path-neglect

Default

BGP does not ignore the AS_PATH attribute when it implements load balancing.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP IPv6 unicast address family view

BGP-VPN IPv6 unicast address family view

Predefined user roles

network-admin

Usage guidelines

For BGP to implement load balancing over routes with different AS_PATH attributes, you must use this command together with the **balance** command.

After this command is executed, BGP ignores the AS_PATH attributes in the routes for load balancing and changes the attributes of the advertised routes to those of the optimal route. The operations might cause routing loops. In addition, this command might also affect the NetStream data. Therefore, use this command with caution.

Examples

In BGP IPv4 unicast address family view, enable BGP to ignore the AS_PATH attribute when it implements load balancing.

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default] address-family ipv4 unicast
[Switch-bgp-default-ipv4] balance as-path-neglect
```

Related commands

balance

5.1.7. bestroute compare-med

Use **bestroute compare-med** to enable MED comparison for routes on a per-AS basis.

Use **undo bestroute compare-med** to restore the default.

Syntax

bestroute compare-med

undo bestroute compare-med

Default

MED comparison for routes on a per-AS basis is disabled.

Views

BGP instance view

BGP-VPN instance view

Predefined user roles

network-admin

Usage guidelines

By default, BGP does not compare MEDs for routes from the same AS. When a router learns a new route, it compares the route with the optimal route in its BGP routing table. If the new route is more optimal, it becomes the optimal route in the BGP routing table. In this way, route learning sequence might affect optimal route selection.

To solve the selection problem, the router puts routes received from the same AS into a group when the **bestroute compare-med** command is configured. The router then selects the route with the lowest MED from the same group, and compares routes from different groups.

Examples

In BGP instance view, enable MED comparison for routes on a per-AS basis.

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default] bestroute compare-med
```

5.1.8. bestroute med-confederation

Use **bestroute med-confederation** to enable MED comparison for routes received from confederation peers.

Use **undo bestroute med-confederation** to restore the default.

Syntax

bestroute med-confederation

undo bestroute med-confederation

Default

MED comparison is disabled for routes received from confederation peers.

Views

BGP instance view

BGP-VPN instance view

Predefined user roles

network-admin

Usage guidelines

This command enables BGP to compare the MEDs of routes received from confederation peers. However, if a route from a confederation peer has an AS number that does not belong to the confederation, BGP does not compare the route with other routes. For example, a confederation has three AS numbers 65006, 65007, and 65009. BGP receives three routes from different confederation peers. The AS_PATH attributes of these routes are 65006 65009, 65007 65009, and 65008 65009, and the MED values of them are 2, 3, and 1. Because the third route's AS_PATH attribute contains AS number 65008, which does not belong to the confederation, BGP does not compare it with other routes. As a result, the first route becomes the optimal route.

Examples

In BGP instance view, enable MED comparison for routes received from confederation peers.

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default] bestroute med-confederation
```

5.1.9. bgp

Use **bgp** to enable a BGP instance and enter its view.

Use **undo bgp** to disable a BGP instance.

Syntax

bgp *as-number*

undo bgp [*as-number*]

Default

BGP is disabled and no BGP instances exist.

Views

System view

Predefined user roles

network-admin

Parameters

as-number: Specifies a local AS by its number in the range of 1 to 4294967295.

Usage guidelines

A router supports 4-byte AS number.

A BGP router can run multiple BGP processes. Each BGP process corresponds to a BGP instance. BGP maintains an independent routing table for each BGP instance.

You can create multiple public address families for a BGP instance. However, each public address family (except for public IPv4/IPv6 unicast address family) can belong to only one BGP instance.

You can create multiple VPN instances for a BGP instance, and each VPN instance can have multiple address families. A VPN instance can belong to only one BGP instance.

You cannot specify the same peer for the same address family of different BGP instances.

Different BGP instances can have the same AS number but cannot have the same name.

Examples

Enable BGP instance **default**, set the local AS number to 100, and enter BGP instance view.

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default]
```

5.1.10. compare-different-as-med

Use **compare-different-as-med** to enable MED comparison for routes from peers in different ASs.

Use **undo compare-different-as-med** to restore the default.

Syntax

compare-different-as-med

undo compare-different-as-med

Default

MED comparison is disabled for routes from peers in different ASs.

Views

BGP instance view

BGP-VPN instance view

Predefined user roles

network-admin

Usage guidelines

If multiple routes to a destination exist, the route with the smallest MED is selected.

Do not use this command unless relevant ASs adopt the same IGP protocol and routing selection method.

Examples

In BGP instance view, enable MED comparison for routes from peers in different ASs.

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default] compare-different-as-med
```

5.1.11. confederation id

Use **confederation id** to configure a confederation ID.

Use **undo confederation id** to restore the default.

Syntax

confederation id *as-number*

undo confederation id

Default

No confederation ID is configured.

Views

BGP instance view

Predefined user roles

network-admin

Parameters

as-number: Specifies an AS number that identifies the confederation, in the range of 1 to 4294967295.

Usage guidelines

You can split an AS into several sub-ASs, and each sub-AS remains fully meshed. These sub-ASs form a confederation. Key path attributes of a route, such as the Next_HOP, MED, and LOCAL_PREF, are not discarded when crossing each sub-AS. The sub-ASs still look like one AS from the perspective of other ASs. The AS number is the confederation ID.

Confederation can ensure the integrity of the former AS, and solve the problem of too many IBGP connections in the AS.

Configure the same confederation ID for all routers in one confederation.

For a non-confederation BGP router that establishes a BGP connection to a router in a confederation, the confederation ID is the AS number of the router.

Examples

Confederation 9 consists of four sub-ASs numbered 38, 39, 40 and 41. Peer 10.1.1.1 is a member of sub-AS 38. Peer 200.1.1.1 is a member outside of confederation 9, which belongs to AS 98. Confederation 9 looks like one AS (with AS number 9) from the perspective of peer 200.1.1.1. This example uses a router in sub-AS 41.

```
<Switch> system-view
[Switch] bgp 41
[Switch-bgp-default] confederation id 9
[Switch-bgp-default] confederation peer-as 38 39 40
[Switch-bgp-default] group Confed38 external
[Switch-bgp-default] peer Confed38 as-number 38
```

```
[Switch-bgp-default] peer 10.1.1.1 group Confed38
[Switch-bgp-default] group Remote98 external
[Switch-bgp-default] peer Remote98 as-number 98
[Switch-bgp-default] peer 200.1.1.1 group Remote98
```

Related commands

confederation nonstandard

confederation peer-as

5.1.12. confederation nonstandard

Use **confederation nonstandard** to enable compatibility with routers not compliant with RFC 3065 in the confederation.

Use **undo confederation nonstandard** to restore the default.

Syntax

confederation nonstandard

undo confederation nonstandard

Default

The device is compatible with only routers compliant with RFC 3065 in the confederation.

Views

BGP instance view

Predefined user roles

network-admin

Usage guidelines

Configure this command on all routers compliant with RFC 3065 to interact with those routers not compliant with RFC 3065 in the confederation.

Examples

Confederation 100 consists of two sub-ASs, 64000 and 65000, and contains routers not compliant with RFC 3065. Enable compatibility with routers not compliant with RFC 3065 in the confederation.

```
<Switch> system-view
[Switch] bgp 64000
[Switch-bgp-default] confederation id 100
[Switch-bgp-default] confederation peer-as 65000
[Switch-bgp-default] confederation nonstandard
```

Related commands

confederation id

confederation peer-as

5.1.13. confederation peer-as

Use **confederation peer-as** to specify confederation peer sub-ASs.

Use **undo confederation peer-as** to remove the specified confederation peer sub-ASs.

Syntax

confederation peer-as *as-number-list*

undo confederation peer-as [*as-number-list*]

Default

No confederation peer sub-ASs are specified.

Views

BGP instance view

Predefined user roles

network-admin

Parameters

as-number-list: Specifies a sub-AS number list. A maximum of 32 sub-ASs can be configured in one command line. The expression is *as-number-list* = *as-number* &<1-32>. The *as-number* argument specifies a sub-AS number in the range of 1 to 4294967295, and &<1-32> indicates that a maximum of 32 numbers can be specified.

Usage guidelines

Before this configuration, use the **confederation id** command to specify the confederation ID for the sub-ASs.

If the **undo confederation peer-as** command is executed without the *as-number-list* argument, all confederation peer sub-ASs are removed.

Examples

In BGP instance view, specify confederation peer sub-ASs 2000 and 2001.

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default] confederation id 10
[Switch-bgp-default] confederation peer-as 2000 2001
```

Related commands

confederation id

confederation nonstandard

5.1.14. dampening

Use **dampening** to enable BGP route dampening.

Use **undo dampening** to restore the default.

Syntax

dampening [*half-life-reachable half-life-unreachable reuse suppress ceiling* | **route-policy** *route-policy-name*] *

undo dampening

Default

Route dampening is disabled.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP IPv6 unicast address family view

BGP-VPN IPv6 unicast address family view

Predefined user roles

network-admin

Parameters

half-life-reachable: Specifies a half-life for active routes, in the range of 1 to 45 minutes. By default, the value is 15 minutes.

half-life-unreachable: Specifies a half-life for suppressed routes, in the range of 1 to 45 minutes. By default, the value is 15 minutes.

reuse: Specifies a reuse threshold value for suppressed routes, in the range of 1 to 20000. A suppressed route whose penalty value decreases under the value is reused. By default, the reuse value is 750. The reuse threshold must be less than the suppression threshold.

suppress: Specifies a suppression threshold in the range of 1 to 20000. The route with a penalty value greater than the threshold is suppressed. The default value is 2000.

ceiling: Specifies a ceiling penalty value in the range of 1001 to 20000. The value must be greater than the *suppress* value. By default, the value is 16000.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters.

Usage guidelines

This command dampens only EBGP routes.

If an EBGP peer goes down after you configure this command, routes coming from the peer are dampened but not deleted.

Examples

In BGP IPv4 unicast address family view, configure BGP route dampening. Set the half-life for both active and suppressed routes to 10 minutes, the reuse threshold to 1000, the suppression threshold to 2000, and the ceiling penalty to 10000.

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default] address-family ipv4 unicast
[Switch-bgp-default-ipv4] dampening 10 10 1000 2000 10000
```

5.1.15. default local-preference

Use **default local-preference** to configure a default local preference.

Use **undo default local-preference** to restore the default.

Syntax

default local-preference *value*

undo default local-preference

Default

The default local preference is 100.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP IPv6 unicast address family view

BGP-VPN IPv6 unicast address family view

Predefined user roles

network-admin

Parameters

value: Specifies a default local preference in the range of 0 to 4294967295. A larger value represents a higher preference.

Usage guidelines

You can also use the **apply local-preference** command in a routing policy to configure the local preference for BGP routes. If no routing policy is configured, all BGP routes use the local preference set by the **default local-preference** command. If a routing policy is configured, BGP routes matching the routing policy use the local preference set by the **apply local-preference** command. Other BGP routes use the local preference set by the **default local-preference** command.

Examples

In BGP IPv4 unicast address family view, set the default local preference to 180.

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default] address-family ipv4 unicast
[Switch-bgp-default-ipv4] default local-preference 180
```

Related commands

apply local-preference

route-policy

5.1.16. default med

Use **default med** to specify a default MED value.

Use **undo default med** to restore the default.

Syntax

default med *med-value*

undo default med

Default

The default MED value is 0.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP IPv6 unicast address family view

BGP-VPN IPv6 unicast address family view

Predefined user roles

network-admin

Parameters

med-value: Specifies the default MED value in the range of 0 to 4294967295.

Usage guidelines

BGP selects a MED value in the following order:

1. MED set by the **apply cost** command.
2. MED set by the **med** keyword in the **import-route** command.
3. MED set by the **default med** command.
4. Original MED of a BGP route, or MED changed from the metric of a redistributed IGP route.

Examples

In BGP IPv4 unicast address family view, set the default MED to 25.

```
<Switch> system-view
```

```
[Switch] bgp 100
[Switch-bgp-default] address-family ipv4 unicast
[Switch-bgp-default-ipv4] default med 25
```

Related commands

apply cost

import-route

route-policy

5.1.17. default-route imported

Use **default-route imported** to enable default route redistribution into the BGP routing table.

Use **undo default-route imported** to restore the default.

Syntax

default-route imported

undo default-route imported

Default

Default route redistribution into the BGP routing table is disabled.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP IPv6 unicast address family view

BGP-VPN IPv6 unicast address family view

Predefined user roles

network-admin

Usage guidelines

By default, BGP does not redistribute default IGP routes. To redistribute default IGP routes into the BGP routing table, you must use the **default-route imported** command together with the **import-route** command.

Examples

In BGP IPv4 unicast address family view, enable default route redistribution from OSPF process 1 into the BGP routing table.

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default] address-family ipv4 unicast
[Switch-bgp-default-ipv4] default-route imported
```

```
[Switch-bgp-default-ipv4] import-route ospf 1
```

Related commands

import-route

5.1.18. display bgp group

Use **display bgp group** to display BGP peer group information.

Syntax

display bgp group ipv4 [**unicast**] [**vpn-instance** *vpn-instance-name*] [**group-name** *group-name*]

display bgp group ipv6 [**unicast**] [**vpn-instance** *vpn-instance-name*] [**group-name** *group-name*]

display bgp group l2vpn evpn [**group-name** *group-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ipv4: Displays IPv4 BGP peer group information.

ipv6: Displays IPv6 BGP peer group information.

unicast: Displays BGP unicast peer group information.

evpn: Displays BGP EVPN peer group information.

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays BGP peer group information for the public network.

group-name *group-name*: Specifies a BGP peer group by its name, a case-sensitive string of 1 to 47 characters. If you do not specify a group, this command displays brief information about all BGP peer groups for the specified address family.

Examples

Display brief information about all BGP IPv4 unicast peer groups.

```
 BGP peer group: group1
 Remote AS: 600
 Type: external
 Members:
  1.1.1.10
```

```
 BGP peer group: group2
 Remote AS number: not specified
 Type: external
 Members:
  2.2.2.2
```

Display detailed information about BGP IPv4 unicast peer group **group1**.

```
<Switch> display bgp group ipv4 group-name group1
 BGP peer group: group1
 Remote AS: 600
 Type: external
 Maximum number of prefixes allowed: 4294967295
 Threshold: 75%
 Configured hold time: 180 seconds
 Keepalive time: 60 seconds
 Minimum time between advertisements: 30 seconds
 Peer preferred value: 0
 Site-of-Origin: Not specified

 Routing policy configured:
 No routing policy is configured

 Members:
* - Dynamically created peer
  Peer                    AS  MsgRcvd  MsgSent OutQ PrefRcv Up/Down  State

  1.1.1.10               600        0        0    0       0 00:00:55 Established
```

Display detailed information about BGP IPv6 unicast peer group **group2**.

```
<Switch> display bgp group ipv6 group-name group2
 BGP peer group: group2
 Remote AS: 600
 Type: external
 Maximum number of prefixes allowed: 4294967295
 Threshold: 75%
 Configured hold time: 180 seconds
 Keepalive time: 60 seconds
 Minimum time between advertisements: 30 seconds
 Peer preferred value: 0
 IPsec profile name: profile001
 Site-of-Origin: Not specified

 Routing policy configured:
 No routing policy is configured

 Members:
* - Dynamically created peer
```

```
Peer                    AS  MsgRcvd  MsgSent OutQ PrefRcv Up/Down  State

2::2                   600        0        0    0       0 00:00:45 Established
3::3                   600        0        0    0       0 00:00:40 Established
```

Table 5-2 Command output

Field	Description
BGP peer group	Name of the BGP peer group.
Remote AS	AS number of the peer group.
Type	Type of the peer groups: • **external**—EBGP peer group. • **internal**—IBGP peer group.
Maximum number of prefixes allowed	Maximum number of routes allowed to learn from the peer.
Threshold	Percentage of received routes from the peer to maximum routes allowed to learn from the peer. If the percentage is reached, the system generates a log message.
Configured hold time	Configured hold interval in seconds.
Keepalive time	Keepalive interval in seconds.
Minimum time between advertisements	Minimum route advertisement interval in seconds.
Peer preferred value	Preferred value specified for routes from the peer.
Site-of-Origin	SoO for the peer group.
Routing policy configured	Routing policy configured for the peer group. If you do not specify a routing policy, this field displays **No routing policy is configured**.
Members	Information about peers included in the peer group.
* - Dynamically created peer	An asterisk (*) before a peer address indicates that the peer is a dynamic peer.
Peer	IPv4 or IPv6 address of the peer.
AS	AS number of the peer.
MsgRcvd	Number of messages received.
MsgSent	Number of messages sent.
OutQ	Number of messages to be sent.
PrefRcv	For the IPv4 and IPv6 address families, this field displays the number of prefixes received from the peer.
Up/Down	Lasting time of the current BGP session state.
State	Current state of the BGP session between the local router and the peer.
IPsec profile name	IPsec profile applied to the IPv6 BGP peer group.

5.1.19. display bgp network

Use **display bgp network** to display information about routes advertised by the **network** command and shortcut routes configured by the **network short-cut** command.

Syntax

display bgp network { **ipv4** | **ipv6** } [**unicast**] [**vpn-instance** *vpn-instance-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ipv4: Displays IPv4 address family information.

ipv6: Displays IPv6 address family information.

unicast: Displays BGP unicast address family information.

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays routing information for the public network.

Examples

Display information about routes advertised by the **network** command and shortcut routes configured by the **network short-cut** command in the IPv4 unicast address family.

```
<Switch> display bgp network ipv4

  BGP local router ID: 192.168.1.135
  Local AS number: 100

  Network           Mask            Route-policy        Short-cut
  20.1.1.0          255.255.255.0                       No
  40.1.1.0          255.255.255.0   abc                 No
  30.1.1.0          255.255.255.0                       Yes
```

Display information about routes advertised by the **network** command and shortcut routes configured by the **network short-cut** command in the IPv6 unicast address family.

```
<Switch> display bgp network ipv6

  BGP local router ID: 192.168.1.135
  Local AS number: 100

  Network           PrefixLen       Route-policy        Short-cut
```

```
1::                 24                                      No
2::                 24                                      No
3::                 64                  policy1             No
2::                 24                                      Yes
```

Table 5-3 Command output

Field	Description
Network	Destination network address of the routes advertised by the **network** command and the shortcut routes.
Mask	Mask of the destination network address.
PrefixLen	Prefix length of the destination network address.
Route-policy	Routing policy that is applied to the route.
Short-cut	Whether the route is a shortcut route: • Yes. • No.

5.1.20. display bgp paths

Use **display bgp paths** to display BGP path attribute information.

Syntax

display bgp paths [*as-regular-expression*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

as-regular-expression: Displays information about BGP path attributes whose AS_PATH attribute matches the specified regular expression. The *as-regular-expression* argument is a string of 1 to 256 characters. If you do not specify this argument, the command displays information about all BGP path attributes.

Examples

Display information about all BGP path attributes.

```
<Switch> display bgp paths

  RefCount     MED          Path/Origin
  3            0            ?
  2            0            100i
  3            0            100i
  1            0            ?
```

```
1            0            ?
1            0            ?
```

Table 5-4 Command output

Field	Description
RefCount	Number of BGP routes with these path attributes.
MED	MULTI_EXIT_DISC attribute.

Path/Origin	AS_PATH and ORIGIN attributes of the route:
	• **AS_PATH attribute**—Records the ASs the route has passed, which avoids routing loops.
	• **ORIGIN attribute**—Identifies the origin of the route:
	  ○ **i**—Originated in the AS. The origin of routes advertised with the **network** command is IGP.
	  ○ **e**—Learned through EGP.
	  ○ **?**—Unknown origin. The origin of routes redistributed from IGP protocols is INCOMPLETE.

5.1.21. display bgp peer

Use **display bgp peer** to display BGP peer or peer group information.

Syntax

display bgp peer ipv4 [**unicast**] [**vpn-instance** *vpn-instance-name*] [*ipv4-address mask-length* | { *ipv4-address* | **group-name** *group-name* } **log-info** | [*ipv4-address*] **verbose**]

display bgp peer ipv6 [**unicast**] [**vpn-instance** *vpn-instance-name*] [*ipv6-address prefix-length* | { *ipv6-address* | **group-name** *group-name* } **log-info** | [*ipv6-address*] **verbose**]

display bgp peer ipv6 [**unicast**] [*ipv4-address mask-length* | *ipv4-address* **log-info** | [*ipv4-address*] **verbose**]

display bgp peer l2vpn evpn [*ipv4-address mask-length* | { *ipv4-address* | **group-name** *group-name* } **log-info** | [*ipv4-address*] **verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ipv4: Displays IPv4 BGP peer or peer group information.

ipv6: Displays IPv6 BGP peer or peer group information.

evpn: Displays BGP EVPN peer or peer group information.

unicast: Displays BGP unicast peer or peer group information.

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays BGP peer or peer group information for the public network.

ipv4-address mask-length: Specifies a subnet. The value range for the mask length is 0 to 32. If you specify a subnet, this command displays information about all dynamic peers in the subnet.

ipv4-address: Specifies a peer by its IPv4 address.

ipv6-address prefix-length: Specifies a subnet. The value range for the prefix length is 0 to 128. If you specify a subnet, this command displays information about all dynamic peers in the subnet.

ipv6-address: Specifies a peer by its IPv6 address.

group-name *group-name*: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters.

log-info: Displays log information.

verbose: Displays detailed information. If you do not specify this keyword, the command displays brief BGP peer or peer group information.

Usage guidelines

If you do not specify any parameters, this command displays brief information about all BGP peers for the specified address family.

Examples

Display brief information about all BGP IPv4 unicast peers.

```
<Switch> display bgp peer ipv4

 BGP local router ID: 192.168.100.1
 Local AS number: 100
 Total number of peers: 1                 Peers in established state: 1

  * - Dynamically created peer
  Peer                    AS  MsgRcvd  MsgSent OutQ PrefRcv Up/Down  State

  10.2.1.2               200       13       16    0       0 00:10:34 Established
```

Table 5-5 Command output

Field	Description
* - Dynamically created peer	An asterisk (*) before a peer address indicates that the peer is a dynamic peer.
VPN instance	Name of the VPN instance to which the peer belongs.

Field	Description
Peer	IPv4 or IPv6 address of the peer.
AS	AS number of the peer.
MsgRcvd	Number of messages received.
MsgSent	Number of messages sent.
OutQ	Number of messages to be sent.
PrefRcv	For the IPv4 and IPv6 address families, this field displays the number of prefixes that have been received from the peer and added into the local BGP routing table.
Up/Down	Lasting time of the current BGP session state.
State	Current state of the BGP session between the local router and the peer.

Display brief information about all dynamic peers in network 1.1.1.0/24.

```
<Switch> display bgp peer ipv4 1.1.1.0 24

 Type: EBGP link
 Dynamic address range: 1.1.1.0 24
 Configured: Active Hold Time: 3 sec     Keepalive Time: 1 sec
 Address family IPv4 Unicast: Configured

 Maximum allowed prefix number: 100
 Threshold: 75%
 Minimum time between advertisements is 100 seconds
 Optional capabilities:
  Multi-protocol extended capability has been enabled
  Route refresh capability has been enabled
 Nexthop self has been configured
 Keep-all-routes has been configured
 Send community has been configured
 Send extend community has been configured
 Default route originating has been configured
 Multi-hop ebgp has been enabled
 Peer preferred value: 100
 BFD: Enabled
 Site-of-Origin: 1:1
 Routing policy configured:
 No import as-path-acl list
 Export as-path-acl list is: 22
 No import prefix list
 Export prefix list is: p1
 No import route policy
 Export route policy is: p1
 No import filter-policy
 No export filter-policy
```

```
 Dynamic peers:
  1.1.1.3
```

Display brief information about all dynamic peers in network 1::/64.

```
<Switch> display bgp peer ipv6 1:: 64

 Type: IBGP link
 Dynamic address range: 1:: 64
 Configured: Active Hold Time: 180 sec   Keepalive Time: 60 sec
 Address family IPv6 Unicast: Configured

 Maximum allowed prefix number: 4294967295
 Threshold: 75%
 Minimum time between advertisements is 15 seconds
 Optional capabilities:
  Multi-protocol extended capability has been enabled
  Route refresh capability has been enabled
 Send community has been configured
 Peer preferred value: 0
 Site-of-Origin: Not specified
 Routing policy configured:
 No routing policy is configured

 Dynamic peers:
  1::1
```

Table 5-6 Command output

Field	Description
Type	BGP connection type between the local router and the dynamic peer: • **IBGP link**—IBGP connection. • **EBGP link**—EBGP connection.
Configured	Timers configured on the local router in seconds, including the hold time (Active Hold Time) and keepalive interval (Keepalive Time).
Address family IPv4 Unicast	IPv4 unicast address family capability.
Address family link-state	LS address family capability.
Address family IPv6 Unicast	IPv6 unicast address family capability.
Address family IPv4 Multicast	IPv4 multicast address family capability.
Address family IPv6 Multicast	IPv6 multicast address family capability.
Maximum allowed prefix number	Maximum number of routes allowed to learn from the peer.
Threshold	Percentage of received routes from the peer to maximum routes allowed to learn from the peer. If the percentage is reached, the system generates alarm messages.
Minimum time between advertisements	Minimum route advertisement interval in seconds.

Field	Description
Optional capabilities	Optional capabilities supported by the local end.
Peer Preferred Value	Preferred value specified for the routes from the peer.
BFD	Whether BFD is enabled to detect the link to the BGP peers.
IPsec profile name	IPsec profile applied to the IPv6 BGP peer. This field is available only for the IPv6 unicast and IPv6 multicast address families.
Routing policy configured	Routing policy configured for the peer. If you do not specify a routing policy, this field displays **No routing policy is configured**.
Dynamic peers	IP addresses of dynamic peers.

Display detailed information about BGP IPv4 unicast peer 10.2.1.2.

```
<Switch> display bgp peer ipv4 10.2.1.2 verbose

         Peer: 10.2.1.2          Local: 192.168.100.1
         Type: EBGP link
         BGP version 4, remote router ID 192.168.100.2
         BGP current state: Established, Up for 00h11m10s
         BGP current event: RecvKeepalive
         BGP last state: OpenConfirm
         Port:  Local - 179      Remote - 60672
         Configured: Active Hold Time: 180 sec   Keepalive Time: 60 sec
         Received  : Active Hold Time: 180 sec
         Negotiated: Active Hold Time: 180 sec   Keepalive Time: 60 sec
         Peer optional capabilities:
         Peer support BGP multi-protocol extended
         Peer support BGP route refresh capability
         Peer support BGP route AS4 capability
         Address family IPv4 Unicast: advertised and received

InQ updates: 0, OutQ updates: 0
 NLRI statistics:
         Rcvd:   UnReach NLRI          0,      Reach NLRI          0
         Sent:   UnReach NLRI          0,      Reach NLRI          0

 Message statistics:
 Msg type     Last rcvd time/      Current rcvd count/      History rcvd count/
              Last sent time       Current sent count       History sent count
 Open         10:38:50-2013.7.23   1                        1
              10:38:50-2013.7.23   1                        1
 Update       10:38:51-2013.7.23   1                        1
              10:38:51-2013.7.23   1                        1
 Notification -                    0                        0
              -                    0                        0
```

```
Keepalive    10:38:50-2013.7.23   1                       1
             10:38:50-2013.7.23   1                       1
RouteRefresh -                    0                       0
             -                    0                       0
Total        -                    3                       3
             -                    3                       3

Maximum allowed prefix number: 4294967295
Threshold: 75%
Minimum time between advertisements is 30 seconds
Optional capabilities:
 Multi-protocol extended capability has been enabled
 Route refresh capability has been enabled
Peer Preferred Value: 0
GTSM has been enabled, and the maximum number of hops is 10
BFD: Enabled
Site-of-Origin: Not specified

Routing policy configured:
No routing policy is configured
```

Display detailed information about BGP IPv6 unicast peer 1::2.

```
<Switch> display bgp peer ipv6 1::2 verbose

        Peer: 1::2      Local: 192.168.1.136
        Type: EBGP link
        BGP version 4, remote router ID 192.168.1.135
        BGP current state: Established, Up for 00h05m48s
        BGP current event: RecvKeepalive
        BGP last state: OpenConfirm
        Port:  Local - 13184    Remote - 179
        Configured: Active Hold Time: 180 sec   Keepalive Time: 60 sec
        Received  : Active Hold Time: 180 sec
        Negotiated: Active Hold Time: 180 sec   Keepalive Time: 60 sec
        Peer optional capabilities:
        Peer support BGP multi-protocol extended
        Peer support BGP route refresh capability
        Peer support BGP route AS4 capability
        Address family IPv6 Unicast: advertised and received

InQ updates: 0, OutQ updates: 0
NLRI statistics:
        Rcvd:   UnReach NLRI          0,       Reach NLRI          0
        Sent:   UnReach NLRI          0,       Reach NLRI          3

Message statistics:
Msg type     Last rcvd time/      Current rcvd count/      History rcvd count/
             Last sent time       Current sent count       History sent count
```

```
Open          18:59:15-2013.4.24   1                    1
              18:59:15-2013.4.24   1                    2
Update        -                    0                    0
              18:59:16-2013.4.24   1                    1
Notification  -                    0                    0
              18:59:15-2013.4.24   0                    1
Keepalive     18:59:15-2013.4.24   1                    1
              18:59:15-2013.4.24   1                    1
RouteRefresh  -                    0                    0
              -                    0                    0
Total         -                    2                    2
              -                    3                    5

Maximum allowed prefix number: 4294967295
Threshold: 75%
Minimum time between advertisements is 30 seconds
Optional capabilities:
 Multi-protocol extended capability has been enabled
 Route refresh capability has been enabled
Peer preferred value: 0
GTSM has been enabled, and the maximum number of hops is 10
BFD: Enabled
IPsec profile name: profile001
Site-of-Origin: Not specified

Routing policy configured:
No routing policy is configured
```

Table 5-7 Command output

Field	Description
Peer	IPv4 or IPv6 address of the peer.
Local	Local router ID.
VPN instance	Name of the VPN instance to which the peer belongs.
Type	BGP connection type between the local router and the peer: • **IBGP link**—IBGP connection. • **EBGP link**—EBGP connection.
remote router ID	Router ID of the peer.
BGP current state	Current state of the BGP session between the local router and the peer.
Up for	Lasting time of the BGP session.
BGP current event	Current event of the BGP session between the local router and the peer.
BGP last state	Previous state of the BGP session.
Port	TCP port numbers of the local router and its peer.

Field	Description
Configured	Timers configured on the local router in seconds, including the hold time (Active Hold Time) and keepalive interval (Keepalive Time).
Received	Received timer (configured on the peer) in seconds, including the hold time (Active Hold Time).
Negotiated	Negotiated timers in seconds, including the hold time (Active Hold Time) and keepalive interval (Keepalive Time).
Peer optional capabilities	Optional capabilities supported by the peer.
Peer support BGP route AS4 capability	The peer supports 4-byte AS number.
Address family IPv4 Unicast	IPv4 unicast address family capability: routes of the address family can be advertised and received.
Address family LS	LS address family capability: routes of the address family can be advertised and received.
Address family IPv6 Unicast	IPv6 unicast address family capability: routes of the address family can be advertised and received.
Address family IPv4 Multicast	IPv4 multicast address family capability: routes of the address family can be advertised and received.
Address family IPv6 Multicast	IPv6 multicast address family capability: routes of the address family can be advertised and received.
InQ updates	Number of received updates to be processed.
OutQ updates	Number of updates to be sent to the peer.
NLRI statistics	Number of the reachable and unreachable routes received from and sent to the peer after the BGP session is established.
Message statistics	BGP message statistics.
Msg type	BGP message type.
Last rcvd time/Last sent time	Time when the most recent BGP message was received from or sent to the peer.
Current rcvd count/Current sent count	Number of BGP messages received from or sent to the peer on the current BGP session.
History rcvd count/History sent count	Number of BGP messages received from or sent to the peer since the BGP peer relationship was established.
Total	Total number of received and sent messages.
Maximum allowed prefix number	Maximum number of routes allowed to learn from the peer.
Threshold	Percentage of received routes from the peer to maximum routes allowed to learn from the peer. If the percentage is reached, the system generates alarm messages.
Minimum time between advertisements	Minimum route advertisement interval in seconds.
Optional capabilities	Optional capabilities supported by the local end.
Peer Preferred Value	Preferred value specified for the routes from the peer.

Field	Description
GTSM has been enabled	GTSM is supported.
the maximum number of hops	Maximum number of hops to the specified peer.
BFD	Whether BFD is enabled to detect the link to the BGP peer.
IPsec profile name	IPsec profile applied to the IPv6 BGP peer. This field is available only for the IPv6 unicast and IPv6 multicast address families.
Routing policy configured	Routing policy configured for the peer. If you do not specify a routing policy, this field displays **No routing policy is configured**.

Display log information for BGP IPv4 unicast peer 1.1.1.1.

```
<Switch> display bgp peer ipv4 1.1.1.1 log-info

 Peer : 1.1.1.1

     Date       Time     State Notification
                              Error/SubError

 06-Feb-2013 22:54:42 Down  Send notification with error 6/4
                            Cease/Administrative Reset
                            <administrative reset>
```

Table 5-8 Command output

Field	Description
Peer	IPv4 or IPv6 address of the peer.
Date	Date on which the Notification was sent or received.
Time	Time at which the Notification was sent or received.
State	BGP session state: • **Up**—The BGP session is in Established state. • **Down**—The BGP session is down.
Notification Error/SubError	Error code of the Notification, indicating the cause of why the BGP session was down. • **Error**—Refers to the error code, which identifies the type of the Notification. • **SubError**—Refers to the error subcode of the Notification, which identifies the specific information about the reported error.

5.1.22. display bgp routing-table dampened

Use **display bgp routing-table dampened** to display dampened BGP routes.

Syntax

display bgp routing-table dampened { **ipv4** | **ipv6** } [**unicast**] [**vpn-instance** *vpn-instance-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ipv4: Displays dampened BGP IPv4 routes.

ipv6: Displays dampened BGP IPv6 routes.

unicast: Displays dampened BGP unicast routes.

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays dampened BGP routes for the public network.

Examples

Display dampened BGP IPv4 unicast routes.

```
<Switch> display bgp routing-table dampened ipv4

 Total number of routes: 1

 BGP local router ID is 192.168.1.135
 Status codes: * - valid, > - best, d - dampened, h - history,
               s - suppressed, S - stale, i - internal, e - external
               a - additional-path
               Origin: i - IGP, e - EGP, ? - incomplete

     Network            From            Reuse                         Path/Ogn

  de 20.1.1.0/24        10.1.1.2        00:56:27                      100i
```

Display dampened BGP IPv6 unicast routes.

```
<Switch> display bgp routing-table dampened ipv6

 Total number of routes: 2

 BGP local router ID is 192.168.1.135
 Status codes: * - valid, > - best, d - dampened, h - history,
               s - suppressed, S - stale, i - internal, e - external
               a - additional-path
               Origin: i - IGP, e - EGP, ? - incomplete
```

```
de Network : 2::                                    PrefixLen : 64
   From    : 10.1.1.1                               Reuse     : 00:39:49
   Path/Ogn: 100i

de Network : 2::                                    PrefixLen : 64
   From    : 1::1                                   Reuse     : 00:39:49
   Path/Ogn: 100i
```

Table 5-9 Command output

Field	Description
Status codes	Status codes: • *** – valid**—Valid route. • **> – best**—Optimal route. • **d – dampened**—Dampened route. • **h – history**—History route. • **s – suppressed**—Suppressed route. • **S – stale**—Stale route. • **i – internal**—Internal route. • **e – external**—External route. • **a – additional-path**—Add-Path optimal route.
Origin	Origin of the route: • **i – IGP**—Originated in the AS. The origin of routes advertised with the **network** command is IGP. • **e – EGP**—Learned through EGP. • **?– incomplete**—Unknown origin. The origin of routes redistributed from IGP protocols is INCOMPLETE.
Network	Destination network address.
From	IP address from which the route was received.
Reuse	Reuse time of the route.
Path/Ogn	AS_PATH and ORIGIN attributes of the route: • **AS_PATH attribute**—Records the ASs the route has passed, which avoids routing loops. • **ORIGIN attribute**—Identifies the origin of the route.

Related commands

dampening

reset bgp dampening

5.1.23. display bgp routing-table flap-info

Use **display bgp routing-table flap-info** to display BGP route flap statistics.

Syntax

display bgp routing-table flap-info ipv4 [**unicast**] [**vpn-instance** *vpn-instance-name*] [*ipv4-address* [{ *mask-length* | *mask* } [**longest-match**]] | **as-path-acl** *as-path-acl-number*]

display bgp routing-table flap-info ipv6 [**unicast**] [**vpn-instance** *vpn-instance-name*] [*ipv6-address prefix-length* | **as-path-acl** *as-path-acl-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ipv4: Displays BGP IPv4 route flap statistics.

ipv6: Displays BGP IPv6 route flap statistics.

unicast: Displays BGP unicast route flap statistics.

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays BGP route flap statistics for the public network.

ipv4-address: Specifies a destination network address.

mask-length: Specifies a mask length in the range of 0 to 32.

mask: Specifies a network mask in dotted decimal notation.

longest-match: Specifies longest match mode, which selects the longest matching route through the following steps:

1. ANDs the specified network address with the mask of each route.
2. Matches a route if the AND result is the same as the network address of the route and the mask of the route is shorter than or equal to the specified mask.
3. Selects the route with the longest mask among the matching routes.

ipv6-address prefix-length: Displays route flap statistics for BGP IPv6 routes that match the specified network address, and match the prefix length in the range of 0 to 128.

as-path-acl *as-path-acl-number*: Displays route flap statistics for BGP routes that match the AS path list specified by its number in the range of 1 to 256.

Usage guidelines

If you specify only the *ipv4-address* argument, the system ANDs the network address with the mask of a route. If the result matches the network address of the route, the command displays flap statistics of the route.

If you specify the *ipv4-address mask* or *ipv4-address mask-length* argument, and do not specify the **longest-match** keyword, the command displays flap statistics of the BGP IPv4 unicast or multicast route that matches both the specified destination network address and the mask (or mask length).

Examples

Display BGP IPv4 unicast route flap statistics.

```
<Switch> display bgp routing-table flap-info ipv4

 Total number of routes: 1

 BGP local router ID is 192.168.1.135
 Status codes: * - valid, > - best, d - dampened, h - history,
               s - suppressed, S - stale, i - internal, e - external
               a - additional-path
               Origin: i - IGP, e - EGP, ? - incomplete

     Network            From            Flaps   Duration  Reuse        Path/Ogn

  de 20.1.1.0/24        10.1.1.2        1       00:02:36  00:53:58     100i
```

Display BGP IPv6 unicast route flap statistics.

```
<Switch> display bgp routing-table flap-info ipv6

 Total number of routes: 2

 BGP local router ID is 192.168.1.135
 Status codes: * - valid, > - best, d - dampened, h - history,
               s - suppressed, S - stale, i - internal, e - external
               a - additional-path
               Origin: i - IGP, e - EGP, ? - incomplete

  de Network : 2::                                  PrefixLen : 64
     From    : 10.1.1.1                             Flaps     : 5
     Duration: 00:03:25                             Reuse     : 00:39:28
     Path/Ogn: 100i

  de Network : 2::                                  PrefixLen : 64
     From    : 1::1                                 Flaps     : 5
     Duration: 00:03:25                             Reuse     : 00:39:28
     Path/Ogn: 100i
```

Table 5-10 Command output

Field	Description
Status codes	Status codes: • *** – valid**—Valid route. • **> – best**—Optimal route. • **d – dampened**—Dampened route. • **h – history**—History route. • **s – suppressed**—Suppressed route. • **S – stale**—Stale route. • **i – internal**—Internal route. • **e – external**—External route. • a – additional-path.
Origin	Origin of the route: • **i – IGP**—Originated in the AS. The origin of routes advertised with the **network** command is IGP. • **e – EGP**—Learned through EGP. • **?– incomplete**—Unknown origin. The origin of routes redistributed from IGP protocols is INCOMPLETE.
Network	Destination network address.
From	Source IP address of the route.
Flaps	Number of routing flaps.
Duration	Duration time of the flap route.
Reuse	Reuse time of the route.
Path/Ogn	AS_PATH and ORIGIN attributes of the route: • **AS_PATH attribute**—Records the ASs the route has passed, which avoids routing loops. • **ORIGIN attribute**—Identifies the origin of the route.

Related commands

dampening

reset bgp flap-info

5.1.24. display bgp routing-table ipv4 unicast

Use **display bgp routing-table ipv4 unicast** to display BGP IPv4 unicast routing information.

Syntax

display bgp routing-table ipv4 [**unicast**] [**vpn-instance** *vpn-instance-name*] [*ipv4-address* [{ *mask-length* | *mask* } [**longest-match**]] | **as-path-acl** *as-path-acl-number* | **community-list** { { *basic-community-list-number* | *comm-list-name* } [**whole-match**] | *adv-community-list-number* | ext-community } | **peer** *ipv4-address*

{ **advertised-routes** | **received-routes** } [*ipv4-address* [*mask-length* | *mask*] | **statistics**] | **statistics**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

instance *instance-name*: Specifies a BGP instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the command displays BGP IPv4 unicast routing information for the default BGP instance.

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays the BGP IPv4 unicast routing information for the public network.

ipv4-address: Specifies a destination network address.

mask-length: Specifies a mask length in the range of 0 to 32.

mask: Specifies a network mask in dotted decimal notation.

longest-match: Specifies longest match mode, which selects the longest matching route through the following steps:

1. ANDs the specified network address with the mask of each route.
2. Matches a route if the AND result is the same as the network address of the route and the mask of the route is shorter than or equal to the specified mask.
3. Selects the route with the longest mask among the matching routes.

as-path-acl *as-path-acl-number*: Displays BGP IPv4 unicast routes that match the AS path list specified by its number in the range of 1 to 256.

community-list: Displays BGP IPv4 unicast routes that match a community list.

ext-community: Displays extended community attribute information for BGP IPv4 unicast routes or displays BGP IPv4 unicast routes that match the extended community attribute criterion specified for route filtering.

basic-community-list-number: Specifies a basic community list by its number in the range of 1 to 99.

comm-list-name: Specifies a community list by its name, a case-sensitive string of 1 to 63 characters.

whole-match: Displays routes exactly matching the specified community list. If you do not specify this keyword, the command displays routes whose COMMUNITY attributes include the specified community list.

adv-community-list-number: Specifies an advanced community list by its number in the range of 100 to 199.

peer *ipv4-address*: Displays BGP IPv4 unicast routing information advertised to or received from the specified peer.

advertised-routes: Displays routing information advertised to the specified peer.

received-routes: Displays routing information received from the specified peer.

statistics: Displays routing statistics.

Usage guidelines

If you do not specify any parameters, this command displays brief information about all BGP IPv4 unicast routes.

If you specify only the *ipv4-address* argument, the system ANDs the network address with the mask of a route. If the result matches the network address of the route, the command displays information about the route.

If you specify the *ipv4-address mask* or *ipv4-address mask-length* argument and do not specify the **longest-match** keyword, this command displays information about the BGP IPv4 unicast route that matches both the specified destination network address and the mask (or mask length).

This command displays BGP IPv4 unicast routing information regardless of whether the **unicast** keyword is specified.

Examples

Display brief information about all BGP IPv4 unicast routes.

```
<Switch> display bgp routing-table ipv4

 Total number of routes: 4

 BGP local router ID is 192.168.100.1
 Status codes: * - valid, > - best, d - dampened, h - history,
               s - suppressed, S - stale, i - internal, e - external
               a - additional-path
               Origin: i - IGP, e - EGP, ? - incomplete

     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn

* >  10.2.1.0/24        10.2.1.1        0                     0       i
   e                    10.2.1.2        0                     0       200i
* >  192.168.1.0        192.168.1.135   0                     0       i
*  e                    10.2.1.2        0                     0       200i
```

Display information about BGP IPv4 unicast routes that match AS path list 1.

```
<Switch> display bgp routing-table ipv4 as-path-acl 1
```

```
 Total number of routes: 1

 BGP local router ID is 2.2.2.2
 Status codes: * - valid, > - best, d - dampened, h - history,
               s - suppressed, S - stale, i - internal, e - external
               a - additional-path
               Origin: i - IGP, e - EGP, ? - incomplete

     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn

* >e 30.1.1.0/24        20.1.1.1                              0       200i
```

Display information about all public BGP IPv4 unicast routes advertised to peer 10.2.1.2.

```
<Switch> display bgp routing-table ipv4 peer 10.2.1.2 advertised-routes

 Total number of routes: 2

 BGP local router ID is 192.168.100.1
 Status codes: * - valid, > - best, d - damped, h - history,
               s - suppressed, S - Stale, i - internal, e - external
               a - additional-path
               Origin: i - IGP, e - EGP, ? - incomplete

     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn

* >  10.2.1.0/24        10.2.1.1        0                     0       i
* >  192.168.1.0        192.168.1.135   0                     0       i
```

Display information about all public BGP IPv4 unicast routes received from peer 10.2.1.2.

```
<Switch> display bgp routing-table ipv4 peer 10.2.1.2 received-routes

 Total number of routes: 2

 BGP local router ID is 192.168.100.1
 Status codes: * - valid, > - best, d - damped, h - history,
               s - suppressed, S - Stale, i - internal, e - external
               a - additional-path
               Origin: i - IGP, e - EGP, ? - incomplete

     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn

   e 10.2.1.0/24        10.2.1.2        0                     0       200i
*  e 192.168.1.0        10.2.1.2        0                     0       200i
```

Display information about the public-network BGP IPv4 unicast routes that have extended community attributes in BGP instance **default**.

```
<Sysname> dis bgp routing-table ipv4 ext-community

  Total number of routes: 1
```

```
BGP local router ID is 192.168.184.56
Status codes: * - valid, > - best, d - dampened, h - history,
              s - suppressed, S - stale, i - internal, e - external
              a - additional-path
      Origin: i - IGP, e - EGP, ? - incomplete

   Network          NextHop        MED        LocPrf     PrefVal Ext-Community

* >i 9.1.1.0/24      120.1.1.1        0          100        0       <RT: 1:1>
```

Table 5-11 Command output

Field	Description
Status codes	Status codes: • *** – valid**—Valid route. • **> – best**—Optimal route. • **d – dampened**—Dampened route. • **h – history**—History route. • **s – suppressed**—Suppressed route. • **S – stale**—Stale route. • **i – internal**—Internal route. • **e – external**—External route. • **a – additional-path**—Add-Path optimal route.
Origin	Origin of the route: • **i – IGP**—Originated in the AS. The origin of routes advertised with the **network** command is IGP. • **e – EGP**—Learned through EGP. • **?– incomplete**—Unknown origin. The origin of routes redistributed from IGP protocols is INCOMPLETE.
Network	Destination network address.
NextHop	Next hop IP address.
MED	MULTI_EXIT_DISC attribute.
LocPrf	Local preference value.
PrefVal	Preferred value of the route.
Path/Ogn	AS_PATH and ORIGIN attributes of the route: • **AS_PATH**—Records the ASs the route has passed, which avoids routing loops. • **ORIGIN**—Identifies the origin of the route.
Ext-Community	Extended community attribute value.

Display detailed information about BGP IPv4 unicast routes destined to network 10.2.1.0/24.

```
<Switch> display bgp routing-table ipv4 10.2.1.0 24

 BGP local router ID: 192.168.100.1
 Local AS number: 100
```

```
 Paths:   2 available, 1 best

 BGP routing table information of 10.2.1.0/24:
 Imported route.
 Original nexthop: 10.2.1.1
 OutLabel        : NULL
 RxPathID        : 0x0
 TxPathID        : 0x0
 AS-path         : (null)
 Origin          : igp
 Attribute value : MED 0, pref-val 0, pre 0
 State           : valid, local, best
 IP precedence   : N/A
 QoS local ID    : N/A
 Traffic index   : N/A

 From            : 10.2.1.2 (192.168.100.2)
 Rely nexthop   : not resolved
 Original nexthop: 10.2.1.2
 OutLabel        : NULL
 RxPathID        : 0x0
 TxPathID        : 0x0
 AS-path         : 200
 Origin          : igp
 Attribute value : MED 0, pref-val 0, pre 255
 State           : external
 IP precedence   : N/A
 QoS local ID    : N/A
 Traffic index   : N/A
```

Display detailed information about the BGP IPv4 unicast route destined to address 1.1.1.1/32.

```
<Switch> display bgp routing-table ipv4 1.1.1.1 32

 BGP local router ID: 192.168.100.1
 Local AS number: 100

 Paths:   2 available, 1 best

 BGP routing table information of 1.1.1.1/32:
 From            : 10.2.1.1 (192.168.100.3)
 Rely nexthop    : 10.2.1.1
 Original nexthop: 10.2.1.1
 OutLabel        : NULL
 RxPathID        : 0x0
 TxPathID        : 0x0
 AS-path         : (null)
 Origin          : igp
```

```
Attribute value : MED 0, pref-val 0, pre 0
State           : valid, local, best
IP precedence   : N/A
QoS local ID    : N/A
Traffic index   : N/A


Backup route.
From            : 10.2.1.2 (192.168.100.2)
Rely nexthop    : 10.2.1.2
Original nexthop: 10.2.1.2
OutLabel        : NULL
RxPathID        : 0x0
TxPathID        : 0x0
AS-path         : 200
Origin          : igp
Attribute value : MED 0, pref-val 0, pre 255
State           : external
IP precedence   : N/A
QoS local ID    : N/A
Traffic index   : N/A
```

Table 5-12 Command output

Field	Description
Paths	Number of routes: • **available**—Number of valid routes. • **best**—Number of optimal routes.
Original nexthop	Original next hop of the route. If the route was obtained from a BGP update message, the original next hop is the next hop IP address in the message.
OutLabel	This field is not supported in the current software version. Outgoing label of the route.
RxPathID	Add-Path ID of received routes.
TxPathID	Add-Path ID of advertised routes.
AS-path	AS_PATH attribute of the route, which records the ASs the route has passed and avoids routing loops.
Origin	Origin of the route: • **igp**—Originated in the AS. The origin of routes advertised with the **network** command is IGP. • **egp**—Learned through EGP. • **incomplete**—Unknown origin. The origin of routes redistributed from IGP protocols is INCOMPLETE.
Attribute value	BGP path attributes: • **MED**—MED value. • **localpref**–Local preference value. • **pref-val**—Preferred value. • **pre**—Route preference.

Field	Description
State	Current state of the route: • valid. • internal. • external. • local. • synchronize. • best.
From	IP address of the BGP peer that advertised the route.
Rely Nexthop	Next hop found by route recursion. If no next hop is found, this field displays **not resolved**.
IP precedence	IP precedence in the range of 0 to 7. **N/A** indicates that the route does not support this field.
QoS local ID	QoS local ID in the range of 1 to 4095. **N/A** indicates that the route does not support this field.
Traffic index	Traffic index in the range of 1 to 64. **N/A** indicates that the route does not support this field.

Display statistics for public BGP IPv4 unicast routes advertised to peer 10.2.1.2.

```
<Switch> display bgp routing-table ipv4 peer 10.2.1.2 advertised-routes statistics

 Advertised routes total: 2
```

Display statistics for public BGP IPv4 unicast routes received from peer 10.2.1.2.

```
<Switch> display bgp routing-table ipv4 peer 10.2.1.2 received-routes statistics

 Received routes total: 2
```

Table 5-13 Command output

Field	Description
Advertised routes total	Total number of advertised routes.
Received routes total	Total number of received routes.

Display BGP IPv4 unicast route statistics.

```
<Switch> display bgp routing-table ipv4 statistics

 Total number of routes: 4
```

Table 5-14 Command output

Field	Description
Total number of routes	Total number of routes.

Related commands

ip as-path

ip community-list

5.1.25. display bgp routing-table ipv6 unicast

Use **display bgp routing-table ipv6 unicast** to display BGP IPv6 unicast routing information.

Syntax

display bgp routing-table ipv6 [**unicast**] [**vpn-instance** *vpn-instance-name*] [*ipv6-address prefix-length* | **as-path-acl** *as-path-acl-number* | **community-list** { { *basic-community-list-number* | *comm-list-name* } [**whole-match**] | *adv-community-list-number* } | **peer** *ipv6-address* { **advertised-routes** | **received-routes** } [*ipv6-address prefix-length* | **statistics**] | **statistics**]

display bgp routing-table ipv6 [**unicast**] **peer** *ipv4-address* { **advertised-routes** | **received-routes** } [*ipv6-address prefix-length* | **statistics**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays the BGP IPv6 unicast routing information for the public network.

ipv6-address prefix-length: Specifies the destination network address and prefix length. The value range for the *prefix-length* argument is 0 to 128. If you do not specify this argument, the command displays brief information about all BGP IPv6 unicast routing information.

as-path-acl *as-path-acl-number*: Displays BGP IPv6 unicast routes that match the AS path list specified by its number in the range of 1 to 256.

community-list: Displays BGP IPv6 unicast routes that match a community list.

basic-community-list-number: Specifies a basic community list by its number in the range of 1 to 99.

comm-list-name: Specifies a community list by its name, a case-sensitive string of 1 to 63 characters.

whole-match: Displays routes exactly matching the specified community list. If you do not specify this keyword, the command displays routes whose COMMUNITY attributes include the specified community list.

adv-community-list-number: Specifies an advanced community list by its number in the range of 100 to 199.

peer: Displays BGP IPv6 unicast routing information advertised to or received from the specified peer.

ipv4-address: Specifies the peer IPv4 address.

ipv6-address: Specifies the peer IPv6 address.

advertised-routes: Displays routing information advertised to the specified peer.

received-routes: Displays routing information received from the specified peer.

statistics: Displays routing statistics.

Usage guidelines

This command displays BGP IPv6 unicast routing information regardless of whether the **unicast** keyword is specified.

Examples

Display brief information about all BGP IPv6 unicast routes.

```
<Switch> display bgp routing-table ipv6

 Total number of routes: 1

 BGP local router ID is 192.168.1.136
 Status codes: * - valid, > - best, d - dampened, h - history,
               s - suppressed, S - stale, i - internal, e - external
               a - additional-path
               Origin: i - IGP, e - EGP, ? - incomplete

* >e Network : 3::                                    PrefixLen : 64
     NextHop : 1::2                                   LocPrf    :
     PrefVal : 0                                      OutLabel  : NULL
     MED     :
     Path/Ogn: 100i
```

Display information about BGP IPv6 unicast routes that match AS path list 1.

```
<Switch> display bgp routing-table ipv6 as-path-acl 1

 Total number of routes: 2

 BGP local router ID is 192.168.1.136
 Status codes: * - valid, > - best, d - dampened, h - history,
               s - suppressed, S - stale, i - internal, e - external
               a - additional-path
               Origin: i - IGP, e - EGP, ? - incomplete

* >e Network : 2::                                    PrefixLen : 64
```

```
     NextHop : 1::2                                  LocPrf    :
     PrefVal : 0                                     OutLabel  : NULL
     MED     :
     Path/Ogn: 100i

* >e Network : 3::                                  PrefixLen : 64
     NextHop : 1::2                                  LocPrf    :
     PrefVal : 0                                     OutLabel  : NULL
     MED     :
     Path/Ogn: 100i
```

Display information about BGP IPv6 unicast routes that match BGP community list 100.

```
<Switch> display bgp routing-table ipv6 community-list 100

 Total number of routes: 2

 BGP local router ID is 192.168.1.136
 Status codes: * - valid, > - best, d - dampened, h - history,
               s - suppressed, S - stale, i - internal, e - external
               a - additional-path
               Origin: i - IGP, e - EGP, ? - incomplete

* >e Network : 2::                                  PrefixLen : 64
     NextHop : 1::2                                  LocPrf    :
     PrefVal : 0                                     OutLabel  : NULL
     MED     :
     Path/Ogn: 100i

* >e Network : 3::                                  PrefixLen : 64
     NextHop : 1::2                                  LocPrf    :
     PrefVal : 0                                     OutLabel  : NULL
     MED     :
     Path/Ogn: 100i
```

Display information about all BGP IPv6 unicast routes advertised to peer 1::1.

```
<Switch> display bgp routing-table ipv6 peer 1::1 advertised-routes

 Total number of routes: 1

 BGP local router ID is 192.168.1.136
 Status codes: * - valid, > - best, d - dampened, h - history,
               s - suppressed, S - stale, i - internal, e - external
               a - additional-path
               Origin: i - IGP, e - EGP, ? - incomplete

* >  Network : 2::                                  PrefixLen : 64
     NextHop : ::                                    LocPrf    :
     MED     : 0                                     OutLabel  : NULL
```

```
     Path/Ogn: i
```

Display information about all BGP IPv6 unicast routes received from peer 1::1.

```
<Switch> display bgp routing-table ipv6 peer 1::1 received-routes

 Total number of routes: 1

 BGP local router ID is 192.168.1.135
 Status codes: * - valid, > - best, d - dampened, h - history,
               s - suppressed, S - stale, i - internal, e - external
               a - additional-path
               Origin: i - IGP, e - EGP, ? - incomplete

* >e Network : 2::                                    PrefixLen : 64
     NextHop : ::FFFF:10.1.1.1                       LocPrf    :
     PrefVal : 0                                     OutLabel  : NULL
     MED     : 0
     Path/Ogn: 100i
```

Table 5-15 Command output

Field	Description
Status codes	Status codes: • *** – valid**—Valid route. • **> – best**—Optimal route. • **d – dampened**—Dampened route. • **h – history**—History route. • **s – suppressed**—Suppressed route. • **S – stale**—Stale route. • **i – internal**—Internal route. • **e – external**—External route. • **a – additional-path**—Add-Path optimal route.
Origin	Origin of the route: • **i – IGP**—Originated in the AS. The origin of routes advertised with the **network** command is IGP. • **e – EGP**—Learned through EGP. • **?– incomplete**—Unknown origin. The origin of routes redistributed from IGP protocols is INCOMPLETE.
Network	Destination network address.
PrefixLen	Prefix length of the destination network address.
NextHop	Next hop IPv6 address.
LocPrf	Local preference value.
PrefVal	Preferred value of the route.
OutLabel	This field is not supported in the current software version. Outgoing label of the route.
MED	MULTI_EXIT_DISC attribute.
Path/Ogn	AS_PATH and ORIGIN attributes of the route:

Field	Description
	• **AS_PATH attribute**—Records the ASs the route has passed, which avoids routing loops. • **ORIGIN attribute**—Identifies the origin of the route.

Display detailed information about BGP IPv6 unicast routes destined to network 2::/64.

```
<Switch> display bgp routing-table ipv6 2:: 64

 BGP local router ID: 192.168.1.135
 Local AS number: 200

 Paths:   2 available, 1 best

 BGP routing table information of 2::/64:
 From            : 10.1.1.1 (192.168.1.136)
 Relay nexthop   : ::FFFF:10.1.1.1
 Original nexthop: ::FFFF:10.1.1.1
 OutLabel        : NULL
 RxPathID        : 0x0
 TxPathID        : 0x0
 AS-path         : 100
 Origin          : igp
 Attribute value : MED 0, pref-val 0
 State           : valid, external, best
 IP precedence   : N/A
 QoS local ID    : N/A
 Traffic index   : N/A

 From            : 1::1 (192.168.1.136)
 Relay nexthop   : 1::1
 Original nexthop: 1::1
 OutLabel        : NULL
 RxPathID        : 0x0
 TxPathID        : 0x0
 AS-path         : 100
 Origin          : igp
 Attribute value : MED 0, pref-val 0
 State           : valid, external
 IP precedence   : N/A
 QoS local ID    : N/A
 Traffic index   : N/A
```

Table 5-16 Command output

Field	Description
Paths	Number of routes: • **available**—Number of valid routes. • **best**—Number of optimal routes.

Field	Description
Original nexthop	Original next hop of the route. If the route was obtained from a BGP update message, the original next hop is the next hop IP address in the message.
OutLabel	This field is not supported in the current software version. Outgoing label of the route.
RxPathID	Add-Path ID of received routes.
TxPathID	Add-Path ID of advertised routes.
AS-path	AS_PATH attribute of the route, which records the ASs the route has passed and avoids routing loops.
Origin	Origin of the route: • **igp**—Originated in the AS. The origin of routes advertised with the **network** command is IGP. • **egp**—Learned through EGP. • **incomplete**—Unknown origin. The origin of routes redistributed from IGP protocols is INCOMPLETE.
Attribute value	BGP path attributes: • **MED**—MED value. • **localpref**–Local preference value. • **pref-val**—Preferred value. • **pre**—Route preference.
State	Current state of the route: • valid. • internal. • external. • local. • best.
From	IP address of the BGP peer that advertised the route.
Relay Nexthop	Next hop found by route recursion. If no next hop is found, this field displays **not resolved**.
IP precedence	IP precedence in the range of 0 to 7. **N/A** indicates that the route does not support this field.
QoS local ID	QoS local ID in the range of 1 to 4095. **N/A** indicates that the route does not support this field.
Traffic index	Traffic index in the range of 1 to 64. **N/A** indicates that the route does not support this field.

Display statistics for BGP IPv6 unicast routes advertised to peer 1::1.

```
<Switch> display bgp routing-table ipv6 peer 1::1 advertised-routes statistics

 Advertised routes total: 1
```

Display statistics for BGP IPv6 unicast routes received from peer 1::1.

```
<Switch> display bgp routing-table ipv6 peer 1::1 received-routes statistics

 Received routes total: 1
```

Table 5-17 Command output

Field	Description
Advertised routes total	Total number of advertised routes.
Received routes total	Total number of received routes.

Display BGP IPv6 unicast route statistics.

```
<Switch> display bgp routing-table ipv6 statistics

 Total number of routes: 4
```

Table 5-18 Command output

Field	Description
Total number of routes	Total number of routes.

Related commands

ip as-path

ip community-list

5.1.26. ebgp-interface-sensitive

Use **ebgp-interface-sensitive** to enable immediate re-establishment of direct EBGP sessions.

Use **undo ebgp-interface-sensitive** to disable immediate re-establishment of direct EBGP sessions.

Syntax

ebgp-interface-sensitive

undo ebgp-interface-sensitive

Default

Immediate re-establishment of direct EBGP sessions is enabled.

Views

BGP instance view

Predefined user roles

network-admin

Usage guidelines

When a direct link to an EBGP peer fails, BGP tears down the session and re-establishes a session to the peer immediately. If the feature is not enabled, the router does not tear down the session until the hold time expires. However, disabling this feature can prevent routing flaps from affecting EBGP session state.

This command applies only to direct EBGP sessions.

Examples

Enable immediate re-establishment of direct EBGP sessions.

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default] ebgp-interface-sensitive
```

5.1.27. extcommunity-type tag

Use **extcommunity-type tag** to set the type value for the tag community attribute.

Use **undo extcommunity-type tag** to restore the default.

Syntax

extcommunity-type tag *tag-type-value*

undo extcommunity-type tag

Default

The type value for the tag community attribute is 83cf in hexadecimal notation.

Views

BGP instance view

Predefined user roles

network-admin

Parameters

tag-type-value: Specifies a type value in the range of 0 to ffff, which is in hexadecimal notation.

Usage guidelines

The tag community attribute is an NEC-proprietary extended community attribute. It might be unrecognizable for devices from other vendors or have conflicts with other private extended community attributes. You can use this command to adjust the type value to a recognizable or non-conflicting one for the tag community attribute.

Examples

Set the type value to 0x5688 for the tag community attribute.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] extcommunity-type tag 5688。
```

Related commands

peer advertise tag

5.1.28. filter-policy export

Use **filter-policy export** to filter advertised BGP routes.

Use **undo filter-policy export** to remove the route filter.

Syntax

In BGP IPv4 unicast address family view/BGP-VPN IPv4 unicast address family view:

filter-policy { *ipv4-acl-number* | **prefix-list** *prefix-list-name* } **export** [*protocol process-id*]

undo filter-policy export [*protocol process-id*]

In BGP IPv6 unicast address family view/BGP-VPN IPv6 unicast address family view:

filter-policy { *ipv6-acl-number* | **prefix-list** *ipv6-prefix-name* } **export** [*protocol process-id*]

undo filter-policy export [*protocol process-id*]

Default

Advertised BGP routes are not filtered.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP IPv6 unicast address family view

BGP-VPN IPv6 unicast address family view

Predefined user roles

network-admin

Parameters

ipv4-acl-number: Specifies an IPv4 ACL by its number in the range of 2000 to 3999, to match routes by destination.

ipv6-acl-number: Specifies an IPv6 ACL by its number in the range of 2000 to 3999, to match routes by destination.

prefix-list *prefix-list-name*: Specifies an IPv4 prefix list by its name, a case-sensitive string of 1 to 63 characters, to match routes by destination.

prefix-list *ipv6-prefix-name*: Specifies an IPv6 prefix list by its name, a case-sensitive string of 1 to 63 characters, to match routes by destination.

protocol: Filters routes redistributed from the routing protocol.

process-id: Specifies a routing protocol by its ID in the range of 1 to 65535. For IPv4 routes, this argument is available only when the protocol is **ospf**, or **rip**. For IPv6 routes, this argument is available only when the protocol is **ospfv3**, or **ripng**.

Usage guidelines

If you specify a protocol (such as **direct**), this command filters only routes redistributed from the specified protocol. If you do not specify a protocol, this command filters all advertised routes, including the following routes:

- Redistributed from IGP.
- Injected by the **network** command.
- Learned from BGP peers.

If you use a basic ACL (with a number from 2000 to 2999) configured with the **rule** [*rule-id*] { **deny** | **permit** } **source** *source-address source-wildcard* command, the command matches routes whose destination network addresses match the *source-address source-wildcard* argument. However, it does not match the masks of the destination addresses.

To use an advanced ACL (with a number from 3000 to 3999) in the command, configure the ACL using one of the following steps:

- To deny/permit a route with the specified destination, use the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* command.
- To deny/permit a route with the specified destination and mask, use the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* **destination** *dest-addr dest-wildcard* command.

The **source** keyword specifies the destination address of a route and the **destination** keyword specifies the subnet mask of the destination address. For the mask configuration to take effect, specify a contiguous subnet mask.

Examples

In BGP IPv4 unicast address family view, use IPv4 basic ACL 2000 to filter advertised BGP IPv4 routes.

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default] address-family ipv4 unicast
[Switch-bgp-default-ipv4] filter-policy 2000 export
```

Related commands

filter-policy import

peer as-path-acl

peer filter-policy

peer prefix-list

peer route-policy

5.1.29. filter-policy import

Use **filter-policy import** to filter received BGP routes.

Use **undo filter-policy import** to restore the default.

Syntax

In BGP IPv4 unicast address family view/BGP-VPN IPv4 unicast address family view:

filter-policy { *ipv4-acl-number* | **prefix-list** *prefix-list-name* } **import**

undo filter-policy import

In BGP IPv6 unicast address family view/BGP-VPN IPv6 unicast address family view:

filter-policy { *ipv6-acl-number* | **prefix-list** *ipv6-prefix-name* } **import**

undo filter-policy import

Default

Received BGP routes are not filtered.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP IPv6 unicast address family view

BGP-VPN IPv6 unicast address family view

Predefined user roles

network-admin

Parameters

ipv4-acl-number: Specifies an IPv4 ACL by its number in the range of 2000 to 3999, to match routes by destination.

ipv6-acl-number: Specifies an IPv6 ACL by its number in the range of 2000 to 3999, to match routes by destination.

prefix-list *prefix-list-name*: Specifies an IPv4 prefix list by its name, a case-sensitive string of 1 to 63 characters, to match routes by destination.

prefix-list *ipv6-prefix-name*: Specifies an IPv6 prefix list by its name, a case-sensitive string of 1 to 63 characters, to match routes by destination.

Usage guidelines

If you use a basic ACL (with a number from 2000 to 2999) configured with the **rule** [*rule-id*] { **deny** | **permit** } **source** *source-address source-wildcard* command, the

command matches routes whose destination network addresses match the *source-address source-wildcard* argument. However, it does not match the masks of the destination addresses.

To use an advanced ACL (with a number from 3000 to 3999) in the command, configure the ACL using one of the following steps:

- To deny/permit a route with the specified destination, use the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* command.
- To deny/permit a route with the specified destination and mask, use the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* **destination** *dest-addr dest-wildcard* command.

The **source** keyword specifies the destination address of a route and the **destination** keyword specifies the subnet mask of the destination address. For the mask configuration to take effect, specify a contiguous subnet mask.

Examples

In BGP IPv4 unicast address family view, use IPv4 basic ACL 2000 to filter received BGP routes.

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default] address-family ipv4 unicast
[Switch-bgp-default-ipv4] filter-policy 2000 import
```

Related commands

filter-policy export

peer as-path-acl

peer filter-policy

peer prefix-list

peer route-policy

5.1.30. graceful-restart

Use **graceful-restart** to enable BGP Graceful Restart (GR) capability.

Use **undo graceful-restart** to disable BGP GR capability.

Syntax

graceful-restart

undo graceful-restart

Default

BGP GR capability is disabled.

Views

BGP instance view

Predefined user roles

network-admin

Usage guidelines

GR ensures continuous forwarding when BGP restarts or an active/standby switchover occurs.

BGP peers exchange Open messages containing GR information. If both parties have GR capability, they establish a GR-capable session.

After you execute this command, the device re-establishes BGP sessions.

Examples

Enable GR capability for BGP process 100.

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default] graceful-restart
```

Related commands

graceful-restart timer restart

graceful-restart timer wait-for-rib

5.1.31. graceful-restart timer restart

Use **graceful-restart timer restart** to configure the GR timer.

Use **undo graceful-restart timer restart** to restore the default.

Syntax

graceful-restart timer restart *timer*

undo graceful-restart timer restart

Default

The GR timer is 150 seconds.

Views

BGP instance view

Predefined user roles

network-admin

Parameters

timer: Specifies the GR timer in the range of 3 to 600 seconds.

Usage guidelines

The GR restarter sends the GR timer to the GR helper in an Open message. When the GR helper detects that an active/standby switchover or a BGP restart occurred on the GR restarter, the GR helper performs the following operations:

1. Marks all routes learned from the GR restarter as stale.
2. Starts the GR timer.
3. If no BGP session is established before the GR timer expires, the GR helper removes the stale routes.

Before you configure this command, enable the BGP GR capability.

To apply a new GR timer, you must re-establish BGP sessions.

Examples

Set the GR timer to 300 seconds.

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default] graceful-restart
[Switch-bgp-default] graceful-restart timer restart 300
```

Related commands

graceful-restart

graceful-restart timer wait-for-rib

5.1.32. graceful-restart timer wait-for-rib

Use **graceful-restart timer wait-for-rib** to configure the time to wait for the End-of-RIB marker.

Use **undo graceful-restart timer wait-for-rib** to restore the default.

Syntax

graceful-restart timer wait-for-rib *timer*

undo graceful-restart timer wait-for-rib

Default

The time to wait for the End-of-RIB marker is 600 seconds.

Views

BGP instance view

Predefined user roles

network-admin

Parameters

timer: Specifies the time to wait for the End-of-RIB marker, in the range of 3 to 3600 seconds.

Usage guidelines

BGP uses this timer to control the time to receive updates from the peer. The timer is not advertised to the peer.

After the GR restarter and GR helper re-establish a BGP session, they start this timer. If they do not complete route exchange within the time period, the GR restarter does not receive new routes. It updates its routing table and forwarding table with learned BGP routes, and the GR helper removes the stale routes. Set a large value for the maximum time to wait for the End-of-RIB marker when a large number of routes exist.

This command controls the routing convergence speed. A smaller timer value means faster routing convergence but possibly results in incomplete routing information.

Before configuring this command, you must enable the BGP GR capability.

Examples

Set the time to wait for the End-of-RIB marker on the local end to 100 seconds.

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default] graceful-restart
[Switch-bgp-default] graceful-restart timer wait-for-rib 100
```

Related commands

graceful-restart

graceful-restart timer restart

5.1.33. group

Use **group** to create a peer group.

Use **undo group** to delete a peer group.

Syntax

group *group-name* [**external** | **internal**]

undo group *group-name*

Default

No peer groups exist.

Views

BGP instance view

BGP-VPN instance view

Predefined user roles

network-admin

Parameters

group-name: Specifies a name for the peer group, a case-sensitive string of 1 to 47 characters.

external: Creates an EBGP peer group.

internal: Creates an IBGP peer group.

Usage guidelines

In a large-scale network, many peers can use the same route selection policy. You can configure a peer group and add these peers into this group. In this way, peers can share the same policy as the peer group. When the policy of the group is modified, the modification also applies to peers in it.

If you do not specify the **internal** or **external** keyword, this command creates an IBGP peer group.

If you perform configurations on a peer group and peers of the peer group, the most recent configuration takes effect.

After you create a peer group, you must use the **peer enable** command to enable BGP to exchange routing information with the specified peer group.

Examples

In BGP instance view, create EBGP peer group **test** with AS number 200, and add EBGP peers 10.1.1.1 and 10.1.2.1 into the group.

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default] group test external
[Switch-bgp-default] peer test as-number 200
[Switch-bgp-default] peer 10.1.1.1 group test
[Switch-bgp-default] peer 10.1.2.1 group test
```

Related commands

display bgp group

peer enable

5.1.34. import-route

Use **import-route** to enable BGP to redistribute routes from an IGP protocol.

Use **undo import-route** to disable route redistribution from an IGP protocol.

Syntax

In BGP IPv4 unicast address family view/BGP-VPN IPv4 unicast address family view:

import-route { **ospf** | **rip** } [{ *process-id* | **all-processes** } [**med** *med-value* | **route-policy** *route-policy-name*] *] [**inherit-tag**]

import-route { **direct** | **static** } [**med** *med-value* | **route-policy** *route-policy-name*]

undo import-route { **direct** | { **ospf** | **rip** } [*process-id* | **all-processes**] | **static** }

In BGP IPv6 unicast address family view/BGP-VPN IPv6 unicast address family view:

import-route { **ospfv3** | **ripng** } [{ *process-id* | **all-processes** } [**med** *med-value* | **route-policy** *route-policy-name*] *] [**inherit-tag**]

import-route { **direct** | **static** } [**med** *med-value* | **route-policy** *route-policy-name*]

undo import-route { **direct** | { **ospfv3** | **ripng** } [*process-id* | **all-processes**] | **static** }

Default

BGP does not redistribute IGP routes.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP IPv6 unicast address family view

BGP-VPN IPv6 unicast address family view

Predefined user roles

network-admin

Parameters

direct: Redistributes direct routes.

ospf: Redistributes OSPF routes.

ospfv3: Redistributes OSPFv3 routes.

rip: Redistributes RIP routes.

ripng: Redistributes RIPng routes.

static: Redistributes static routes.

process-id: Specifies a process by its ID in the range of 1 to 65535. The default is 1. For IPv4 routes, it is available only when the protocol is **ospf**, or **rip**. For IPv6 routes, it is available only when the protocol is **ospfv3**, or **ripng**.

all-processes: Redistributes routes from all the processes of the specified IGP protocol.

med *med-value*: Specifies a MED value for redistributed routes, in the range of 0 to 4294967295. If you do not specify an MED, the metric of a redistributed route is used as its MED.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters, to filter redistributed routes or set route attributes for redistributed routes.

inherit-tag: Adds the tag community attribute to BGP routes generated from redistributed IGP routes, inheriting the original IGP route tags.

Usage guidelines

The **import-route** command cannot redistribute default IGP routes. To redistribute default IGP routes, use the **default-route imported** command together with the **import-route** command.

Only active routes can be redistributed. You can use the **display ip routing-table protocol** or **display ipv6 routing-table protocol** command to view route state information.

The ORIGIN attribute of routes redistributed by the **import-route** command is INCOMPLETE.

If you have specified the **all-processes** keyword to redistribute all routes of a routing protocol, this command no longer takes effect on any processes of the routing protocol.

The tag community attribute added to BGP routes depends on the configuration of the **apply tag** command under the following conditions:

- Both the **inherit-tag** and **route-policy** *route-policy-name* parameters are specified.
- The specified routing policy contains an **apply tag** clause.

Examples

In BGP IPv4 unicast address family view, redistribute routes from RIP process 1, and set the MED value for redistributed routes to 100.

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default] address-family ipv4 unicast
[Switch-bgp-default-ipv4] import-route rip 1 med 100
```

Related commands

display ip routing-table protocol

display ipv6 routing-table protocol

5.1.35. ip vpn-instance (BGP instance view)

Use **ip vpn-instance** to create a BGP-VPN instance and enter its view, or enter the view of an existing BGP-VPN instance.

Use **undo ip vpn-instance** to remove a BGP-VPN instance and all its configurations.

Syntax

ip vpn-instance *vpn-instance-name*

undo ip vpn-instance *vpn-instance-name*

Default

No BGP-VPN instances exist.

Views

BGP instance view

Predefined user roles

network-admin

Parameters

vpn-instance-name: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

After you create a BGP peer in BGP-VPN instance view, the BGP routes learned from the peer are added into the routing table of the specified VPN instance.

This command and all commands in BGP-VPN instance view are typically executed on provider edge (PE) or Multi-VPN-Instance CE (MCE) devices. The commands add routes learned from different sites into different VPN instances.

Before you execute this command, you must perform the following tasks:

- Use the **ip vpn-instance** command to create the VPN instance in system view.
- Use the **route-distinguisher** command to configure a route distinguisher (RD) for the VPN instance.

Examples

Create a BGP-VPN instance and enter its view.

```
<Switch> system-view
[Switch] ip vpn-instance vpn1
[Switch-vpn-instance-vpn1] route-distinguisher 100:1
[Switch-vpn-instance-vpn1] quit
[Switch] bgp 100
[Switch-bgp-default] ip vpn-instance vpn1
[Switch-bgp-default-vpn1]
```

Related commands

ip vpn-instance (system view) (*MCE Command Reference*)

route-distinguisher (*MCE Command Reference*)

5.1.36. log-peer-change

Use **log-peer-change** to enable logging for BGP session state changes globally.

Use **undo log-peer-change** to disable logging for BGP session state changes globally.

Syntax

log-peer-change

undo log-peer-change

Default

Logging for BGP session state changes is enabled globally.

Views

BGP instance view

Predefined user roles

network-admin

Usage guidelines

After you execute both the **log-peer-change** and **peer log-change** commands, BGP logs session establishment and disconnection events for the peer or peer group. To display the log information, use the **display bgp peer ipv4 unicast log-info** command or the **display bgp peer ipv6 unicast log-info** command. The logs are sent to the information center of the device. The output rules of the logs (whether to output the logs and where to output) are determined by the information center configuration. For more information about information center configuration, see *Network Management and Monitoring Configuration Guide*.

If you disable logging for BGP session state changes globally or disable logging for a peer or peer group, BGP does not generate logs for session establishments and disconnections.

Examples

Enable logging for session state changes globally.

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default] log-peer-change
```

Related commands

display bgp peer

peer log-change

5.1.37. network

Use **network** to inject a network to the BGP routing table and configure BGP to advertise the network.

Use **undo network** to remove a local network.

Syntax

In BGP IPv4 unicast address family view/BGP-VPN IPv4 unicast address family view:

network *ipv4-address* [*mask-length* | *mask*] [**route-policy** *route-policy-name*]

undo network *ipv4-address* [*mask-length* | *mask*]

In BGP IPv6 unicast address family view/BGP-VPN IPv6 unicast address family view:

network *ipv6-address prefix-length* [**route-policy** *route-policy-name*]

undo network *ipv6-address prefix-length*

Default

BGP does not advertise local networks.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP IPv6 unicast address family view

BGP-VPN IPv6 unicast address family view

Predefined user roles

network-admin

Parameters

ipv4-address: Specifies an IPv4 network address. If you do not specify the *mask* or *mask-length* argument, natural mask is used.

mask-length: Specifies a mask length in the range of 0 to 32.

mask: Specifies a mask in dotted decimal notation.

ipv6-address: Specifies an IPv6 network address.

prefix-length: Specifies a prefix length in the range of 0 to 128.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters, to filter routes or set the route attributes.

Usage guidelines

The network to be injected must be available and active in the local IP routing table.

The ORIGIN attribute of the route injected with the **network** command is IGP.

When you execute the **undo network** command, you must specify the same mask or mask length/prefix length that you specified for the **network** command. Otherwise, the configuration cannot be removed.

Examples

In BGP IPv4 unicast address family view, inject local network 10.0.0.0/16 to the BGP routing table.

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default] address-family ipv4 unicast
[Switch-bgp-default-ipv4] network 10.0.0.0 255.255.0.0
```

5.1.38. non-stop-routing

MEMO:

non-stop-routing command is supported from later software, including Version 7.2.16.

Use **non-stop-routing** to enable BGP nonstop routing (NSR).

Use **undo non-stop-routing** to disable BGP NSR.

Syntax

non-stop-routing

undo non-stop-routing

Default

BGP NSR is disabled.

Views

BGP instance view

Predefined user roles

network-admin

Usage guidelines

BGP NSR ensures continuous routing by synchronizing BGP state and data information from the active BGP process to the standby BGP process. The standby BGP process can seamlessly take over all services when the active process fails.

Examples

Enable BGP NSR.

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default] non-stop-routing
```

5.1.39. network short-cut

Use **network short-cut** to increase the preference for a received EBGP route. This EBGP route is called a shortcut route.

Use **undo network short-cut** to remove the configuration.

Syntax

In BGP IPv4 unicast address family view/BGP-VPN IPv4 unicast address family view:

network *ipv4-address* [*mask-length* | *mask*] **short-cut**

undo network *ipv4-address* [*mask-length* | *mask*] **short-cut**

In BGP IPv6 unicast address family view/BGP-VPN IPv6 unicast address family view:

network *ipv6-address prefix-length* **short-cut**

undo network *ipv6-address prefix-length* **short-cut**

Default

A received EBGP route has a preference of 255.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP IPv6 unicast address family view

BGP-VPN IPv6 unicast address family view

Predefined user roles

network-admin

Parameters

ipv4-address: Specifies an IPv4 network address. If you do not specify the *mask* or *mask-length* argument, natural mask is used.

mask-length: Specifies a mask length in the range of 0 to 32.

mask: Specifies a mask for the network address, in dotted decimal notation.

ipv6-address: Specifies an IPv6 network address.

prefix-length: Specifies a prefix length in the range of 0 to 128.

Usage guidelines

Different routing protocols might find different routes to the same destination. However, not all of those routes are optimal. For route selection, routing protocols, direct routes, and static routes are assigned different preferences. The route with the highest preference is preferred.

By default, the preference of an EBGP route is lower than a local route. If a device has an EBGP route and a local route to reach the same destination, the device does not select the EBGP route. You can use the **network shortcut** command to configure the EBGP route to have the same preference as the local route so the EBGP route is more likely to become the optimal route.

You can use the **preference** command to modify the preferences for external and local BGP routes.

Examples

In BGP IPv4 unicast address family view, increase the preference of EBGP route 10.0.0.0/16.

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default] address-family ipv4 unicast
[Switch-bgp-default-ipv4] network 10.0.0.0 255.255.0.0 short-cut
```

Related commands

preference

5.1.40. peer additional-paths

Use **peer additional-paths** to configure the BGP additional path capabilities.

Use **undo peer additional-paths** to remove the configuration.

Syntax

In BGP IPv4 unicast address family view/BGP-VPN IPv4 unicast address family view:

peer { *group-name* | *ipv4-address* [*mask-length*] } **additional-paths** { **receive** | **send** } *

undo peer { *group-name* | *ipv4-address* [*mask-length*] } **additional-paths** { **receive** | **send** } *

In BGP IPv6 unicast address family view:

peer { *group-name* | *ipv6-address* [*prefix-length*] } **additional-paths** { **receive** | **send** } *

undo peer { *group-name* | *ipv6-address* [*prefix-length*] } **additional-paths** { **receive** | **send** } *

In BGP-VPN IPv6 unicast address family view:

peer { *group-name* | *ipv6-address* [*prefix-length*] } **additional-paths** { **receive** | **send** } *

undo peer { *group-name* | *ipv6-address* [*prefix-length*] } **additional-paths** { **receive** | **send** } *

Default

No BGP additional path capabilities are configured.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP IPv6 unicast address family view

BGP-VPN IPv6 unicast address family view

Predefined user roles

network-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command configures the BGP additional path capabilities for all dynamic peers in the subnet.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command configures the BGP additional path capabilities for all dynamic peers in the subnet.

receive: Enables the BGP additional path receiving capability.

send: Enables the BGP additional path sending capability.

Usage guidelines

You can enable the BGP additional path sending, receiving, or both sending and receiving capabilities on a BGP router. For two BGP peers to successfully negotiate the additional path capabilities, make sure one end has the sending capability and the other end has the receiving capability.

Examples

In BGP IPv4 unicast address family view, enable the BGP additional path receiving capability.

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default] address-family ipv4 unicast
[Switch-bgp-default-ipv4] peer 1.1.1.1 additional-paths receive
```

5.1.41. peer advertise additional-paths best

Use **peer advertise additional-paths best** to set the maximum number of Add-Path optimal routes that can be advertised to a peer or peer group.

Use **undo peer advertise additional-paths best** to remove the configuration.

Syntax

In BGP IPv4 unicast address family view/BGP-VPN IPv4 unicast address family view:

peer { *group-name* | *ipv4-address* [*mask-length*] } **advertise additional-paths best** *number*

undo peer { *group-name* | *ipv4-address* [*mask-length*] } **advertise additional-paths best**

In BGP IPv6 unicast address family view:

peer { *group-name* | *ipv6-address* [*prefix-length*] } **advertise additional-paths best** *number*

undo peer { *group-name* | *ipv6-address* [*prefix-length*] } **advertise additional-paths best**

In BGP-VPN IPv6 unicast address family view:

peer { *group-name* | *ipv6-address* [*prefix-length*] } **advertise additional-paths best** *number*

undo peer { *group-name* | *ipv6-address* [*prefix-length*] } **advertise additional-paths best**

Default

A maximum of one Add-Path optimal route can be advertised to a peer or peer group.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP IPv6 unicast address family view

BGP-VPN IPv6 unicast address family view

Predefined user roles

network-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command sets the maximum number of Add-Path optimal routes that can be advertised to all dynamic peers in the subnet.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command sets the maximum number of Add-Path optimal routes that can be advertised to all dynamic peers in the subnet.

number: Specifies the maximum number of Add-Path optimal routes that can be advertised to a peer or peer group, in the range of 2 to 32.

Usage guidelines

If the number of Add-Path optimal routes advertised to a peer or peer group exceeds the number of optimal routes, the number of optimal routes takes effect.

Examples

In BGP IPv4 unicast address family view, set the maximum number to 3 for Add-Path optimal routes that can be advertised to peer 1.1.1.1.

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default] address-family ipv4 unicast
[Switch-bgp-default-ipv4] peer 1.1.1.1 advertise additional-paths best 3
```

Related commands

additional-paths select-best

peer additional-paths

5.1.42. peer advertise-community

Use **peer advertise-community** to advertise the COMMUNITY attribute to a peer or peer group.

Use **undo peer advertise-community** to disable the COMMUNITY attribute advertisement to a peer or peer group.

Syntax

In BGP IPv4 unicast address family view/BGP-VPN IPv4 unicast address family view/BGP EVPN address family view:

peer { *group-name* | *ipv4-address* [*mask-length*] } **advertise-community**

undo peer { *group-name* | *ipv4-address* [*mask-length*] } **advertise-community**

In BGP IPv6 unicast address family view:

peer { *group-name* | *ipv6-address* [*prefix-length*] } **advertise-community**

undo peer { *group-name* | *ipv6-address* [*prefix-length*] } **advertise-community**

In BGP-VPN IPv6 unicast address family view:

peer { *group-name* | *ipv6-address* [*prefix-length*] } **advertise-community**

undo peer { *group-name* | *ipv6-address* [*prefix-length*] } **advertise-community**

Default

No COMMUNITY attribute is advertised to any peers or peer groups.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP IPv6 unicast address family view

BGP-VPN IPv6 unicast address family view

BGP EVPN address family view

Predefined user roles

network-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command advertises the COMMUNITY attribute to all dynamic peers in the subnet.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command advertises the COMMUNITY attribute to all dynamic peers in the subnet.

Usage guidelines

The COMMUNITY attribute is a group of specific data carried in update messages. A route can carry one or more COMMUNITY attribute values (each is represented by a 4-byte integer). The receiving router processes the route (for example, determining whether to advertise the route and the scope for advertising the route) based on the COMMUNITY attribute values.

After you execute the **peer advertise-community** command, routing updates advertised to the peer carry the COMMUNITY attribute.

After you execute the **undo peer advertise-community** command, BGP, upon receiving a route with the COMMUNITY attribute, removes the COMMUNITY attribute before sending the route to the peer or peer group.

Examples

In BGP IPv4 unicast address family view, advertise the COMMUNITY attribute to peer group **test**.

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default] address-family ipv4 unicast
[Switch-bgp-default-ipv4] peer test advertise-community
```

Related commands

apply community

if-match community

ip community-list

5.1.43. peer advertise-ext-community

Use **peer advertise-ext-community** to advertise the extended community attribute to a peer or peer group.

Use **undo peer advertise-ext-community** to disable the extended community attribute advertisement to a peer or peer group.

Syntax

In BGP IPv4 unicast address family view/BGP-VPN IPv4 unicast address family view:

peer { *group-name* | *ipv4-address* [*mask-length*] } **advertise-ext-community**

undo peer { *group-name* | *ipv4-address* [*mask-length*] } **advertise-ext-community**

In BGP IPv6 unicast address family view:

peer { *group-name* | *ipv6-address* [*prefix-length*] } **advertise-ext-community**

undo peer { *group-name* | *ipv6-address* [*prefix-length*] } **advertise-ext-community**

In BGP-VPN IPv6 unicast address family view:

peer { *group-name* | *ipv6-address* [*prefix-length*] } **advertise-ext-community**

undo peer { *group-name* | *ipv6-address* [*prefix-length*] } **advertise-ext-community**

Default

No extended community attribute is advertised to any peers or peer groups.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP IPv6 unicast address family view

BGP-VPN IPv6 unicast address family view

Predefined user roles

network-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command advertises the extended community attribute to all dynamic peers in the subnet.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command advertises the extended community attribute to all dynamic peers in the subnet.

Usage guidelines

To meet increasing user demands, BGP defines a new attribute—extended community attribute. The extended community attribute has the following advantages over the COMMUNITY attribute:

- The extended community attribute has an 8-byte length.
- The extended community attribute supports various types. You can select an extended community attribute type as needed to implement route filtering and control. This simplifies configuration and management.

After you execute the **peer advertise-ext-community** command, route updates sent to the peer or peer group carry the extended community attribute.

After you execute the **undo peer advertise-ext-community** command, BGP, upon receiving a route with the extended community attribute, removes the extended community attribute before sending the route to the peer or peer group.

Examples

In BGP IPv4 unicast address family view, advertise the extended community attribute to peer group **test**.

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default] address-family ipv4 unicast
[Switch-bgp-default-ipv4] peer test advertise-ext-community
```

Related commands

apply extcommunity

if-match extcommunity

ip extcommunity-list

5.1.44. peer advertise tag

Use **peer advertise tag** to enable BGP to advertise the tag community attribute to a peer or peer group.

Use **undo peer advertise tag** to restore the default.

Syntax

peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **advertise tag**

undo peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **advertise tag**

Default

BGP does not advertise the tag community attribute to a peer or peer group.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP IPv6 unicast address family view

BGP-VPN IPv6 unicast address family view

BGP VPNv4 address family view

BGP VPNv6 address family view

BGP EVPN address family view

Predefined user roles

network-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, all dynamic peers in the subnet are specified.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, all dynamic peers in the subnet are specified.

Usage guidelines

Application scenarios

When routes are redistributed from a routing protocol into an IGP, the IGP can add a tag for them. This tag can be used for route filtering methods such as routing policies. Routing information is distributed across ASs after it is redistributed between IGPs and BGP. As a result, different route filtering methods might be applied to an IGP route when it exists in different ASs. To remove the impact of route location on the selection of route filtering methods, you can enable BGP to transmit the tag of IGP routes. After IGP routes are distributed to other ASs, IGP routes with the same tag will match the same route filtering method, regardless of their locations.

Operating mechanism

The tag community attribute is an NEC-proprietary extended community attribute, which is designed for transmitting IGP route tags.

NOTE:
For brief introduction, a BGP route carrying the tag community attribute is called tagged route. When BGP tags a route, it adds the tag community attribute to that route. When BGP untags a route, it removes the tag community attribute from that route.

The **peer advertise tag** command functions as follows:

- Before advertising a BGP route derived from a redistributed IGP route to the specified peer or peer group, BGP tags that route. The value of the tag community attribute depends on the configuration of the **import-route** command.
  - After receiving a tagged BGP route, BGP forwards that route to the specified peer or peer group without untagging.

If the **peer advertise tag** commands is not configured or the **undo peer advertise tag** command is configured, BGP untags BGP routes (if tagged) before advertising them to peers. In this situation, BGP does not support the following operations:

- Tags BGP routes before route advertisement.

- Advertises BGP routes without untagging.

Restrictions and guidelines

The tag community attribute might be unrecognizable for devices from other vendors or have conflicts with other private extended community attributes. You can use the **extcommunity-type tag** command to adjust the type value to a recognizable or non-conflicting one for the tag community attribute.

Examples

In BGP IPv4 unicast address family view, enable BGP to advertise the tag community attribute to peer group **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family ipv4 unicast
[Sysname-bgp-default-ipv4] peer test advertise tag
```

Related commands

extcommunity-type tag

5.1.45. peer allow-as-loop

Use **peer allow-as-loop** to allow a local AS number to exist in the AS_PATH attribute of routes from a peer or peer group, and to set the number of times the local AS number can appear.

Use **undo peer allow-as-loop** to remove the configuration.

Syntax

In BGP IPv4 unicast address family view/BGP-VPN IPv4 unicast address family view/BGP EVPN address family view:

peer { *group-name* | *ipv4-address* [*mask-length*] } **allow-as-loop** [*number*]

undo peer { *group-name* | *ipv4-address* [*mask-length*] } **allow-as-loop**

In BGP IPv6 unicast address family view:

peer { *group-name* | *ipv6-address* [*prefix-length*] } **allow-as-loop** [*number*]

undo peer { *group-name* | *ipv6-address* [*prefix-length*] } **allow-as-loop**

In BGP-VPN IPv6 unicast address family view:

peer { *group-name* | *ipv6-address* [*prefix-length*] } **allow-as-loop** [*number*]

undo peer { *group-name* | *ipv6-address* [*prefix-length*] } **allow-as-loop**

Default

The local AS number is not allowed to exist in the AS_PATH attribute of routes from a peer or peer group.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP IPv6 unicast address family view

BGP-VPN IPv6 unicast address family view

BGP EVPN address family view

Predefined user roles

network-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet in this command, BGP allows a local AS number to exist in the AS_PATH attribute of routes from all dynamic peers in the subnet.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet in this command, BGP allows a local AS number to exist in the AS_PATH attribute of routes from all dynamic peers in the subnet.

number: Specifies the number of times for which the local AS number can appear, in the range of 1 to 10. The default number is 1. If the number of times for which the local AS number appears in a route is more than the specified number, BGP considers that a routing loop occurs and discards the route.

Usage guidelines

By default, BGP does not receive routes that contain the local AS number in the AS_PATH attribute to avoid routing loops. However, in some network environments, the AS_PATH attribute of a route from a peer must be allowed to contain the local AS number. Otherwise, the route cannot be advertised correctly.

Examples

In BGP IPv4 unicast address family view, set the number of times the local AS number can appear in AS_PATH attribute of routes from peer group **test** to 2.

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default] address-family ipv4 unicast
[Switch-bgp-default-ipv4] peer test allow-as-loop 2
```

5.1.46. peer as-number (for a BGP peer group)

Use **peer as-number** to specify an AS number for a peer group.

Use **undo peer as-number** to delete the AS number of a peer group.

Syntax

peer *group-name* **as-number** *as-number*

undo peer *group-name* **as-number**

Default

No AS number is specified for a peer group.

Views

BGP instance view

BGP-VPN instance view

Predefined user roles

network-admin

Parameters

group-name: Specifies a name for a peer group, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

as-number: Specifies an AS number for a peer group, in the range of 1 to 4294967295.

Usage guidelines

This command applies only to a peer group with no peers in it.

When you specify an AS number for a peer group and want to add peers to it, make sure the AS number of the peers is the same as the peer group.

If you do not specify an AS number for a peer group, peers added to it can use their own AS numbers.

Examples

In BGP instance view, set the AS number for peer group **test** to 100.

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default] peer test as-number 100
```

Related commands

peer group

5.1.47. peer as-number (for a BGP peer)

Use **peer as-number** to create a BGP peer and specify its AS number.

Use **undo peer** to delete a BGP peer.

Syntax

peer { *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **as-number** *as-number*

undo peer { *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] }

Default

No BGP peers exist.

Views

BGP instance view

BGP-VPN instance view

Predefined user roles

network-admin

Parameters

ipv4-address: Specifies the IPv4 address of a peer.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command enables BGP to establish dynamic peer relationships with all devices in the subnet.

ipv6-address: Specifies the IPv6 address of a peer.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command enables BGP to establish dynamic peer relationships with all devices in the subnet.

as-number: Specifies an AS number for the peer, in the range of 1 to 4294967295. If the AS numbers of the peer and the local router are the same, the peer is an IBGP peer. If they are different, the peer is an EBGP peer.

Usage guidelines

You can also create a peer and add it to a peer group by using the **peer group** command.

To modify the AS number of a peer, do not execute the **peer as-number** command repeatedly. Instead, you must first delete the peer and configure it again.

After you create a peer, you must use the **peer enable** command to enable BGP to exchange routing information with the specified peer.

For a remote device to establish a peer relationship with the local device, you must specify the IP address of the local device on the remote device.

Examples

In BGP instance view, create BGP peer 1.1.1.1 and set its AS number to 100.

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default] peer 1.1.1.1 as-number 100
```

Related commands

display bgp peer

peer enable

peer group

5.1.48. peer as-path-acl

Use **peer as-path-acl** to specify an AS path list to filter routes incoming from or outgoing to a peer or peer group.

Use **undo peer as-path-acl** to delete the AS path list specified to filter routes incoming from or outgoing to a peer or peer group.

Syntax

In BGP IPv4 unicast address family view/BGP-VPN IPv4 unicast address family view:

peer { *group-name* | *ipv4-address* [*mask-length*] } **as-path-acl** as*-path-acl-number* { **export** | **import** }

undo peer { *group-name* | *ipv4-address* [*mask-length*] } **as-path-acl** { **export** | **import** }

In BGP IPv6 unicast address family view:

peer { *group-name* | *ipv6-address* [*prefix-length*] } **as-path-acl** *as-path-acl-number* { **export** | **import** }

undo peer { *group-name* | *ipv6-address* [*prefix-length*] } **as-path-acl** { **export** | **import** }

In BGP-VPN IPv6 unicast address family view:

peer { *group-name* | *ipv6-address* [*prefix-length*] } **as-path-acl** *as-path-acl-number* { **export** | **import** }

undo peer { *group-name* | *ipv6-address* [*prefix-length*] } **as-path-acl** { **export** | **import** }

Default

No AS path list is specified for filtering.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP IPv6 unicast address family view

BGP-VPN IPv6 unicast address family view

Predefined user roles

network-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command specifies an AS path list to filter routes incoming from or outgoing to all dynamic peers in the subnet.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command specifies an AS path list to filter routes incoming from or outgoing to all dynamic peers in the subnet.

as-path-acl-number: Specifies an AS path list by its number in the range of 1 to 256.

export: Filters outgoing routes.

import: Filters incoming routes.

Usage guidelines

The specified AS path list must have been created with the **ip as-path** command in system view. If you specify a nonexistent AS path list, all routes can pass the AS path list.

Examples

In BGP IPv4 unicast address family view, specify AS path list 1 to filter routes outgoing to peer group **test**.

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default] address-family ipv4 unicast
[Switch-bgp-default-ipv4] peer test as-path-acl 1 export
```

Related commands

filter-policy export

filter-policy import

ip as-path

peer filter-policy

peer prefix-list

peer route-policy

5.1.49. peer bfd

Use **peer bfd** to enable BFD for the link to a BGP peer or peer group.

Use **undo peer bfd** to remove the configuration.

Syntax

peer { *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **bfd** [**multi-hop** | **single-hop**]

undo peer { *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **bfd**

Default

BFD is disabled for the link to a BGP peer or peer group.

Views

BGP instance view

BGP-VPN instance view

Predefined user roles

network-admin

Parameters

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command enables BFD for links to all dynamic peers in the subnet.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command enables BFD for links to all dynamic peers in the subnet.

multi-hop: Enables multi-hop BFD.

single-hop: Enables single-hop BFD.

Usage guidelines

When you do not specify the **multi-hop** keyword or the **single-hop** keyword:

- If an IBGP peer or peer group is specified, this command enables multi-hop BFD for the IBGP peer or peer group.
- If a directly connected EBGP peer or peer group is specified and the **peer ebgp-max-hop** command is not configured, this command enables single-hop BFD for the EBGP peer or peer group. If the EBGP peer or peer group is not directly connected or the **peer ebgp-max-hop** command is configured, this command enables multi-hop BFD for the EBGP peer or peer group.

For more information about multi-hop and single-hop BFD, see *High Availability Configuration Guide*.

BFD helps speed up BGP routing convergence upon link failures. However, if you have enabled GR, use BFD with caution. BFD might detect a failure before the system performs GR, resulting in GR failure. If you have enabled both BFD and GR for BGP, do not disable BFD during a GR process to avoid GR failure.

To establish a BFD session to a BGP peer, you must configure the same BFD detection mode (multi-hop or single-hop) on the local router and the BGP peer.

Examples

In BGP instance view, enable BFD for the link to BGP peer group **test**.

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default] peer test bfd
```

Related commands

display bfd session (*High Availability Command Reference*)

display bgp peer

5.1.50. peer capability-advertise conventional

Use **peer capability-advertise conventional** to disable the BGP multi-protocol extension, route refresh, and 4-byte AS number features for a peer or peer group.

Use **undo peer capability-advertise conventional** to enable the BGP multi-protocol extension, route refresh, and 4-byte AS number features for a peer or peer group.

Syntax

peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **capability-advertise conventional**

undo peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **capability-advertise conventional**

Default

The BGP multi-protocol extension, route refresh, and 4-byte AS number features are enabled.

Views

BGP instance view

BGP-VPN instance view

Predefined user roles

network-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command disables BGP multi-protocol extension and route refresh for all dynamic peers in the subnet.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command disables BGP multi-protocol extension and route refresh for all dynamic peers in the subnet.

Usage guidelines

The route refresh feature enables BGP to send and receive Route-refresh messages and implement BGP session soft-reset.

The multi-protocol extension feature enables BGP to advertise and receive routing information for various protocols (for example, IPv6 routing information).

The 4-byte AS number feature enables BGP to use 4-byte AS numbers in the range of 1 to 4294967295.

If both the **peer capability-advertise conventional** and **peer capability-advertise route-refresh** commands are executed, the most recent configuration takes effect.

Examples

In BGP instance view, disable the multi-protocol extension, route refresh, and 4-byte AS number features for peer 1.1.1.1.

```
<Switch> system-view
```

```
[Switch] bgp 100
[Switch-bgp-default] peer 1.1.1.1 as-number 100
[Switch-bgp-default] peer 1.1.1.1 capability-advertise conventional
```

Related commands

display bgp peer

peer capability-advertise route-refresh

5.1.51. peer capability-advertise route-refresh

Use **peer capability-advertise route-refresh** to enable BGP route refresh for a peer or peer group.

Use **undo peer capability-advertise route-refresh** to disable BGP route refresh for a peer or peer group.

Syntax

peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **capability-advertise route-refresh**

undo peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **capability-advertise route-refresh**

Default

BGP route refresh is enabled.

Views

BGP instance view

BGP-VPN instance view

Predefined user roles

network-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command enables BGP route refresh for all dynamic peers in the subnet.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command enables BGP route refresh for all dynamic peers in the subnet.

Usage guidelines

The route refresh feature enables BGP to send and receive Route-refresh messages.

BGP uses the route refresh feature to implement BGP session soft-reset. After a policy is modified, the router advertises a Route-refresh message to the peers. The peers resend their routing information to the router. After receiving the routing information, the router filters the routing information by using the new policy. This method allows you to refresh the BGP routing table and apply the new route selection policy without tearing down BGP sessions.

BGP route refresh requires that both the local router and the peer support route refresh.

If both the **peer capability-advertise route-refresh** and **peer capability-advertise conventional** commands are executed, the most recent configuration takes effect.

Examples

In BGP instance view, enable BGP route refresh for peer 1.1.1.1.

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default] peer 1.1.1.1 as-number 100
[Switch-bgp-default] peer 1.1.1.1 capability-advertise route-refresh
```

Related commands

display bgp peer

peer capability-advertise conventional

peer keep-all-routes

refresh bgp

5.1.52. peer connect-interface

Use **peer connect-interface** to specify a source interface (IPv4 address/IPv6 address) for establishing TCP connections to a peer or peer group.

Use **undo peer connect-interface** to remove the configuration.

Syntax

peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **connect-interface** *interface-type interface-number*

undo peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **connect-interface**

Default

BGP uses the primary IPv4 or IPv6 address of the output interface in the optimal route destined for the BGP peer or peer group as the source address.

Views

BGP instance view

BGP-VPN instance view

Predefined user roles

network-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command specifies a source interface for establishing TCP connections to all dynamic peers in the network.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command specifies a source interface for establishing TCP connections to all dynamic peers in the subnet.

interface-type interface-number: Specifies an interface by its type and number.

Usage guidelines

The **peer connect-interface** command can change the source address for establishing TCP connections. If you execute both commands, the most recent configuration takes effect.

The **peer connect-interface** commands are applicable to the following scenarios:

- The peer's IPv4/IPv6 address does not belong to the interface directly connected to the local router. To ensure successful TCP connection establishment, use one of the following methods:
  - Specify the interface to which the IPv4/IPv6 address belongs as the source interface on the peer.
  - Specify the IPv4/IPv6 address of the interface directly connected to the local router as the source address on the peer.
- A BGP peer at an IPv6 link-local address must be directly connected to the local router. On the local router, you must use the **peer connect-interface** command to specify the interface directly connected to the BGP peer as the source interface of TCP connections.
- On a BGP router that has multiple links to a peer, the source interface for TCP connection changes because the primary source interface fails. To avoid this problem, specify a loopback interface as the source interface or specify the IP address of a loopback interface as the source address.

- You want to establish multiple BGP sessions to a router. In this case, BGP might fail to determine the source address for each TCP connection based on the optimal route to the peer. To prevent this problem, use one of the following methods:
  - If the BGP sessions use IP addresses of different interfaces, specify a source interface or source address for each session.
  - If the BGP sessions use different IP addresses of the same interface, specify a source address for each session.

The source interfaces on the local router and the peer must be reachable to each other.

To specify an indirectly connected interface on an EBGP peer as the source interface, use the **peer ebgp-max-hop** command. The command allows the establishment of an EBGP session to the indirectly connected peer.

If an interface has multiple IPv4 addresses, BGP uses the primary IPv4 address to establish TCP connections. If an interface has multiple IPv6 addresses, BGP selects a source IPv6 address.

You cannot specify a virtual template (VT) interface as the source interface for establishing TCP connections because a VT interface cannot process services.

Examples

In BGP instance view, specify loopback 0 as the source interface for TCP connections to peer group **test**.

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default] peer test connect-interface loopback 0
```

Related commands

peer ebgp-max-hop

5.1.53. peer default-route-advertise

Use **peer default-route-advertise** to advertise a default route to a peer or peer group.

Use **undo peer default-route-advertise** to disable default route advertisement to a peer or peer group.

Syntax

In BGP IPv4 unicast address family view/BGP-VPN IPv4 unicast address family view:

peer { *group-name* | *ipv4-address* [*mask-length*] } **default-route-advertise** [**route-policy** *route-policy-name*]

undo peer { *group-name* | *ipv4-address* [*mask-length*] } **default-route-advertise**

In BGP IPv6 unicast address family view:

peer { *group-name* | *ipv6-address* [*prefix-length*] } **default-route-advertise** [**route-policy** *route-policy-name*]

undo peer { *group-name* | *ipv6-address* [*prefix-length*] } **default-route-advertise**

In BGP-VPN IPv6 unicast address family view:

peer { *group-name* | *ipv6-address* [*prefix-length*] } **default-route-advertise** [**route-policy** *route-policy-name*]

undo peer { *group-name* | *ipv6-address* [*prefix-length*] } **default-route-advertise**

Default

No default route is advertised to any peers or peer groups.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP IPv6 unicast address family view

BGP-VPN IPv6 unicast address family view

Predefined user roles

network-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command advertises a default route to all dynamic peers in the subnet.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command advertises a default route to all dynamic peers in the subnet.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters, to modify the route attribute.

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

This command enables the router to send a default route with the next hop being itself to the peer or peer group regardless of whether the default route exists in the routing table.

Examples

In BGP IPv4 unicast address family view, advertise a default route to peer group **test**.

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default] address-family ipv4 unicast
[Switch-bgp-default-ipv4] peer test default-route-advertise
```

5.1.54. peer description

Use **peer description** to configure a description for a peer or peer group.

Use **undo peer description** to remove the description for a peer or peer group.

Syntax

peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **description** *text*

undo peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **description**

Default

No description information is configured for a peer or peer group.

Views

BGP instance view

BGP-VPN instance view

Predefined user roles

network-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command configures a description for all dynamic peers in the subnet.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command configures a description for all dynamic peers in the subnet.

text: Specifies a description for a peer or peer group, a case-sensitive string of 1 to 79 characters.

Examples

In BGP instance view, set the description for peer group **test** to **ISP1**.

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default] peer test description ISP1
```

5.1.55. peer ebgp-max-hop

Use **peer ebgp-max-hop** to enable BGP to establish an EBGP session to an indirectly connected peer or peer group and specify the maximum hop count.

Use **undo peer ebgp-max-hop** to disable BGP from establishing an EBGP session to an indirectly connected peer or peer group.

Syntax

peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **ebgp-max-hop** [*hop-count*]

undo peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **ebgp-max-hop**

Default

BGP does not establish an EBGP session to an indirectly connected peer or peer group.

Views

BGP instance view

BGP-VPN instance view

Predefined user roles

network-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet in this command, BGP establishes EBGP sessions to all indirectly connected dynamic peers in the subnet.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet in this command, BGP establishes EBGP sessions to all indirectly connected dynamic peers in the subnet.

hop-count: Specifies the maximum number of hop counts, in the range of 1 to 255. The default is 64.

Usage guidelines

To become EBGP peers, two routers must be directly connected and use directly connected interfaces to establish an EBGP session. If they are not directly connected, use the **peer ebgp-max-hop** command to establish an EBGP session over multiple hops between two peers.

This command takes effect only on routes received after you execute this command. To apply this command to existing routes, use the **refresh bgp** command to soft-reset BGP sessions.

When the BGP GTSM feature is enabled, two peers can establish an EBGP session after passing GTSM check, regardless of whether the maximum number of hops is reached.

Examples

In BGP instance view, enable BGP to establish EBGP sessions to indirectly connected EBGP peer group **test**, and set the maximum hop count to 64 (default).

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default] peer test ebgp-max-hop
```

5.1.56. peer enable

Use **peer enable** to enable BGP to exchange routing information for an address family with a peer or peer group.

Use **undo peer enable** to disable BGP from exchanging routing information for an address family with a peer or peer group.

Syntax

In BGP IPv4 unicast address family view/BGP-VPN IPv4 unicast address family view/BGP EVPN address family view:

peer { *group-name* | *ipv4-address* [*mask-length*] } **enable**

undo peer { *group-name* | *ipv4-address* [*mask-length*] } **enable**

In BGP IPv6 unicast address family view:

peer { *group-name* | *ipv6-address* [*prefix-length*] } **enable**

undo peer { *group-name* | *ipv6-address* [*prefix-length*] } **enable**

In BGP-VPN IPv6 unicast address family view:

peer { *group-name* | *ipv6-address* [*prefix-length*] } **enable**

undo peer { *group-name* | *ipv6-address* [*prefix-length*] } **enable**

Default

BGP cannot exchange routing information with a peer or peer group.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP IPv6 unicast address family view

BGP-VPN IPv6 unicast address family view

BGP EVPN address family view

Predefined user roles

network-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet in this command, BGP exchanges routing information for an address family with all dynamic peers in the subnet.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet in this command, BGP exchanges routing information for an address family with all dynamic peers in the subnet.

Usage guidelines

Executing the **peer enable** command in different views enables BGP to exchange routing information for the corresponding address families with the specified peer.

- In BGP IPv4 unicast address family view, the command enables the capability to exchange IPv4 unicast routing information. It also adds the learned routes to the BGP routing table of the public network.
- In BGP-VPN IPv4 unicast address family view, the command enables the capability to exchange IPv4 unicast routing information. It also adds the learned routes to the BGP routing table of the specified VPN instance.

- In BGP IPv6 unicast address family view, the command enables the capability to exchange IPv6 unicast routing information. It also adds the learned routes to the IPv6 BGP routing table of the public network.
- In BGP-VPN IPv6 unicast address family view, the command enables the capability to exchange IPv6 unicast routing information. It also adds the learned routes to the IPv6 BGP routing table of the specified VPN instance.

The **undo peer enable** command disables BGP to exchange routing information for the corresponding address family with the peer.

Examples

In BGP IPv4 unicast address family view, enable BGP to exchange IPv4 unicast routing information with peer 1.1.1.1.

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default] address-family ipv4 unicast
[Switch-bgp-default-ipv4] peer 1.1.1.1 enable
```

Related commands

display bgp peer

5.1.57. peer fake-as

Use **peer fake-as** to advertise a fake AS number to a peer or peer group.

Use **undo peer fake-as** to remove the fake AS number advertised to a peer or peer group.

Syntax

peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **fake-as** *as-number*

undo peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **fake-as**

Default

No fake local AS number is advertised to a peer or peer group.

Views

BGP instance view

BGP-VPN instance view

Predefined user roles

network-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command advertises a fake AS number to all dynamic peers in the subnet.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command advertises a fake AS number to all dynamic peers in the subnet.

as-number: Specifies a fake AS number in the range of 1 to 4294967295.

Usage guidelines

After you move a BGP router from an AS to another AS (from AS 2 to AS 3 for example), you have to modify the AS number of the router on all its EBGP peers. To avoid such modifications, you can configure the router to advertise a fake AS number 2 to its EBGP peers so that the EBGP peers still think that Router A is in AS 2.

The **peer fake-as** command is applicable only to EBGP peers or peer groups.

If you execute the **peer fake-as** command on the local router, specify the local router's AS number on the peer as the fake local AS number specified in the command.

Examples

In BGP instance view, advertise a fake AS number of 200 to peer group **test**.

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default] peer test fake-as 200
```

5.1.58. peer filter-policy

Use **peer filter-policy** to filter routes advertised to or received from a peer or peer group by using an ACL.

Use **undo peer filter-policy** to remove the ACL specified to filter routes advertised to or received from a peer or peer group.

Syntax

In BGP IPv4 unicast address family view/BGP-VPN IPv4 unicast address family view:

peer { *group-name* | *ipv4-address* [*mask-length*] } **filter-policy** *ipv4-acl-number* { **export** | **import** }

undo peer { *group-name* | *ipv4-address* [*mask-length*] } **filter-policy** { **export** | **import** }

In BGP IPv6 unicast address family view:

peer { *group-name* | *ipv6-address* [*prefix-length*] } **filter-policy** *ipv6-acl-number* { **export** | **import** }

undo peer { *group-name* | *ipv6-address* [*prefix-length*] } **filter-policy** { **export** | **import** }

In BGP-VPN IPv6 unicast address family view:

peer { *group-name* | *ipv6-address* [*prefix-length*] } **filter-policy** *ipv6-acl-number* { **export** | **import** }

undo peer { *group-name* | *ipv6-address* [*prefix-length*] } **filter-policy** { **export** | **import** }

Default

No ACL-based filtering is configured.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP IPv6 unicast address family view

BGP-VPN IPv6 unicast address family view

Predefined user roles

network-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command filters routes advertised to or received from all dynamic peers in the subnet by using an ACL.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command filters routes advertised to or received from all dynamic peers in the subnet by using an ACL.

ipv4-acl-number: Specifies an ACL by its number in the range of 2000 to 3999.

ipv6-acl-number: Specifies an IPv6 ACL by its number in the range of 2000 to 3999.

export: Filters routes advertised to the peer/peer group.

import: Filters routes received from the peer/peer group.

Usage guidelines

The specified ACL used by the **peer filter-policy** command must have been created with the **acl** command in system view. Otherwise, all routes can pass the ACL.

If you use a basic ACL (with a number from 2000 to 2999) configured with the **rule** [*rule-id*] { **deny** | **permit** } **source** *source-address source-wildcard* command, the command matches routes whose destination network addresses match the *source-address source-wildcard* argument without matching the masks of the destination addresses.

To use an advanced ACL (with a number from 3000 to 3999) in the command, configure the ACL using one of the following steps:

- To deny/permit a route with the specified destination, use the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* command.
- To deny/permit a route with the specified destination and mask, use the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* **destination** *dest-addr dest-wildcard* command.

The **source** keyword specifies the destination address of a route and the **destination** keyword specifies the subnet mask of the destination address. For the mask configuration to take effect, specify a contiguous subnet mask.

Examples

In BGP IPv4 unicast address family view, apply ACL 2000 to filter routes advertised to peer group **test**.

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default] address-family ipv4 unicast
[Switch-bgp-default-ipv4] peer test filter-policy 2000 export
```

Related commands

acl (*ACL and QoS Command Reference*)

filter-policy export

filter-policy import

peer as-path-acl

peer prefix-list

peer route-policy

5.1.59. peer group

Use **peer group** to add a peer to a peer group.

Use **undo peer group** to delete a peer from a peer group.

Syntax

peer { *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] }
group *group-name* [**as-number** *as-number*]

undo peer { *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] }
group *group-name*

Default

No peers exist in a peer group.

Views

BGP instance view

BGP-VPN instance view

Predefined user roles

network-admin

Parameters

ipv4-address: Specifies a peer by its IPv4 address.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command adds all dynamic peers in the subnet to a peer group.

ipv6-address: Specifies a peer by its IPv6 address.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command adds all dynamic peers in the subnet to a peer group.

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

as-number *as-number*: Specifies an AS for a peer by its number in the range of 1 to 4294967295.

Usage guidelines

You can add a peer to a peer group in the following ways:

- Use the **peer as-number** command to create a peer and specify its AS number, and then use the **peer group** command to add the peer to the peer group.
  - You can specify the **as-number** keyword for the **peer group** command. The AS number must be the same as the AS number specified in the **peer as-number** command.
  - If you have specified the AS number of the peer group with the **peer as-number** command, the peer to be added must have the same AS number as the peer group.
  - To add a peer to an IBGP peer group, the peer must be an IBGP peer.
- Use the **peer group** command to create a peer and add it to the peer group.

- If you have specified the AS number of the peer group with the **peer as-number** command, you do not need to specify the **as-number** keyword when you execute the **peer group** command. This is because the AS number of the peer is the same as the peer group. To specify the **as-number** keyword for the **peer group** command, make sure the AS number is the same as the peer group.
- If no AS number is specified for an EBGP peer group, specify the **as-number** keyword when you execute the **peer group** command.
- If no AS number is specified for an IBGP peer group, you do not need to specify the **as-number** keyword when you execute the **peer group** command. This is because the AS number of the IBGP peer group is the local AS number. To specify the **as-number** keyword for the **peer group** command, make sure the AS number is the same as the local AS number.

If you have specified the AS number of a peer group with the **peer as-number** command, only the peers with the same AS number can be added to the peer group. All peers in the group share the same AS number. If you have not specified the AS number for a peer group, peers added to it can use their own AS numbers.

After you add a peer to a peer group, you must use the **peer enable** command to enable BGP to exchange routing information with the peer group.

Examples

In BGP instance view, add peer 10.1.1.1 to EBGP peer group **test**.

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default] group test external
[Switch-bgp-default] peer 10.1.1.1 group test as-number 2004
```

Related commands

group

peer as-number

peer enable

5.1.60. peer ignore

Use **peer ignore** to disable BGP session establishment with a peer or peer group.

Use **undo peer ignore** to enable BGP session establishment with a peer or peer group.

Syntax

peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **ignore**

undo peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **ignore**

Default

BGP can establish a session to a peer or peer group.

Views

BGP instance view

BGP-VPN instance view

Predefined user roles

network-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet in this command, BGP tears down sessions to all dynamic peers in the subnet.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet in this command, BGP tears down sessions to all dynamic peers in the subnet.

graceful *graceful-time*: Gracefully shuts down the session to a peer or peer group in the specified graceful shutdown period of time. The value range for the *graceful-time* argument is 60 to 65535 seconds. If you do not specify this option, the command immediately shuts down the session to the peer or peer group.

community { *community-number* | *aa:nn* }: Specifies the community attribute for advertised routes. The *community-number* argument represents the community sequence number in the range of 1 to 4294967295. The *aa:nn* argument represents the community number. Both *aa* and *nn* are in the range of 0 to 65535. If you do not specify this option, the command does not change the community attribute for advertised routes.

local-preference *preference*: Specifies the local preference for advertised routes, in the range of 0 to 4294967295. A larger value represents a higher preference. If you do not specify this option, the command does not change the local preference for advertised routes.

med *med*: Specifies the MED value for advertised routes, in the range of 0 to 4294967295. The smaller the MED value, the higher the route priority. If you do not specify this option, the command does not change the MED value for advertised routes.

Usage guidelines

This command enables you to temporarily tear down the BGP session to a peer or peer group. You can perform network upgrade and maintenance without needing to delete and reconfigure the peer or peer group. To recover the session, execute the **undo peer ignore** command.

If a session has been established to a peer, executing the **peer ignore** command for the peer tears down the session and clears all related routing information.

If sessions have been established to a peer group, executing the **peer ignore** command for the peer group disables the sessions to all peers in the group and clears all related routing information.

If you specify the **graceful** keyword in the **peer ignore** command, BGP performs the following tasks:

- Gracefully shuts down the session to the specified peer or peer group in the specified graceful shutdown period of time.
- Advertises all routes to the specified peer or peer group and changes the attribute for the advertised routes to the specified value.
- Advertises routes from the specified peer or peer group to other IBGP peers and peer groups and changes the attribute for the advertised routes to the specified value.

Examples

In BGP instance view, disable session establishment with peer 1.1.1.1.

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default] peer 1.1.1.1 ignore
```

In BGP instance view, configure BGP to gracefully shut down the session to peer 1.1.1.1 in 60 seconds, advertise all routes to peer 1.1.1.1, and change the community attribute and local preference for the advertised routes to 1:1 and 200, respectively.

```
<Switch> system-view
[Switch] bgp 1
[Switch-bgp-default] peer 1.1.1.1 ignore graceful 60 community 1:1 local-preference 200
```

5.1.61. peer keep-all-routes

Use **peer keep-all-routes** to save all route updates from a peer or peer group, regardless of whether the routes have passed the configured routing policy.

Use **undo peer keep-all-routes** to remove the configuration.

Syntax

In BGP IPv4 unicast address family view/BGP-VPN IPv4 unicast address family view:

peer { *group-name* | *ipv4-address* [*mask-length*] } **keep-all-routes**

undo peer { *group-name* | *ipv4-address* [*mask-length*] } **keep-all-routes**

In BGP IPv6 unicast address family view:

peer { *group-name* | *ipv6-address* [*prefix-length*] } **keep-all-routes**

undo peer { *group-name* | *ipv6-address* [*prefix-length*] } **keep-all-routes**

In BGP-VPN IPv6 unicast address family view:

peer { *group-name* | *ipv6-address* [*prefix-length*] } **keep-all-routes**

undo peer { *group-name* | *ipv6-address* [*prefix-length*] } **keep-all-routes**

Default

Route updates from a peer or peer group are not saved.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP IPv6 unicast address family view

BGP-VPN IPv6 unicast address family view

Predefined user roles

network-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command saves all route updates from all dynamic peers in the subnet, regardless of whether the routes have passed the configured routing policy.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command saves all route updates from all dynamic peers in the subnet, regardless of whether the routes have passed the configured routing policy.

Usage guidelines

To implement BGP session soft-reset when the local router and a peer or peer group do not support the route refresh feature, use the **peer keep-all-routes** command. The command saves all route updates received from the peer or peer group. After modifying the route selection policy, filter all saved routes with the new policy to refresh the routing table. This method avoids tearing down BGP sessions.

Examples

In BGP IPv4 unicast address family view, save all route updates from peer 1.1.1.1.

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default] address-family ipv4 unicast
```

```
[Switch-bgp-default-ipv4] peer 1.1.1.1 keep-all-routes
```

Related commands

peer capability-advertise route-refresh

refresh bgp

5.1.62. peer log-change

Use **peer log-change** to enable logging for BGP session state changes for a peer or peer group.

Use **undo peer log-change** to disable logging for BGP session state changes for a peer or peer group.

Syntax

peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **log-change**

undo peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **log-change**

Default

Logging for BGP session state changes is enabled for all peers or peer groups.

Views

BGP instance view

BGP-VPN instance view

Predefined user roles

network-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must already exist.

ipv4-address: Specifies the IPv4 address of a peer. The peer must already exist.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command enables the logging of BGP session state changes for all dynamic peers in the subnet.

ipv6-address: Specifies the IPv6 address of a peer. The peer must already exist.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command enables the logging of BGP session state changes for all dynamic peers in the subnet.

Usage guidelines

After you execute both the **log-peer-change** and **peer log-change** commands, BGP logs session establishment and disconnection events for the peer or peer group. To view the log information, use the **display bgp peer ipv4 unicast log-info** command or the **display bgp peer ipv6 unicast log-info** command. The logs are sent to the information center of the device. The output rules of the logs (whether to output the logs and where to output) are determined by the information center configuration. For more information about information center configuration, see *Network Management and Monitoring Configuration Guide*.

If you disable logging for BGP session state changes globally or disable logging for a peer or peer group, BGP does not generate logs for session establishments and disconnections.

Examples

In BGP instance view, enable logging for BGP session state changes for peer 1.1.1.1.

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default] peer 1.1.1.1 as-number 200
[Switch-bgp-default] peer 1.1.1.1 log-change
```

Related commands

display bgp peer

log-peer-change

5.1.63. peer next-hop-local

Use **peer next-hop-local** to set the local router as the next hop for routes sent to a peer or peer group.

Use **undo peer next-hop-local** to remove the configuration.

Syntax

In BGP IPv4 unicast address family view/BGP-VPN IPv4 unicast address family view/BGP EVPN address family view:

peer { *group-name* | *ipv4-address* [*mask-length*] } **next-hop-local**

undo peer { *group-name* | *ipv4-address* [*mask-length*] } **next-hop-local**

In BGP IPv6 unicast address family view/BGP-VPN IPv6 unicast address family view:

peer { *group-name* | *ipv6-address* [*prefix-length*] } **next-hop-local**

undo peer { *group-name* | *ipv6-address* [*prefix-length*] } **next-hop-local**

Default

BGP sets the local router as the next hop for all routes sent to an EBGP peer or peer group.

It does not set the local router as the next hop for EBGP routes sent to an IBGP peer or peer group for other address families.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP IPv6 unicast address family view

BGP-VPN IPv6 unicast address family view

BGP EVPN address family view

Predefined user roles

network-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command sets the local router as the next hop for routes sent to all dynamic peers in the subnet.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command sets the local router as the next hop for routes sent to all dynamic peers in the subnet.

Usage guidelines

By default, BGP does not set the local router as the next hop for EBGP routes sent to an IBGP peer or peer group. To ensure that an IBGP peer can find the next hop, you can use this command to specify the router as the next hop for routes sent to the IBGP peer.

Examples

In BGP IPv4 unicast address family view, specify the router as the next hop for routes sent to peer group **test**.

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default] address-family ipv4 unicast
[Switch-bgp-default-ipv4] peer test next-hop-local
```

5.1.64. peer password

Use **peer password** to enable MD5 authentication for a BGP peer or peer group.

Use **undo peer password** to remove MD5 authentication for a BGP peer or peer group.

Syntax

peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **password** { **cipher** | **simple** } *password*

undo peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **password**

Default

MD5 authentication is disabled.

Views

BGP instance view

BGP-VPN instance view

Predefined user roles

network-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command enables MD5 authentication for all dynamic peers in the subnet.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command enables MD5 authentication for all dynamic peers in the subnet.

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

password: Specifies the password. Its encrypted form is a case-sensitive string of 33 to 137 characters. Its plaintext form is a case-sensitive string of 1 to 80 characters.

Usage guidelines

You can enable MD5 authentication to enhance security using the following methods:

- Perform MD5 authentication when establishing TCP connections. Only the two parties that have the same password configured can establish TCP connections.
- Perform MD5 calculation on TCP segments to avoid modification to the encapsulated BGP packets.

Examples

In BGP instance view, perform MD5 authentication on the TCP connection between local router 10.1.100.1 and peer router 10.1.100.2. Set the authentication password to **aabbcc** in plaintext form.

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default] peer 10.1.100.2 password simple aabbcc
```

5.1.65. peer preferred-value

Use **peer preferred-value** to set a preferred value for routes received from a peer or peer group.

Use **undo peer preferred-value** to remove the configuration.

Syntax

In BGP IPv4 unicast address family view/BGP-VPN IPv4 unicast address family view:

peer { *group-name* | *ipv4-address* [*mask-length*] } **preferred-value** *value*

undo peer { *group-name* | *ipv4-address* [*mask-length*] } **preferred-value**

In BGP IPv6 unicast address family view:

peer { *group-name* | *ipv6-address* [*prefix-length*] } **preferred-value** *value*

undo peer { *group-name* | *ipv6-address* [*prefix-length*] } **preferred-value**

In BGP-VPN IPv6 unicast address family view:

peer { *group-name* | *ipv6-address* [*prefix-length*] } **preferred-value** *value*

undo peer { *group-name* | *ipv6-address* [*prefix-length*] } **preferred-value**

Default

The preferred value is 0 for routes received from a peer or peer group.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP IPv6 unicast address family view

BGP-VPN IPv6 unicast address family view

Predefined user roles

network-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command specifies a preferred value for routes received from all dynamic peers in the subnet.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command specifies a preferred value for routes received from all dynamic peers in the subnet.

value: Specifies a preferred value in the range of 0 to 65535.

Usage guidelines

If multiple routes that have the same destination are learned from different peers, you can specify different preferred values for the routes as needed to control BGP path selection. The one with the greatest preferred value is selected as the optimal route to the destination.

The preferred value is used for route selection on the local router and is not advertised to the peer. It has only local significance.

You can also use the **apply preferred-value** command in a routing policy to configure the preferred value for BGP routes. If both the **peer preferred-value** and **apply preferred-value** commands are configured, the **apply preferred-value** command applies. If the preferred value is not set in the routing policy or no routing policy is configured, the **peer preferred-value** command applies.

Examples

In BGP IPv4 unicast address family view, set the preferred value to 50 for routes from peer 1.1.1.1.

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default] address-family ipv4 unicast
[Switch-bgp-default-ipv4] peer 1.1.1.1 preferred-value 50
```

Related commands

apply preferred-value

route-policy

5.1.66. peer prefix-list

Use **peer prefix-list** to specify a prefix list to filter routes received from or advertised to a peer or peer group.

Use **undo peer prefix-list** to remove the prefix list specified to filter routes received from or advertised to a peer or peer group.

Syntax

In BGP IPv4 unicast address family view/BGP-VPN IPv4 unicast address family view:

peer { *group-name* | *ipv4-address* [*mask-length*] } **prefix-list** *prefix-list-name* { **export** | **import** }

undo peer { *group-name* | *ipv4-address* [*mask-length*] } **prefix-list** { **export** | **import** }

In BGP IPv6 unicast address family view:

peer { *group-name* | *ipv6-address* [*prefix-length*] } **prefix-list** *ipv6-prefix-name* { **export** | **import** }

undo peer { *group-name* | *ipv6-address* [*prefix-length*] } **prefix-list** { **export** | **import** }

In BGP-VPN IPv6 unicast address family view:

peer { *group-name* | *ipv6-address* [*prefix-length*] } **prefix-list** *ipv6-prefix-name* { **export** | **import** }

undo peer { *group-name* | *ipv6-address* [*prefix-length*] } **prefix-list** { **export** | **import** }

Default

No prefix list based filtering is configured.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP IPv6 unicast address family view

BGP-VPN IPv6 unicast address family view

Predefined user roles

network-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command uses a prefix list to filter routes received from or advertised to all dynamic peers in the subnet.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command uses a prefix list to filter routes received from or advertised to all dynamic peers in the subnet.

prefix-list-name: Specifies an IPv4 prefix list by its name, a case-sensitive string of 1 to 63 characters.

ipv6-prefix-name: Specifies an IPv6 prefix list by its name, a case-sensitive string of 1 to 63 characters.

export: Applies the filter to routes advertised to the specified peer/peer group.

import: Applies the filter to routes received from the specified peer/peer group.

Usage guidelines

The specified prefix list must have been created with the **ip prefix-list** or **ipv6 prefix-list** command in system view. If you specify a nonexistent IPv4/IPv6 prefix list, all routes can pass the prefix list.

Examples

In BGP IPv4 unicast address family view, use IPv4 prefix list **list1** to filter routes advertised to peer group **test**.

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default] address-family ipv4 unicast
[Switch-bgp-default-ipv4] peer test prefix-list list1 export
```

Related commands

filter-policy export

filter-policy import

ip prefix-list

ipv6 prefix-list

peer as-path-acl

peer filter-policy

peer route-policy

5.1.67. peer public-as-only

Use **peer public-as-only** to remove private AS numbers in BGP updates sent to an EBGP peer or peer group.

Use **undo peer public-as-only** to remove the configuration.

Syntax

In BGP IPv4 unicast address family view/BGP-VPN IPv4 unicast address family view:

peer { *group-name* | *ipv4-address* [*mask-length*] } **public-as-only**

undo peer { *group-name* | *ipv4-address* [*mask-length*] } **public-as-only**

In BGP IPv6 unicast address family view:

peer { *group-name* | *ipv6-address* [*prefix-length*] } **public-as-only**

undo peer { *group-name* | *ipv6-address* [*prefix-length*] } **public-as-only**

In BGP-VPN IPv6 unicast address family view:

peer { *group-name* | *ipv6-address* [*prefix-length*] } **public-as-only**

undo peer { *group-name* | *ipv6-address* [*prefix-length*] } **public-as-only**

Default

BGP updates sent to an EBGP peer or peer group can carry both public and private AS numbers.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP IPv6 unicast address family view

BGP-VPN IPv6 unicast address family view

Predefined user roles

network-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a

subnet, this command removes private AS numbers in BGP updates sent to all dynamic peers in the subnet.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command removes private AS numbers in BGP updates sent to all dynamic peers in the subnet.

Usage guidelines

Private AS numbers are typically used in test networks, and need not be transmitted in public networks. The range of private AS numbers is from 64512 to 65535.

After you execute the command, you can get the following results:

- If the AS_PATH attribute of a BGP update carries only private AS numbers, the device removes the AS numbers before sending the update to the EBGP peer or peer group.
- If the AS_PATH attribute carries both public and private AS numbers, the command does not take effect. The device sends the BGP update to the EBGP peer or peer group without removing the private AS numbers.
- If the AS_PATH attribute carries AS numbers of the peer or peer group, the command does not take effect. The device sends the BGP update to the peer or peer group without removing the private AS numbers.

This command is applicable only to EBGP peers and peer groups.

Examples

In BGP IPv4 unicast address family view, remove private AS numbers in BGP updates sent to EBGP peer group **test**.

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default] address-family ipv4 unicast
[Switch-bgp-default-ipv4] peer test public-as-only
```

5.1.68. peer reflect-client

Use **peer reflect-client** to configure the device as a route reflector and specify a peer or peer group as a client.

Use **undo peer reflect-client** to remove the configuration.

Syntax

In BGP IPv4 unicast address family view/BGP-VPN IPv4 unicast address family view/BGP EVPN address family view:

peer { *group-name* | *ipv4-address* [*mask-length*] } **reflect-client**

undo peer { *group-name* | *ipv4-address* [*mask-length*] } **reflect-client**

In BGP IPv6 unicast address family view:

peer { *group-name* | *ipv6-address* [*prefix-length*] } **reflect-client**

undo peer { *group-name* | *ipv6-address* [*prefix-length*] } **reflect-client**

In BGP-VPN IPv6 unicast address family view:

peer { *group-name* | *ipv6-address* [*prefix-length*] } **reflect-client**

undo peer { *group-name* | *ipv6-address* [*prefix-length*] } **reflect-client**

Default

Neither the route reflector nor the client is configured.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP IPv6 unicast address family view

BGP-VPN IPv6 unicast address family view

BGP EVPN address family view

Predefined user roles

network-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command configures the device as a route reflector and specifies all dynamic peers in the subnet as clients.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command configures the device as a route reflector and specifies all dynamic peers in the subnet as clients.

Usage guidelines

Using route reflectors can solve the issue brought by too many IBGP connections. In an AS, a router acts as a route reflector, and other routers act as clients connecting to the route reflector. The route reflector forwards the routing information received from a client to other clients. In this

way, all clients can receive routing information from one another without establishing BGP sessions.

Examples

In BGP IPv4 unicast address family view, configure the local device as a route reflector and specify IBGP peer group **test** as a client.

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default] address-family ipv4 unicast
[Switch-bgp-default-ipv4] peer test reflect-client
```

Related commands

reflect between-clients

reflector cluster-id

5.1.69. peer route-limit

Use **peer route-limit** to set the maximum number of routes that can be received from a peer or peer group.

Use **undo peer route-limit** to remove the configuration.

Syntax

In BGP IPv4 unicast address family view/BGP-VPN IPv4 unicast address family view:

peer { *group-name* | *ipv4-address* [*mask-length*] } **route-limit** *prefix-number* [{ **alert-only** | **discard** | **reconnect** *reconnect-time* } | *percentage-value*] *

undo peer { *group-name* | *ipv4-address* [*mask-length*] } **route-limit**

In BGP IPv6 unicast address family view:

peer { *group-name* | *ipv6-address* [*prefix-length*] } **route-limit** *prefix-number* [{ **alert-only** | **discard** | **reconnect** *reconnect-time* } | *percentage-value*] *

undo peer { *group-name* | *ipv6-address* [*prefix-length*] } **route-limit**

In BGP-VPN IPv6 unicast address family view:

peer { *group-name* | *ipv6-address* [*prefix-length*] } **route-limit** *prefix-number* [{ **alert-only** | **discard** | **reconnect** *reconnect-time* } | *percentage-value*] *

undo peer { *group-name* | *ipv6-address* [*prefix-length*] } **route-limit**

Default

The number of routes that can be received from a peer or peer group is not limited.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP IPv6 unicast address family view

BGP-VPN IPv6 unicast address family view

Predefined user roles

network-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command specifies the maximum number of routes that can be received from all dynamic peers in the subnet.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command specifies the maximum number of routes that can be received from all dynamic peers in the subnet.

prefix-number: Specifies the number of routes that can be received from the peer or peer group. The value range for this argument is 1 to 4294967295. The router will tear down the session to the peer or peer group if the following conditions exist:

- The **alert-only**, **discard**, and **reconnect** keywords are not specified.
- The number of routes received from the peer or peer group reaches the *prefix-number*.

The router will not attempt to re-establish the session to a dynamic BGP peer until the router receives a connection request from the peer. For other peers, you can use the **reset bgp** command to re-establish the sessions.

alert-only: If the number of routes received from the peer or peer group reaches the *prefix-number*, the router generates a log message instead of tearing down the session to the peer or peer group. The router can continue to receive routes from the peer or peer group.

discard: If the number of routes received from the peer or peer group reaches the *prefix-number*, the router retains the session to the peer or peer group. However, it discards excess routes and generates a log message. After the number of routes received from the peer or peer group falls below the *prefix-number*, the router can continue to receive routes from the peer or peer group. To restore the discarded routes, use the **refresh bgp import** command to request the peer or peer group to resend the routes.

reconnect *reconnect-time*: Specifies a reconnect time. After the specified time is reached, the router re-establishes a session to the peer or peer group when the number of routes received from the peer or peer group reaches the *prefix-number*. The value range for the *reconnect-time* argument is 1 to 65535 seconds. This option is not available for dynamic BGP peers.

percentage-value: Specifies the threshold value for the router to generate a log message (the router generates a log message when the ratio of the number of received routes to the *prefix-number* exceeds the percentage value). The value range of this argument is 1 to 100, and the default is 75.

Examples

In BGP IPv4 unicast address family view, set the maximum number of routes that can be received from peer 1.1.1.1 to 10000. Configure the router to tear down the session to the peer if the number is exceeded.

```
<Switch> system-view
[Switch] bgp 109
[Switch-bgp-default] address-family ipv4 unicast
[Switch-bgp-default-ipv4] peer 1.1.1.1 route-limit 10000
```

5.1.70. peer route-policy

Use **peer route-policy** to apply a routing policy to routes incoming from or outgoing to a peer or peer group.

Use **undo peer route-policy** to remove the configuration.

Syntax

In BGP IPv4 unicast address family view/BGP-VPN IPv4 unicast address family view/BGP EVPN address family view:

peer { *group-name* | *ipv4-address* [*mask-length*] } **route-policy** *route-policy-name* { **export** | **import** }

undo peer { *group-name* | *ipv4-address* [*mask-length*] } **route-policy** { **export** | **import** }

In BGP IPv6 unicast address family view:

peer { *group-name* | *ipv6-address* [*prefix-length*] } **route-policy** *route-policy-name* { **export** | **import** }

undo peer { *group-name* | *ipv6-address* [*prefix-length*] } **route-policy** { **export** | **import** }

In BGP-VPN IPv6 unicast address family view:

peer { *group-name* | *ipv6-address* [*prefix-length*] } **route-policy** *route-policy-name* { **export** | **import** }

undo peer { *group-name* | *ipv6-address* [*prefix-length*] } **route-policy** { **export** | **import** }

Default

No routing policy is applied to routes incoming from or outgoing to a peer or peer group.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP IPv6 unicast address family view

BGP-VPN IPv6 unicast address family view

BGP EVPN address family view

Predefined user roles

network-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command applies a routing policy to routes incoming from or outgoing to all dynamic peers in the subnet.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command applies a routing policy to routes incoming from or outgoing to all dynamic peers in the subnet.

route-policy-name: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters.

export: Applies the routing policy to routes outgoing to the peer or peer group.

import: Applies the routing policy to routes incoming from the peer or peer group.

Usage guidelines

The specified routing policy must have been configured with the **route-policy** command in system view. If you specify a nonexistent routing policy, all routes can pass the routing policy.

The **if-match interface** command, if configured for the applied routing policy, does not take effect on routes.

Examples

In BGP IPv4 unicast address family view, apply routing policy **test-policy** to routes outgoing to peer group **test**.

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default] address-family ipv4 unicast
[Switch-bgp-default-ipv4] peer test route-policy test-policy export
```

Related commands

filter-policy export

filter-policy import

peer as-path-acl

peer filter-policy

peer prefix-list

route-policy

5.1.71. peer route-update-interval

Use **peer route-update-interval** to specify an interval for sending the same update to a peer or peer group.

Use **undo peer route-update-interval** to remove the configuration.

Syntax

peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **route-update-interval** *interval*

undo peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **route-update-interval**

Default

The interval for sending the same update to an IBGP peer is 15 seconds and the interval for sending the same update to an EBGP peer is 30 seconds.

Views

BGP instance view

BGP-VPN instance view

Predefined user roles

network-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command specifies an interval for sending the same update to all dynamic peers in the subnet.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command specifies an interval for sending the same update to all dynamic peers in the subnet.

interval: Specifies a minimum interval for sending the same update message, in the range of 0 to 600 seconds.

Usage guidelines

A BGP router sends an update message to its peers when a route is changed. If the route changes frequently, the BGP router sends many updates for the route, resulting in routing flaps. By configuring the interval for sending the same update to a peer or peer group, you can avoid such routing flaps.

This command does not apply to withdrawn route updates. BGP sends withdrawal messages immediately for withdrawn routes.

Examples

In BGP instance view, set the interval for sending the same update to peer group **test** to 10 seconds.

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default] peer test as-number 100
[Switch-bgp-default] peer test route-update-interval 10
```

5.1.72. peer source-address

Use **peer source-address** to specify a source IPv4 or IPv6 address for establishing TCP connections to a peer or peer group.

Use **undo peer source-address** to remove the configuration.

Syntax

peer *ipv4-address* [*mask-length*] **source-address** *source-ipv4-address*

peer *ipv6-address* [*prefix-length*] **source-address** *source-ipv6-address*

undo peer { *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **source-address**

peer *group-name* **source-address** { *source-ipv4-address* | *source-ipv6-address* } *

undo peer *group-name* **source-address** [*source-ipv4-address* | *source-ipv6-address*]

Default

BGP uses the primary IPv4 or IPv6 address of the output interface in the optimal route destined for the BGP peer or peer group as the source address for TCP connection establishment.

Views

BGP instance view

BGP-VPN instance view

Predefined user roles

network-admin

Parameters

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command specifies a source IP address for establishing TCP connections to all dynamic peers in the subnet.

source-ipv4-address: Specifies a source IPv4 address.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command specifies a source IPv6 address for establishing TCP connections to all dynamic peers in the subnet.

source-ipv6-address: Specifies a source IPv6 address.

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

Usage guidelines

The **peer connect-interface** command and the **peer source-address** command can both change the source address for establishing TCP connections. If you execute both commands, the most recent configuration takes effect.

The **peer source-address** and **peer connect-interface** commands are applicable to the following scenarios:

- The peer's IPv4/IPv6 address does not belong to the interface directly connected to the local router. To ensure successful TCP connection establishment, use one of the following methods:

- Specify the interface to which the IPv4/IPv6 address belongs as the source interface on the peer.
- Specify the IPv4/IPv6 address of the interface directly connected to the local router as the source address on the peer.

- A BGP peer at an IPv6 link-local address must be directly connected to the local router. On the local router, you must use the **peer connect-interface** command to specify the interface directly connected to the BGP peer as the source interface of TCP connections.
- On a BGP router that has multiple links to a peer, the source interface for TCP connection changes because the primary source interface fails. To avoid this problem, specify a loopback interface as the source interface or specify the IP address of a loopback interface as the source address.
- You want to establish multiple BGP sessions to a router. In this case, BGP might fail to determine the source address for each TCP connection based on the optimal route to the peer. To prevent this problem, use one of the following methods:
  - If the BGP sessions use IP addresses of different interfaces, specify a source interface or source address for each session.
  - If the BGP sessions use different IP addresses of the same interface, specify a source address for each session.

The source addresses on the local router and the peer must be reachable to each other.

To specify the address of an indirectly connected interface as the source address, use the **peer ebgp-max-hop** command. The command allows the establishment of an EBGP session to the indirectly connected peer.

You can specify both a source IPv4 address and a source IPv6 address for a peer group. BGP uses the source IPv4 address to establish TCP connections to IPv4 peers in the group. It also uses the source IPv6 address to establish TCP connections to IPv6 peers in the group.

Examples

In BGP instance view, specify source IPv4 address 1.1.1.1 for peer group **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] peer test source-address 1.1.1.1
```

Related commands

peer connect-interface

peer ebgp-max-hop

5.1.73. peer substitute-as

Use **peer substitute-as** to replace the AS number of a peer or peer group in the AS_PATH attribute with the local AS number.

Use **undo peer substitute-as** to remove the configuration.

Syntax

peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **substitute-as**

undo peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **substitute-as**

Default

The AS number of a peer or peer group in the AS_PATH attribute is not replaced.

Views

BGP instance view

BGP-VPN instance view

Predefined user roles

network-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command replaces the AS number of all dynamic peers in the subnet in the AS_PATH attribute with the local AS number.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command replaces the AS number of all dynamic peers in the subnet in the AS_PATH attribute with the local AS number.

Usage guidelines

If different CEs use the same AS number, you must configure the relevant PE to replace the AS number of the CE as its own AS number. This ensures correct advertisement of private network routes.

Examples

In BGP instance view, substitute the local AS number for the AS number of peer 1.1.1.1.

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default] peer 1.1.1.1 substitute-as
```

5.1.74. peer timer

Use **peer timer** to set a keepalive interval and hold time for a peer or peer group.

Use **undo peer timer** to remove the configuration.

Syntax

peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **timer keepalive** *keepalive* **hold** *holdtime*

undo peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **timer**

Default

The keepalive interval is 60 seconds, and the hold time is 180 seconds.

Views

BGP instance view

BGP-VPN instance view

Predefined user roles

network-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command configures a keepalive interval and hold time for all dynamic peers in the subnet.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command configures a keepalive interval and hold time for all dynamic peers in the subnet.

keepalive *keepalive*: Sets a keepalive interval in the range of 0 to 21845 seconds.

hold *holdtime*: Sets a hold time in the range of 3 to 65535 seconds. The hold time must be at least three times the keepalive interval.

Usage guidelines

After establishing a BGP session, two routers send keepalive messages at the specified keepalive interval to each other to keep the session.

If a router receives no keepalive or update message from the peer within the hold time, it tears down the session.

The timers configured with this command are preferred to the timers configured with the **timer** command.

If the hold time settings on the local and peer routers are different, the smaller one is used.

If the hold time is set to 0, no keepalive message will be sent to the peer, and the peer session will never time out. If neither the hold time nor the keepalive interval is set to 0, the actual keepalive interval is the smaller one between one third of the hold time and the keepalive interval.

The timers configured with this command do not take effect until a session is re-established (for example, a session is reset).

Examples

In BGP instance view, set the keepalive interval and hold time for peer group **test** to 60 seconds and 180 seconds, respectively.

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default] peer test timer keepalive 60 hold 180
```

Related commands

display bgp peer

timer

5.1.75. preference

Use **preference** to configure preferences for BGP routes.

Use **undo preference** to restore the default.

Syntax

preference { *external-preference internal-preference local-preference* | **route-policy** *route-policy-name* }

undo preference

Default

The preferences of external, internal, and local BGP routes are 255, 255, and 130, respectively.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP IPv6 unicast address family view

BGP-VPN IPv6 unicast address family view

Predefined user roles

network-admin

Parameters

external-preference: Specifies a preference for EBGP routes, in the range of 1 to 255.

internal-preference: Specifies a preference for IBGP routes, in the range of 1 to 255.

local-preference: Specifies a preference for local routes, in the range of 1 to 255.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters, to set the route preference for matching routes. Routes not matching the routing policy use the default preference.

Usage guidelines

Different routing protocols might find different routes to the same destination. However, not all of those routes are optimal. For route selection, routing protocols, direct routes, and static routes are assigned different preferences. The route with the highest preference is preferred.

Configuring the preferences for BGP routes changes the possibility for the routes to become the optimal route.

To use a routing policy to set the preference, you must configure the preference with the **apply preference** command in the routing policy in advance. Otherwise, all matching routes use the default preference.

Examples

In BGP IPv4 unicast address family view, set preferences for EBGP, IBGP, and local routes to 20, 20, and 200, respectively.

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default] address-family ipv4 unicast
[Switch-bgp-default-ipv4] preference 20 20 200
```

5.1.76. reflect between-clients

Use **reflect between-clients** to enable route reflection between clients.

Use **undo reflect between-clients** to disable route reflection between clients.

Syntax

reflect between-clients

undo reflect between-clients

Default

Route reflection between clients is enabled.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP IPv6 unicast address family view

BGP-VPN IPv6 unicast address family view

BGP EVPN address family view

Predefined user roles

network-admin

Usage guidelines

When a route reflector is configured, and the clients of a route reflector are fully meshed, route reflection is unnecessary because it consumes more bandwidth resources. You can use the **undo reflect between-clients** command to disable route reflection instead of modifying network configuration or changing network topology.

After route reflection is disabled between clients, routes can still be reflected between a client and a non-client.

Examples

In BGP IPv4 unicast address family view, disable route reflection between clients.

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default] address-family ipv4 unicast
[Switch-bgp-default-ipv4] undo reflect between-clients
```

Related commands

peer reflect-client

reflector cluster-id

5.1.77. reflector cluster-id

Use **reflector cluster-id** to configure the cluster ID for a route reflector.

Use **undo reflector cluster-id** to restore the default.

Syntax

reflector cluster-id { *cluster-id* | *ipv4-address* }

undo reflector cluster-id

Default

A route reflector uses its router ID as the cluster ID.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP IPv6 unicast address family view

BGP-VPN IPv6 unicast address family view

BGP EVPN address family view

Predefined user roles

network-admin

Parameters

cluster-id: Specifies the cluster ID in the format of an integer, in the range of 1 to 4294967295.

ipv4-address: Specifies the cluster ID in the format of an IPv4 address in dotted decimal notation.

Usage guidelines

The route reflector and clients form a cluster. Typically a cluster has one route reflector. The ID of the route reflector is the cluster ID.

You can configure more than one route reflector in a cluster to improve network reliability and prevent a single point of failure. Use this command to configure the same cluster ID for all route reflectors in the cluster to avoid routing loops.

Do not configure the router ID of a client as the cluster ID.

Examples

In BGP IPv4 unicast address family view, set the cluster ID on the local router (a reflector in the cluster) to 80.

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default] address-family ipv4 unicast
[Switch-bgp-default-ipv4] reflector cluster-id 80
```

Related commands

peer reflect-client

reflect between-clients

5.1.78. refresh bgp

Use **refresh bgp** to manually soft-reset BGP sessions.

Syntax

refresh bgp { *ipv4-address* [*mask-length*] | **all** | **external** | **group** *group-name* | **internal** } { **export** | **import** } **ipv4** [**unicast**] [**vpn-instance** *vpn-instance-name*]

refresh bgp { *ipv6-address* [*prefix-length*] | **all** | **external** | **group** *group-name* | **internal** } { **export** | **import** } **ipv6** [**unicast**] [**vpn-instance** *vpn-instance-name*]

refresh bgp *ipv4-address* [*mask-length*] { **export** | **import** } **ipv6** [**unicast**]

refresh bgp { *ipv4-address* [*mask-length*] | **all** | **external** | **group** *group-name* | **internal** } { **export** | **import** } **l2vpn evpn**

Views

User view

Predefined user roles

network-admin

Parameters

ipv4-address: Soft-resets the BGP session to a peer specified by its IP address.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command soft-resets BGP sessions to all dynamic peers in the subnet.

ipv6-address: Soft-resets the BGP session to a peer specified by its IPv6 address.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command soft-resets BGP sessions to all dynamic peers in the subnet.

all: Soft-resets all BGP sessions.

external: Soft-resets all EBGP sessions.

group *group-name*: Soft-resets the BGP sessions to the peers of the specified peer group. The *group-name* argument refers to the name of a peer group, a case-sensitive string of 1 to 47 characters.

internal: Soft-resets all IBGP sessions.

export: Performs outbound soft-reset (filters routes advertised to the specified peer or peer group by using the new configuration).

import: Performs inbound soft-reset (filters routes received from the specified peer or peer group by using the new configuration).

ipv4: Soft-resets BGP sessions for IPv4 address family.

ipv6: Soft-resets BGP sessions for IPv6 address family.

unicast: Soft-resets BGP sessions for unicast address family.

evpn: Soft-resets BGP sessions for EVPN address family.

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command soft-resets BGP sessions for the specified address family on the public network.

Usage guidelines

A soft-reset operation enables the router to apply a new route selection policy without tearing down BGP connections.

To apply a new policy to outbound BGP sessions, execute this command with the **export** keyword. The router uses the new policy to filter routing information and sends the routing information that passes the filtering to the BGP peers.

To apply a new policy to inbound sessions, execute this command with the **import** keyword. The router advertises a route-refresh message to the peer and the peer resends its routing information to the router. After receiving the routing information, the router uses the new policy to filter the routing information.

This command requires that both the local router and the peer support route refresh.

If the **peer keep-all-routes** command is configured, the **refresh bgp import** command does not take effect.

Examples

Soft-reset all inbound BGP sessions for the IPv4 unicast address family.

```
<Switch> refresh bgp all import ipv4
```

Related commands

peer capability-advertise route-refresh

peer keep-all-routes

5.1.79. reset bgp

Use **reset bgp** to reset BGP sessions for the specified address family.

Syntax

reset bgp { *as-number* | *ipv4-address* [*mask-length*] | **all** | **external** | **group** *group-name* | **internal** } **ipv4** [**unicast**] [**vpn-instance** *vpn-instance-name*]

reset bgp { *as-number* | *ipv6-address* [*prefix-length*] | **all** | **external** | **group** *group-name* | **internal** } **ipv6** [**unicast**] [**vpn-instance** *vpn-instance-name*]

reset bgp *ipv4-address* [*mask-length*] **ipv6** [**unicast**]

reset bgp { *as-number* | *ipv4-address* [*mask-length*] | **all** | **external** | **group** *group-name* | **internal** } **l2vpn evpn**

Views

User view

Predefined user roles

network-admin

Parameters

as-number: Resets BGP sessions to peers in the AS specified by its number in the range of 1 to 4294967295.

ipv4-address: Resets the BGP session to a peer specified by its IPv4 address.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command resets BGP sessions to all dynamic peers in the subnet.

ipv6-address: Resets the BGP session to a peer specified by its IPv6 address.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command resets BGP sessions to all dynamic peers in the subnet.

all: Resets all BGP sessions.

external: Resets all EBGP sessions.

group *group-name*: Resets the BGP sessions to the peers in the peer group specified by its name, a case-sensitive string of 1 to 47 characters.

internal: Resets all IBGP sessions.

ipv4: Resets BGP sessions for IPv4 address family.

ipv6: Resets BGP sessions for IPv6 address family.

unicast: Resets BGP sessions for unicast address family.

evpn: Resets BGP sessions for EVPN address family.

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command resets BGP sessions for the specified address family on the public network.

Usage guidelines

A reset operation enables the router to apply a new route selection policy by re-establishing BGP sessions. This operation breaks down BGP sessions for a short period of time.

Examples

Reset all BGP sessions for the IPv4 unicast address family.

```
<Switch> reset bgp all ipv4
```

5.1.80. reset bgp all

Use **reset bgp all** to reset all BGP sessions for all address families.

Syntax

reset bgp all

Views

User view

Predefined user roles

network-admin

Usage guidelines

A reset operation enables the router to apply a new route selection policy by re-establishing BGP sessions. This operation breaks down BGP sessions for a short while.

Examples

Reset all BGP sessions.

```
<Switch> reset bgp all
```

5.1.81. reset bgp dampening

Use **reset bgp dampening** to clear BGP route dampening information and release suppressed BGP routes.

Syntax

reset bgp dampening ipv4 [**unicast**] [**vpn-instance** *vpn-instance-name*] [*ipv4-address* [*mask-length* | *mask*]]

reset bgp dampening ipv6 [**unicast**] [**vpn-instance** *vpn-instance-name*] [*ipv6-address prefix-length*]

Views

User view

Predefined user roles

network-admin

Parameters

ipv4: Clears BGP IPv4 route dampening information and release suppressed BGP IPv4 routes.

ipv6: Clears BGP IPv6 route dampening information and release suppressed BGP IPv6 routes.

unicast: Clears BGP unicast route dampening information and release suppressed BGP unicast routes.

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command clears BGP route dampening information for the public network, and releases suppressed BGP routes.

ipv4-address: Specifies an IPv4 destination network address. If you do not specify a network address, this command clears all BGP route dampening information, and releases all suppressed BGP routes.

mask-length: Specifies a mask length in the range of 0 to 32.

mask: Specifies a network mask in dotted decimal notation.

ipv6-address: Specifies an IPv6 destination network address. If you do not specify a network address, this command clears all BGP route dampening information, and releases all suppressed BGP routes.

prefix-length: Specifies a prefix length in the range of 0 to 128.

Usage guidelines

When you execute the **reset bgp dampening ipv4** command:

- If you specify only the *ipv4-address* argument, the system ANDs the network address with the mask of a route. If the result matches the network address of the route, the command clears dampening information for the route, and releases the suppressed route.
- If you specify the *ipv4-address mask* or *ipv4-address mask-length* argument, this command does the following:
  - Clears dampening information for the route that matches both the specified destination network address and the mask (or mask length).
  - Releases the suppressed route.

Examples

Clear dampening information for the BGP IPv4 unicast route to network 20.1.0.0/16 and release the suppressed route.

```
<Switch> reset bgp dampening ipv4 20.1.0.0 255.255.0.0
```

Related commands

dampening

display bgp routing-table dampened

5.1.82. reset bgp flap-info

Use **reset bgp flap-info** to clear flap statistics for BGP routes.

Syntax

reset bgp flap-info ipv4 [**unicast**] [**vpn-instance** *vpn-instance-name*] [*ipv4-address* [*mask-length* | *mask*] | **as-path-acl** *as-path-acl-number* | **peer** *ipv4-address*]

reset bgp flap-info ipv6 [**unicast**] [**vpn-instance** *vpn-instance-name*] [*ipv6-address prefix-length* | **as-path-acl** *as-path-acl-number* | **peer** *ipv6-address*]

Views

User view

Predefined user roles

network-admin

Parameters

ipv4: Clears flap statistics for BGP IPv4 routes.

ipv6: Clears flap statistics for BGP IPv6 routes.

unicast: Clears flap statistics for BGP unicast routes.

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command clears flap statistics for public BGP routes.

ipv4-address: Specifies an IPv4 destination network address.

mask-length: Specifies a mask length in the range of 0 to 32.

mask: Specifies a network mask in dotted decimal notation.

ipv6-address: Specifies an IPv6 destination network address.

prefix-length: Specifies a prefix length in the range of 0 to 128.

as-path-acl *as-path-acl-number*: Specifies an AS path list by its number in the range of 1 to 256, to filter BGP route flap statistics.

peer *ipv4-address* [*mask-length*]: Clears flap statistics for BGP routes learned from the specified IPv4 BGP peer. The *mask-length* argument specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command clears flap statistics for BGP routes learned from all dynamic peers in the subnet.

peer *ipv6-address*: Clears flap statistics for BGP routes learned from the specified IPv6 BGP peer. The *prefix-length* argument specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* arguments together to specify a subnet. If you specify a subnet, this command clears flap statistics for BGP routes learned from all dynamic peers in the subnet.

Usage guidelines

When you execute the **reset bgp flap-info ipv4** command:

- If you specify only the *ipv4-address* argument, the system ANDs the IPv4 network address with the mask of a route. If the result matches the IPv4 network address of the route, this command clears the flap statistics of the route.
- If you specify the *ipv4-address mask* or *ipv4-address mask-length* argument, this command clears the flap statistics of the route that matches both the specified IPv4 destination network address and the mask (or mask length).

Examples

Clear flap statistics for the BGP IPv4 unicast route to network 20.1.0.0/16.

```
<Switch> reset bgp flap-info ipv4 20.1.0.0 16
```

Related commands

dampening

display bgp routing-table flap-info

5.1.83. router id

Use **router id** to configure a global router ID.

Use **undo router id** to restore the default.

Syntax

router id *router-id*

undo router id

Default

No global router ID is configured.

Views

System view

Predefined user roles

network-admin

Parameters

router-id: Specifies a router ID in IP address format.

Usage guidelines

Some routing protocols use a router ID to identify a device. You can configure a global router ID, which is used by routing protocols that have no router ID configured.

If no global router ID is configured, the highest loopback address, if any, is used as the router ID. If no loopback address is available, the highest physical interface IP address is used, regardless of the interface status. If no IP address is configured for any interface, the router ID is 0.0.0.0.

During an active/standby switchover, the standby main processing unit (MPU) checks the validity of the previous router ID backed up before switchover. If it is not valid, it selects a new router ID.

If the interface IP address that is selected as the router ID is removed or modified, a new router ID is selected. The following events will not trigger a router ID re-selection:

- The interface goes down.
- After a physical interface address is selected as the router ID, an IP address is configured for a loopback interface.
- A higher interface IP address is configured.

After a router ID is changed, use the **reset** command to make it effective.

Examples

Configure a global router ID as 1.1.1.1.

```
<Switch> system-view
[Switch] router id 1.1.1.1
```

Related commands

router-id (BGP instance view)

router-id (BGP-VPN instance view)

5.1.84. router-id (BGP instance view)

Use **router-id** to configure a router ID for a BGP instance.

Use **undo router-id** to restore the default.

Syntax

router-id *router-id*

undo router-id

Default

No router ID is configured for a BGP instance, and the BGP instance uses the global router ID configured by the **router id** command in system view.

Views

BGP instance view

Predefined user roles

network-admin

Parameters

router-id: Specifies a router ID for BGP, in IP address format.

Usage guidelines

To run BGP, a BGP instance must have a router ID, which is an unsigned 32-bit integer that uniquely identifies the router in the AS.

To modify a non-zero router ID for BGP, execute the **router-id** command in BGP instance view.

To improve availability, specify the IP address of a loopback interface as the router ID for BGP.

If you execute this command in the same BGP instance view multiple times, the most recent configuration takes effect.

You can configure the same router ID for different BGP instances.

Examples

In BGP instance view, set the router ID for BGP to 1.1.1.1.

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default] router-id 1.1.1.1
```

Related commands

router id

router-id (BGP-VPN instance view)

5.1.85. router-id (BGP-VPN instance view)

Use **router-id** to configure a router ID for a BGP VPN instance.

Use **undo router-id** to restore the default.

Syntax

router-id { *router-id* | **auto-select** }

undo router-id

Default

No router ID is configured for a BGP VPN instance, and the BGP VPN instance uses the router ID configured in BGP instance view. If no router ID is configured in BGP instance view, the BGP VPN instance uses the global router ID configured in system view.

Views

BGP-VPN instance view

Predefined user roles

network-admin

Parameters

router-id: Specifies a router ID in IP address format.

auto-select: Automatically selects a router ID for the BGP VPN instance.

Usage guidelines

To run BGP, a VPN instance of a BGP instance must have a router ID, which is an unsigned 32-bit integer that uniquely identifies the BGP VPN router in the AS.

If the **auto-select** keyword is specified, the system selects a router ID for the BGP VPN instance in the following order:

1. The highest loopback address in the BGP VPN instance as the router ID.
2. The highest physical interface address in the BGP VPN instance as the router ID, regardless of the interface status.
3. 0.0.0.0 as the router ID.

If a non-zero router ID is selected for the BGP VPN instance, the router ID will not change when a more preferable router ID is available in the BGP VPN instance.

To improve availability, specify the IP address of a loopback interface as the router ID.

You can specify a different router ID for each VPN instance on a device.

If you execute this command in the same BGP-VPN instance view multiple times, the most recent configuration takes effect.

Examples

In BGP-VPN instance view, set the router ID to 1.1.1.1.

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default] ip vpn-instance vpn1
[Switch-bgp-default-vpn1] router-id 1.1.1.1
```

Related commands

router id

router-id (BGP instance view)

5.1.86. snmp-agent trap enable bgp

Use **snmp-agent trap enable bgp** to enable SNMP notifications for BGP.

Use **undo snmp-agent trap enable bgp** to disable SNMP notifications for BGP.

Syntax

snmp-agent trap enable bgp

undo snmp-agent trap enable bgp

Default

SNMP notifications for BGP are enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

After you enable SNMP notifications for BGP, the device generates a notification when a BGP neighbor state change occurs. The notification includes the neighbor address, the error code and subcode of the most recent error, and the current neighbor state.

For BGP notifications to be sent correctly, you must also configure SNMP on the device. For more information about SNMP configuration, see the network management and monitoring configuration guide for the device.

Examples

Enable SNMP notifications for BGP.

```
<Switch> system-view
[Switch] snmp-agent trap enable bgp
```

5.1.87. summary automatic

Use **summary automatic** to configure automatic route summarization for redistributed IGP subnet routes.

Use **undo summary automatic** to restore the default.

Syntax

summary automatic

undo summary automatic

Default

Automatic route summarization is not performed for redistributed IGP subnet routes.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

Predefined user roles

network-admin

Usage guidelines

After the **summary automatic** command is configured, BGP summarizes IGP subnets redistributed by the **import-route** command.

Automatic summary routes can be manually summarized, but cannot be added to the IP routing table.

Examples

In BGP IPv4 unicast address family view, configure automatic route summarization for redistributed IGP subnet routes.

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default] address-family ipv4 unicast
[Switch-bgp-default-ipv4] summary automatic
```

Related commands

aggregate

import-route

5.1.88. timer

Use **timer** to configure a BGP keepalive interval and hold time.

Use **undo timer** to restore the default.

Syntax

timer keepalive *keepalive* **hold** *holdtime*

undo timer

Default

The BGP keepalive interval and the hold time are 60 seconds and 180 seconds, respectively.

Views

BGP instance view

BGP-VPN instance view

Predefined user roles

network-admin

Parameters

keepalive *keepalive*: Configures a keepalive interval in the range of 0 to 21845 seconds.

hold *holdtime*: Configures a hold time in seconds, whose value is 0 or in the range of 3 to 65535. The hold time must be at least three times the keepalive interval.

Usage guidelines

After establishing a BGP session, two routers send keepalive messages at the specified keepalive interval to each other to keep the session.

If a router receives no keepalive or update message from the peer within the hold time, it tears down the session.

Use the **timer** command to configure the keepalive interval and hold time for all BGP peers. Use the **peer timer** command to configure the keepalive interval and hold time for a peer or peer

group. If both commands are configured, the intervals configured by the **peer timer** command have higher priority.

If the hold time settings on the local and peer routers are different, the smaller one is used.

If the hold time is set to 0, no keepalive message will be sent to the peer, and the peer session will never time out. If neither the hold time nor the keepalive interval is set to 0, the actual keepalive interval is the smaller one between one third of the hold time and the keepalive interval.

The **timer** command affects only new BGP sessions.

After the **timer** command is executed, no peer session is closed at once. The configured hold time is used for negotiation in session re-establishment (for example, when you reset the BGP session).

Examples

In BGP instance view, set the keepalive interval and hold time to 60 seconds and 180 seconds, respectively.

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default] timer keepalive 60 hold 180
```

Related commands

display bgp peer

peer timer

Contents

A page of this section is **5-x-x**

6. Policy-based routing commands 6-1
6.1. Policy-based routing commands 6-1
6.1.1. apply next-hop 6-1
6.1.2. display ip policy-based-route 6-2
6.1.3. display ip policy-based-route interface 6-3
6.1.4. display ip policy-based-route setup 6-4
6.1.5. if-match acl 6-5
6.1.6. ip local policy-based-route 6-6
6.1.7. ip policy-based-route 6-7
6.1.8. policy-based-route 6-8
6.1.9. reset ip policy-based-route statistics 6-9

6. Policy-based routing commands

6.1. Policy-based routing commands

6.1.1. apply next-hop

Use **apply next-hop** to set next hops.

Use **undo apply next-hop** to remove next hops.

Syntax

apply next-hop [**vpn-instance** *vpn-instance-name*] { *ip-address* [**direct**] [**track** *track-entry-number*] }&<1-2>

undo apply next-hop [[**vpn-instance** *vpn-instance-name*] *ip-address*&<1-2>]

Default

No next hop is set.

Views

Policy node view

Predefined user roles

network-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. The specified VPN instance must already exist.

ip-address: Specifies the IP address of the next hop. If you do not specify the **vpn-instance** *vpn-instance-name* option, the next hop belongs to the public network.

direct: Specifies that the next hop must be directly connected to take effect.

track *track-entry-number*: Specifies a track entry by its number in the range of 1 to 1024.

&<1-2>: Indicates that the argument before it can be entered up to two times.

Usage guidelines

You can specify multiple next hops for backup in one command line or by executing this command multiple times.

With a next hop specified, the **undo apply next-hop** command removes the next hop.

Without any next hop specified, the **undo apply next-hop** command removes all next hops.

Examples

Set a directly-connected next hop of 1.1.1.1.

```
<Switch> system-view
[Switch] policy-based-route aa permit node 11
[Switch-pbr-aa-11] apply next-hop 1.1.1.1 direct
```

6.1.2. display ip policy-based-route

Use **display ip policy-based-route** to display PBR policy information.

Syntax

display ip policy-based-route [**policy** *policy-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

policy *policy-name*: Specifies a policy by its name, a case-sensitive string of 1 to 19 characters. If you do not specify a policy, this command displays information for all PBR policies.

Examples

Display all policy information.

```
<Switch> display ip policy-based-route
Policy name: aaa
  node 1 permit:
    if-match acl 2000
    apply next-hop 1.1.1.1
```

Table 6-1 Command output

Field	Description
node 1 permit	The match mode of Node 1 is **permit**.
if-match acl	Compares packets with the ACL.
apply next-hop	Specifies a next hop for permitted packets.

Related commands

policy-based-route

6.1.3. display ip policy-based-route interface

Use **display ip policy-based-route interface** to display interface PBR configuration and statistics.

Syntax

display ip policy-based-route interface *interface-type interface-number* [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number: Specifies an interface by its type and number.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information on the master device.

Examples

Display PBR configuration and statistics on VLAN-interface 2.

```
<Switch> display ip policy-based-route interface vlan-interface 2
Policy based routing information for interface Vlan-interface2:
Policy name: aaa
  node 0 deny:
  Matched: 0
  node 1 permit:
    if-match acl 3999
  Matched: 0
  node 2 permit:
    if-match acl 2000
    apply next-hop 2.2.2.2
  Matched: 0
  node 5 permit:
    if-match acl 3101
    apply next-hop 1.1.1.1
  Matched: 0
Total matched: 0
<Switch> display ip policy-based-route interface vlan-interface 2
Policy based routing information for interface Vlan-interface2:
Policy name: aaa
  node 0 deny:
  Matched: 0
  node 1 permit:
```

```
    if-match acl 3999
  Matched: 0
  node 2 permit:
    if-match acl 2000
    apply next-hop 2.2.2.2
  Matched: 0
  node 5 permit:
    if-match acl 3101
    apply next-hop 1.1.1.1
  Matched: 0
Total matched: 0
```

Table 6-2 Command output

Field	Description
Policy based routing information for interface *XXXX*(failed)	PBR configuration and statistics on the interface. **NOTE:** If you specify a slot number, this field displays **failed** in brackets for a policy that failed to be issued to the driver. The failure means that all node configurations in the PBR policy failed to be issued.
node 0 deny(not support) node 2 permit(no resource)	Match mode of the node, **permit** or **deny**. **NOTE:** If you specify a slot number, this field displays the cause in brackets for a node that does not take effect: • **not support**—The device does not support the match criteria configured on the node. • **no resource**—The node does not have sufficient resources (for example, ACLs).
if-match acl	Compares packets with the ACL.
apply next-hop	Specifies a next hop for permitted packets.
Matched: 0 (no statistics resource)	Number of successful matches on the node. **NOTE:** If you specify a slot number but the device does not have sufficient resources to collect statistics on the slot, this field displays **no statistics resource** in brackets.
Total matched	Total number of successful matches on all nodes.

Related commands

reset ip policy-based-route statistics

6.1.4. display ip policy-based-route setup

Use **display ip policy-based-route setup** to display PBR configuration.

Syntax

display ip policy-based-route setup

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display PBR configuration.

```
<Switch> display ip policy-based-route setup
Policy name              Type     Interface
pr01                     Forward  Vlan-interface2
aaa                      Local    N/A
```

Table 6-3 Command output

Field	Description
Type	Type of the PBR: • **Forward**—Interface PBR. • **Local**—Local PBR.
Interface	Interface where the policy is applied.

Related commands

ip policy-based-route

6.1.5. if-match acl

Use **if-match acl** to set an ACL match criterion.

Use **undo if-match acl** to restore the default.

Syntax

if-match acl { *acl-number* | **name** *acl-name* }

undo if-match acl

Default

No ACL match criterion is set.

Views

Policy node view

Predefined user roles

network-admin

Parameters

acl-number: Specifies an ACL by its number in the range of 2000 to 2999 for a basic ACL, and in the range of 3000 to 3999 for an advanced ACL.

name *acl-name*: Specifies an ACL by its name, a case-insensitive string of 1 to 63 characters starting with letter *a* to *z* or *A* to *Z*. The ACL name cannot be **all**. For the command to take effect, make sure the specified ACL is a basic or advanced ACL.

Examples

Configure Node 11 of policy **aa** to permit the packets matching ACL 2011.

```
<Switch> system-view
[Switch] policy-based-route aa permit node 11
[Switch-pbr-aa-11] if-match acl 2011
```

Configure Node 11 of policy **aa** to permit the packets matching ACL **aaa**.

```
<Switch> system-view
[Switch] policy-based-route aa permit node 11
[Switch-pbr-aa-11] if-match acl name aaa
```

6.1.6. ip local policy-based-route

Use **ip local policy-based-route** to specify a policy for local PBR.

Use **undo ip local policy-based-route** to restore the default.

Syntax

ip local policy-based-route *policy-name*

undo ip local policy-based-route

Default

No policy is referenced for local PBR.

Views

System view

Predefined user roles

network-admin

Parameters

policy-name: Specifies a policy by its name, a case-sensitive string of 1 to 19 characters. The specified policy must already exist.

Usage guidelines

Local PBR guides the forwarding of locally generated packets, such as ICMP packets generated by using the **ping** command.

Local PBR might affect local services, such as ping and Telnet. When you use local PBR, make sure you fully understand its impact on local services of the device.

You can specify only one policy for local PBR and must make sure the specified policy already exists.

Before you apply a new policy, you must first remove the current policy.

Examples

Configure local PBR based on policy **aaa**.

```
<Switch> system-view
[Switch] ip local policy-based-route aaa
```

Related commands

display ip policy-based-route setup

policy-based-route

6.1.7. ip policy-based-route

Use **ip policy-based-route** to specify a policy for interface PBR on an interface.

Use **undo ip policy-based-route** to restore the default.

Syntax

ip policy-based-route *policy-name*

undo ip policy-based-route

Default

No policy is applied to an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

policy-name: Specifies a policy by its name, a case-sensitive string of 1 to 19 characters. The specified policy must already exist.

Examples

Apply policy **aaa** to VLAN-interface 2.

```
<Switch> system-view
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip policy-based-route aaa
```

Related commands

display ip policy-based-route setup

policy-based-route

6.1.8. policy-based-route

Use **policy-based-route** to create a policy node and enter its view, or enter the view of an existing policy node.

Use **undo policy-based-route** to delete a policy or policy node.

Syntax

policy-based-route *policy-name* [**deny** | **permit**] **node** *node-number*

undo policy-based-route *policy-name* [**deny** | **node** *node-number* | **permit**]

Default

No policy nodes exist.

Views

System view

Predefined user roles

network-admin

Parameters

policy-name: Specifies a policy by its name, a case-sensitive string of 1 to 19 characters.

deny: Specifies the match mode for the policy node as **deny**.

permit: Specifies the match mode for the policy node as **permit** (default mode).

node *node-number*: Specifies a policy node by its number in the range of 0 to 255. A smaller number has a higher priority.

Usage guidelines

A policy that has been applied to an interface or locally cannot be deleted. To delete it, you must first cancel the application.

- If a policy node is specified, the **undo policy-based-route** command deletes the specified policy node.
- If a match mode is specified, the command deletes all nodes configured with the match mode.
- If no policy node or match mode is specified, the command deletes the whole policy.

Examples

Create permit-mode of Node 10 for policy **policy1** and enter its view.

```
<Switch> system-view
[Switch] policy-based-route policy1 permit node 10
[Switch-pbr-policy1-10]
```

Related commands

display ip policy-based-route

6.1.9. reset ip policy-based-route statistics

Use **reset ip policy-based-route statistics** to clear PBR statistics.

Syntax

reset ip policy-based-route statistics [**policy** *policy-name*]

Views

User view

Predefined user roles

network-admin

Parameters

policy *policy-name*: Specifies a policy by its name, a case-sensitive string of 1 to 19 characters. If you do not specify a policy, this command clears PBR statistics for all policies.

Examples

Clear all PBR statistics.

```
<Switch> reset ip policy-based-route statistics
```

Related commands

display ip policy-based-route interface

Contents

A page of this section is **5-x-x**

7. IPv6 static routing commands 7-1
7.1. IPv6 static routing commands 7-1
7.1.1. delete ipv6 static-routes all 7-1
7.1.2. ipv6 route-static 7-1
7.1.3. ipv6 route-static default-preference 7-4

7. IPv6 static routing commands

7.1. IPv6 static routing commands

7.1.1. delete ipv6 static-routes all

Use **delete ipv6 static-routes all** to delete all IPv6 static routes.

Syntax

delete ipv6 [**vpn-instance** *vpn-instance-name*] **static-routes all**

Views

System view

Predefined user roles

network-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command deletes all IPv6 static routes for the public network.

Usage guidelines

When you use this command, the system will prompt you to confirm the operation before deleting all the IPv6 static routes.

Examples

Delete all IPv6 static routes.

```
<Switch> system-view
[Switch] delete ipv6 static-routes all
This will erase all IPv6 static routes and their configurations, you must reconfigure
all static routes.
Are you sure?[Y/N]:y
```

Related commands

ipv6 route-static

7.1.2. ipv6 route-static

Use **ipv6 route-static** to configure an IPv6 static route.

Use **undo ipv6 route-static** to remove an IPv6 static route.

Syntax

ipv6 route-static *ipv6-address prefix-length* { *interface-type interface-number* [*next-hop-address*] [**bfd** { **control-packet** | **echo-packet** } | **permanent**] | [**vpn-instance** *d-vpn-instance-name*] *next-hop-address* [**bfd control-packet bfd-source** *ip-address* | **permanent**] } [**preference** *preference*] [**tag** *tag-value*] [**description** *text*]

undo ipv6 route-static *ipv6-address prefix-length* [*interface-type interface-number* [*next-hop-address*] | [**vpn-instance** *d-vpn-instance-name*] *next-hop-address*] [**preference** *preference*]

ipv6 route-static vpn-instance *s-vpn-instance-name ipv6-address prefix-length* { *interface-type interface-number* [*next-hop-address*] [**bfd** { **control-packet** | **echo-packet** } | **permanent**] | *next-hop-address* [**public**] [**bfd control-packet bfd-source** *ip-address* | **permanent**] | **vpn-instance** *d-vpn-instance-name next-hop-address* [**bfd control-packet bfd-source** *ipv6-address* | **permanent**] } [**preference** *preference*] [**tag** *tag-value*] [**description** *text*]

undo ipv6 route-static vpn-instance *s-vpn-instance-name ipv6-address prefix-length* [*interface-type interface-number* [*next-hop-address*] | *next-hop-address* [**public**] | **vpn-instance** *d-vpn-instance-name next-hop-address*] [**preference** *preference*]

Default

No IPv6 static route is configured.

Views

System view

Predefined user roles

network-admin

Parameters

ipv6-address prefix-length: Specifies the IPv6 address and prefix length.

interface-type interface-number: Specifies an output interface by its type and number. If the output interface is an NBMA interface or broadcast interface and not a point-to-point (P2P) interface, the next hop address must be specified.

next-hop-address: Specifies the next hop IPv6 address.

bfd: Enables BFD to detect reachability of the static route's next hop.

control-packet: Specifies the BFD control mode.

bfd-source *ip-address*: Specifies the source IPv6 address of BFD packets.

echo-packet: Specifies the BFD echo mode.

permanent: Specifies the IPv6 route as a permanent IPv6 static route. If the output interface is down, the permanent IPv6 static route is still active.

public: Indicates the next hop is on the public network.

vpn-instance *d-vpn-instance-name*: Specifies a destination VPN instance by its name, a case-sensitive string of 1 to 31 characters. If a destination VPN is specified, packets will search for the output interface based on the specified next hop (IPv6 address) for the static route.

preference *preference*: Specifies a preference for IPv6 static routes, in the range of 1 to 255. The default is 60.

tag *tag-value*: Sets a tag for marking the static route, in the range of 1 to 4294967295. The default is 0. Tags of routes are used for route control in routing policies. For more information about routing policies, see *Layer 3—IP Routing Configuration Guide*.

description *text*: Configures a description for the IPv6 static route, which consists of 1 to 60 characters, including special characters such as the space, but excluding the question mark (?).

vpn-instance *s-vpn-instance-name*: Specifies a source VPN instance by its name, a case-sensitive string of 1 to 31 characters. Each VPN has its own routing table, and the configured static route is installed in the routing tables of the specified VPNs.

Usage guidelines

An IPv6 static route that has the destination address configured as **::/0** (a prefix length of 0) is the default IPv6 route. If the destination address of an IPv6 packet does not match any entry in the routing table, this default route is used to forward the packet.

Follow these guidelines to configure the output interface, next hop address, or both for a static route:

- If the output interface is a broadcast interface or an NBMA interface, the next hop address must be specified.
- If the output interface is a P2P interface, you can specify only the output interface. You do not need to change the configuration of the route even if the peer address is changed.

Follow these guidelines when you configure BFD for IPv6 static routes:

- If you specify the source IPv6 address of BFD packets, you must specify the IPv6 address as the next hop IPv6 address on the peer device.

Follow these guidelines when you configure a static route:

- Enabling BFD for a flapping route could worsen the route flapping situation. Therefore, use it with caution. For more information about BFD, see *High Availability Configuration Guide*.
- The next hop IPv6 address of echo packets must be a global unicast address.
- Do not specify the **permanent** keyword together with the **bfd** keyword.

Examples

Configure an IPv6 static route, with the destination address 1:1:2::/64 and next hop 1:1:3::1.

```
<Switch> system-view
[Switch] ipv6 route-static 1:1:2:: 64 1:1:3::1
```

Related commands

display ipv6 routing-table protocol

7.1.3. ipv6 route-static default-preference

Use **ipv6 route-static default-preference** to set a default preference for IPv6 static routes.

Use **undo ipv6 route-static default-preference** to restore the default.

Syntax

ipv6 route-static default-preference *default-preference*

undo ipv6 route-static default-preference

Default

The default preference of IPv6 static routes is 60.

Views

System view

Predefined user roles

network-admin

Parameters

default-preference: Specifies a default preference for IPv6 static routes, in the range of 1 to 255.

Usage guidelines

If no preference is specified for an IPv6 static route, the default preference applies.

When the default preference is reconfigured, it applies only to newly added IPv6 static routes.

Examples

Set a default preference of 120 for IPv6 static routes.

```
<Switch> system-view
[Switch] ipv6 route-static default-preference 120
```

Related commands

display ipv6 routing-table protocol

Contents

A page of this section is **5-x-x**

8. RIPng commands 8-1
8.1. RIPng commands 8-1
8.1.1. checkzero 8-1
8.1.2. default cost 8-1
8.1.3. display ripng 8-2
8.1.4. display ripng database 8-4
8.1.5. display ripng interface 8-4
8.1.6. display ripng route 8-6
8.1.7. filter-policy export 8-8
8.1.8. filter-policy import 8-9
8.1.9. graceful-restart 8-10
8.1.10. import-route 8-11
8.1.11. maximum load-balancing 8-12
8.1.12. non-stop-routing 8-13
8.1.13. preference 8-14
8.1.14. reset ripng process 8-15
8.1.15. reset ripng statistics 8-15
8.1.16. ripng 8-16
8.1.17. ripng default-route 8-17
8.1.18. ripng enable 8-17
8.1.19. ripng metricin 8-18
8.1.20. ripng metricout 8-19
8.1.21. ripng poison-reverse 8-19
8.1.22. ripng split-horizon 8-20
8.1.23. ripng summary-address 8-20
8.1.24. timers 8-21

8. RIPng commands

8.1. RIPng commands

8.1.1. checkzero

Use **checkzero** to enable zero field check on RIPng packets.

Use **undo checkzero** to disable zero field check.

Syntax

checkzero

undo checkzero

Default

Zero field check is enabled.

Views

RIPng view

Predefined user roles

network-admin

Usage guidelines

Some fields in RIPng packet headers must be zero. These fields are called zero fields. You can enable zero field check on incoming RIPng packets. If a zero field of a packet contains a non-zero value, RIPng discards the packet.

Examples

Disable zero field check on RIPng packets for RIPng 100.

```
<Switch> system-view
[Switch] ripng 100
[Switch-ripng-100] undo checkzero
```

8.1.2. default cost

Use **default cost** to configure a default metric for redistributed routes.

Use **undo default cost** to restore the default.

Syntax

default cost *cost-value*

undo default cost

Default

The default metric of redistributed routes is 0.

Views

RIPng view

Predefined user roles

network-admin

Parameters

cost-value: Specifies a default metric for redistributed routes, in the range of 0 to 16.

Usage guidelines

When you use the **import-route** command to redistribute routes from another routing protocol without specifying a metric, the metric specified by the **default cost** command applies.

Examples

Configure a default metric of 2 for redistributed routes.

```
<Switch> system-view
[Switch] ripng 100
[Switch-ripng-100] default cost 2
```

Related commands

import-route

8.1.3. display ripng

Use **display ripng** to display state and configuration information for a RIPng process.

Syntax

display ripng [*process-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies a RIPng process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays information about all RIPng processes.

Examples

Display state and configuration information for all configured RIPng processes.

```
<Switch> display ripng
  Public VPN-instance name:
```

```
RIPng process: 1
       Preference: 100
           Routing policy: abc
       Fast-reroute:
           Routing policy: abc
       Checkzero: Enabled
       Default cost: 0
       Maximum number of load balanced routes: 6
       Update time   :   30 secs  Timeout time         :  180 secs
       Suppress time :  120 secs  Garbage-collect time :  120 secs
       Update output delay:   20(ms)  Output count:    3
       Graceful-restart interval:   60 secs
       Triggered Interval : 5 50 200
       Number of periodic updates sent: 256
       Number of trigger updates sent: 1
```

Table 8-1 Command output

Field	Description
Public VPN-instance name	Public network where the RIPng process runs.
Private VPN-instance name	VPN where the RIPng process runs.
RIPng process	RIPng process ID.
Preference	RIPng preference.
Checkzero	Indicates whether zero field check for RIPng packet headers is enabled: **Enabled** or **Disabled**.
Default Cost	Default metric of redistributed routes.
Fast-reroute	RIPng FRR.
Maximum number of balanced paths	Maximum number of load-balanced routes.
Update time	RIPng update interval, in seconds.
Timeout time	RIPng timeout interval, in seconds.
Suppress time	RIPng suppress interval, in seconds.
Garbage-Collect time	RIPng garbage collection interval, in seconds.
Update output delay	RIPng packet sending interval, in milliseconds.
Output count	Maximum number of RIPng packets that can be sent at an interval.
Graceful-restart interval	GR interval in seconds.
Triggered Interval	Triggered update sending interval.

8.1.4. display ripng database

Use **display ripng database** to display all active routes in the advertising database for a RIPng process.

Syntax

display ripng *process-id* **database** [*ipv6-address prefix-length*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies a RIPng process by its ID in the range of 1 to 65535.

ipv6-address prefix-length: Specifies an IPv6 address. The *ipv6-address* argument specifies an IPv6 address. The *prefix-length* argument specifies a prefix length in the range of 0 to 128.

Examples

Display active routes for RIPng process 1.

```
<Switch> display ripng 1 database
   1::/64,
        cost 0, RIPng-interface
   10::/32,
        cost 0, imported
   2::2/128,
       via FE80::20C:29FF:FE7A:E3E4, cost 1
```

Table 8-2 Command output

Field	Description
cost	Route metric value.
imported	Indicates the route is redistributed from another routing protocol.
RIPng-interface	Route learned from the interface.
via	Next hop IPv6 address.

8.1.5. display ripng interface

Use **display ripng interface** to display interface information for a RIPng process.

Syntax

display ripng *process-id* **interface** [*interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies a RIPng process by its ID in the range of 1 to 65535.

interface-type interface-number: Specifies an interface by its type and number. If you do not specify this argument, the command displays information about all interfaces for the RIPng process.

Examples

Display interface information for RIPng process 1.

```
<Switch> display ripng 1 interface
Total: 1

 Interface: Vlan-interface100
         Link-local address: FE80::20C:29FF:FEC8:B4DD
         Split-horizon: On                Poison-reverse: Off
         MetricIn: 0                      MetricOut: 1
         Default route: Off
         Primary path detection mode: BFD echo
         Summary address:
                1::/16
```

Table 8-3 Command output

Field	Description
Total	Number of interfaces running RIPng.
Interface	Name of an interface running RIPng.
Link Local Address	Link-local address of an interface running RIPng.
Split-horizon	Indicates whether split horizon is enabled: • **On**—Enabled. • **Off**—Disabled.
Poison-reverse	Indicates whether poison reverse is enabled: • **On**—Enabled. • **Off**—Disabled.
MetricIn/MetricOut	Additional metric to incoming and outgoing routes.
Default route	• **Only**—The interface advertises only a default route. • **Originate**—The interface advertises a default

Field	Description
	route and other RIPng routes. • **Off**—In this state, the interface does not advertise a default route. • **In garbage-collection status**—In this state, the interface advertises a default route with a metric of 16.
Default route cost	Cost of the default route.
Primary path detection mode	**BFD echo** indicates that BFD single-hop echo detection is used to detect primary link failures.

8.1.6. display ripng route

Use **display ripng route** to display all RIPng routes for a RIPng process.

Syntax

display ripng *process-id* **route** [*ipv6-address prefix-length* [**verbose**] | **peer** *ipv6-address* | **statistics**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies a RIPng process by its ID in the range of 1 to 65535.

ipv6-address prefix-length: Specifies an IPv6 address. The *ipv6-address* argument specifies an IPv6 address. The *prefix-length* argument specifies a prefix length in the range of 0 to 128.

verbose: Displays all routing information for the specified destination IPv6 address. If you do not specify this keyword, the command displays only optimal RIPng routes with the specified destination IPv6 address.

peer *ipv6-address*: Specifies a neighbor by its IPv6 address.

statistics: Displays routing information statistics, including total number of routes and the number of routes learned from each neighbor.

Examples

Display routing information for RIPng process 1.

```
<Switch> display ripng 1 route
   Route Flags: A - Aging, S - Suppressed, G - Garbage-collect, D - Direct
                O - Optimal, F - Flush to RIB
 ----------------------------------------------------------------
```

```
Peer FE80::20C:29FF:FED4:7171 on Vlan-interface100
Destination 4::4/128,
    via FE80::20C:29FF:FED4:7171, cost 1, tag 0, AOF, 5 secs
Local route
Destination 3::3/128,
    via ::, cost 0, tag 0, DOF
Destination 6::/64,
    via ::, cost 0, tag 0, DOF
```

Display information about routes with the specified prefix for RIPng process 1.

```
<Switch> display ripng 1 route 3::3 128 verbose
   Route Flags: A - Aging, S - Suppressed, G - Garbage-collect, D – Direct
                O - Optimal, F - Flush to RIB
 ----------------------------------------------------------------
 Peer FE80::4283:59FF:FE97:205 on Vlan-interface100
 Destination 3::3/128,
     via FE80::4283:59FF:FE97:205, cost 1, tag 0, AOF, 28 secs
```

Table 8-4 Command output

Field	Description
A–Aging	The route is in aging state.
S–Suppressed	The route is in suppressed state.
G–Garbage-collect	The route is in Garbage-collect state.
D–Direct	The route is a direct route.
Local route	The route is a locally generated direct route.
O - Optimal	The route is an optimal route.
F - Flush to RIB	The route has been flushed to the RIB.
Peer	Neighbor connected to the interface.
Destination	IPv6 destination address.
via	Next hop IPv6 address.
cost	Routing metric value.
tag	Route tag.
secs	Time a route entry has stayed in the current state.

Display routing information statistics for RIPng process 1.

```
<Switch> display ripng 1 route statistics
Peer                                    Optimal/Aging    Garbage
 FE80::20C:29FF:FED4:7171                1/2              0
 Local                                   2/0              0
 total                                   3/2              0
```

Table 8-5 Command output

Field	Description
Peer	IPv6 address of the neighbor.
Optimal	Number of optimal routes.
Aging	Number of routes in aging state.
Garbage	Number of routes in Garbage-collection state.
Local	Total number of locally generated direct route.
total	Total number of routes learned from RIPng neighbors.

8.1.7. filter-policy export

Use **filter-policy export** to configure RIPng to filter redistributed routes.

Use **undo filter-policy export** to remove the filtering.

Syntax

filter-policy { *ipv6-acl-number* | **prefix-list** *prefix-list-name* } **export** [*protocol* [*process-id*]]

undo filter-policy export [*protocol* [*process-id*]]

Default

RIPng does not filter redistributed routes.

Views

RIPng view

Predefined user roles

network-admin

Parameters

ipv6-acl-number: Specifies an IPv6 ACL by its number in the range of 2000 to 3999 to filter redistributed routes.

prefix-list *prefix-list-name*: Specifies an IPv6 prefix list by its name, a string of 1 to 63 characters, to filter redistributed routes.

protocol: Filters routes redistributed from a routing protocol.

process-id: Specifies the process ID of the specified routing protocol, in the range of 1 to 65535. This argument is available only when the routing protocol is **ripng**, or **ospfv3**. The default is 1.

Usage guidelines

If the *protocol* argument is specified, RIPng filters only routes redistributed from the specified routing protocol. Otherwise, RIPng filters all redistributed routes.

To use an advanced ACL (with a number from 3000 to 3999) in the command, configure the ACL in one of the following ways:

- To deny/permit a route with the specified destination, use the **rule** [*rule-id*] { **deny** | **permit** } **ipv6 source** *sour sour-prefix* command.
- To deny/permit a route with the specified destination and prefix, use the **rule** [*rule-id*] { **deny** | **permit** } **ipv6 source** *sour sour-prefix* **destination** *dest dest-prefix* command.

The **source** keyword specifies the destination address of a route and the **destination** keyword specifies the prefix of the route. For the prefix configuration to take effect, specify a contiguous prefix.

Examples

Use IPv6 prefix list to filter redistributed RIPng updates.

```
<Switch> system-view
[Switch] ipv6 prefix-list abc index 10 permit 100:1:: 32
[Switch] ripng 100
[Switch-ripng-100] filter-policy prefix-list abc export
```

Configure advanced IPv6 ACL 3000 to permit only route 2001::1/128 to pass. Use advanced IPv6 ACL 3000 to filter redistributed routes.

```
<Switch> system-view
[Switch] acl ipv6 advanced 3000
[Switch-acl-ipv6-adv-3000] rule 10 permit ipv6 source 2001::1 128 destination
ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff 128
[Switch-acl-ipv6-adv-3000] rule 100 deny ipv6
[Switch-acl-ipv6-adv-3000] quit
[Switch] ripng 100
[Switch-ripng-100] filter-policy 3000 export
```

8.1.8. filter-policy import

Use **filter-policy import** to configure RIPng to filter received routes.

Use **undo filter-policy import** to restore the default.

Syntax

filter-policy { *ipv6-acl-number* | **prefix-list** *prefix-list-name* } **import**

undo filter-policy import

Default

RIPng does not filter received routes.

Views

RIPng view

Predefined user roles

network-admin

Parameters

ipv6-acl-number: Specifies an IPv6 ACL by its number in the range of 2000 to 3999 to filter received routes.

prefix-list *prefix-list-name*: Specifies an IPv6 prefix list by its name, a string of 1 to 63 characters, to filter received routes.

Usage guidelines

To use an advanced ACL (with a number from 3000 to 3999) in the command, configure the ACL in one of the following ways:

- To deny/permit a route with the specified destination, use the **rule** [*rule-id*] { **deny** | **permit** } **ipv6 source** *sour sour-prefix* command.
- To deny/permit a route with the specified destination and prefix, use the **rule** [*rule-id*] { **deny** | **permit** } **ipv6 source** *sour sour-prefix* **destination** *dest dest-prefix* command.

The **source** keyword specifies the destination address of a route and the **destination** keyword specifies the prefix of the route. For the configuration to take effect, specify a contiguous prefix.

Examples

Use the IPv6 prefix list **abc** to filter received RIPng updates.

```
<Switch> system-view
[Switch] ipv6 prefix-list abc index 10 permit 100:1:: 32
[Switch] ripng 100
[Switch-ripng-100] filter-policy prefix-list abc import
```

Configure advanced IPv6 ACL 3000 to permit only route 2001::1/128 to pass. Use advanced IPv6 ACL 3000 to filter received routes.

```
<Switch> system-view
[Switch] acl ipv6 advanced 3000
[Switch-acl-ipv6-adv-3000] rule 10 permit ipv6 source 2001::1 128 destination
ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff 128
[Switch-acl-ipv6-adv-3000] rule 100 deny ipv6
[Switch-acl-ipv6-adv-3000] quit
[Switch] ripng 100
[Switch-ripng-100] filter-policy 3000 import
```

8.1.9. graceful-restart

Use **graceful-restart** to enable Graceful Restart (GR) for RIPng.

Use **undo graceful-restart** to disable RIPng GR.

Syntax

graceful-restart

undo graceful-restart

Default

RIPng GR is disabled.

Views

RIPng view

Predefined user roles

network-admin

Examples

Enable GR for RIPng process 1.

```
<Switch> system-view
[Switch] ripng 1
[Switch-ripng-1] graceful-restart
```

8.1.10. import-route

Use **import-route** to redistribute routes from another routing protocol.

Use **undo import-route** to remove routes redistributed from another routing protocol.

Syntax

import-route bgp4+ [*as-number*] [**allow-ibgp**] [**cost** *cost-value* | **route-policy** *route-policy-name*] *

undo import-route bgp4+

import-route { **direct** | **static** } [**cost** *cost-value* | **route-policy** *route-policy-name*] *

undo import-route { **direct** | **static** }

import-route { **ospfv3** | **ripng** } [*process-id*] [**cost** *cost-value* | **route-policy** *route-policy-name*] *

undo import-route { **ospfv3** | **ripng** } [*process-id*]

Default

RIPng does not redistribute routes from another routing protocol.

Views

RIPng view

Predefined user roles

network-admin

Parameters

bgp4+: Redistributes BGP4+ routes.

direct: Redistributes direct routes.

ospfv3: Redistributes OSPFv3 routes.

ripng: Redistributes RIPng routes.

static: Redistributes static routes.

as-number: Specifies an AS by its number in the range of 1 to 4294967295. If you do not specify the *as-number* argument, this command redistributes all IPv6 EBGP routes. As a best practice, specify the AS number to avoid redistributing excessive IPv6 EBGP routes.

process-id: Specifies an OSPFv3, or RIPng process by its ID in the range of 1 to 65535. The default is 1.

allow-ibgp: Allows redistribution of IBGP routes. The **import-route bgp4+** command redistributes only EBGP routes. The **import-route bgp4+ allow-ibgp** command additionally redistributes IBGP routes and might cause routing loops. Therefore, use it with caution.

cost *cost-value*: Specifies a metric for redistributed routes, in the range of 0 to 16. The default metric is 0.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters.

Usage guidelines

This command redistributes only active routes. To view route state information, use the **display ipv6 routing-table protocol** command.

Examples

Redistribute routes from OSPFv3 process 7 into RIPng and set the metric for redistributed routes to 7.

```
<Switch> system-view
[Switch] ripng 100
[Switch-ripng-100] import-route ospfv3 7 cost 7
```

8.1.11. maximum load-balancing

Use **maximum load-balancing** to set the maximum number of equal-cost multi-path (ECMP) routes for load balancing.

Use **undo maximum load-balancing** to restore the default.

Syntax

maximum load-balancing *number*

undo maximum load-balancing

Default

8

Views

RIPng view

Predefined user roles

network-admin

Parameters

number: Specifies the maximum number of ECMP routes in the range of 1 to 8. When this argument takes a value of 1, RIPng does not perform load balancing.

Examples

Set the maximum number of ECMP routes to 2.

```
<Switch> system-view
[Switch] ripng 100
[Switch-ripng-100] maximum load-balancing 2
```

Related commands

max-ecmp-num

8.1.12. non-stop-routing

> **MEMO:**
>
> **non-stop-routing** command is supported from later software, including Version 7.2.16.

Use **non-stop-routing** to enable RIPng NSR.

Use **undo non-stop-routing** to disable RIPng NSR.

Syntax

non-stop-routing

undo non-stop-routing

Default

RIPng NSR is disabled.

Views

RIPng view

Predefined user roles

network-admin

Usage guidelines

RIPng NSR enabled for a RIPng process takes effect only on that process. If multiple RIPng processes exist, enable RIPng NSR for each process as a best practice.

RIPng NSR and RIPng GR are mutually exclusive. Do not configure the **non-stop-routing** command and the **graceful-restart** command at the same time.

Examples

Enable NSR for RIPng process 1.

```
<Switch> system-view
[Switch] ripng 1
[Switch-ripng-1] non-stop-routing
```

8.1.13. preference

Use **preference** to set the preference for RIPng routes.

Use **undo preference** to restore the default.

Syntax

preference { *preference* | **route-policy** *route-policy-name* } *

undo preference

Default

The preference of RIPng routes is 100.

Views

RIPng view

Predefined user roles

network-admin

Parameters

preference: Specifies the preference for RIPng routes, in the range of 1 to 255. The smaller the value, the higher the preference.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters.

Usage guidelines

You can specify a routing policy to set a preference for the matching RIPng routes.

- The preference set by the routing policy applies to all matching RIPng routes. The preference of other routes is set by the **preference** command.
- If no preference is set by the routing policy, the preference of all RIPng routes is set by the **preference** command.

Examples

Set the preference for RIPng routes to 120.

```
<Switch> system-view
[Switch] ripng 100
[Switch-ripng-100] preference 120
```

8.1.14. reset ripng process

Use **reset ripng process** to restart a RIPng process.

Syntax

reset ripng *process-id* **process**

Views

User view

Predefined user roles

network-admin

Parameters

process-id: Specifies a RIPng process by its ID in the range of 1 to 65535.

Usage guidelines

After executing the command, you are prompted to confirm the operation.

Examples

Restart RIPng process 100.

```
<Switch> reset ripng 100 process
Reset RIPng process? [Y/N]:y
```

8.1.15. reset ripng statistics

Use **reset ripng statistics** to clear statistics for a RIPng process.

Syntax

reset ripng *process-id* **statistics**

Views

User view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies a RIPng process by its ID in the range of 1 to 65535.

Examples

Clear statistics for RIPng process 100.

```
<Switch> reset ripng 100 statistics
```

8.1.16. ripng

Use **ripng** to enable RIPng and enter RIPng view.

Use **undo ripng** to disable RIPng.

Syntax

ripng [*process-id*] [**vpn-instance** *vpn-instance-name*]

undo ripng [*process-id*]

Default

RIPng is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

process-id: Specifies a RIPng process by its ID in the range of 1 to 65535. The default value is 1.

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the RIPng process runs on the public network.

Usage guidelines

Before you configure global RIPng parameters, you must create a RIPng process. This restriction does not apply to configuring interface RIPng parameters.

If you disable a RIPng process, the configured RIPng parameters become invalid.

Examples

Create RIPng process 100 and enter its view.

```
<Switch> system-view
[Switch] ripng 100
[Switch-ripng-100]
```

8.1.17. ripng default-route

Use **ripng default-route** to configure a RIPng interface to advertise a default route with a specified metric.

Use **undo ripng default-route** to disable a RIPng interface from sending a default route.

Syntax

ripng default-route { **only** | **originate** } [**cost** *cost-value*] *

undo ripng default-route

Default

A RIPng process does not advertise a default route.

Views

Interface view

Predefined user roles

network-admin

Parameters

only: Advertises only an IPv6 default route (::/0).

originate: Advertises an IPv6 default route (::/0) and other routes.

cost-value: Specifies a cost for the default route, in the range of 1 to 15. The default is 1.

Usage guidelines

This command enables the interface to advertise a RIPng default route in a route update regardless of whether the default route exists in the local IPv6 routing table.

A RIPng interface configured to advertise a default route does not receive any default routes from its neighbors.

Examples

Configure RIPng on VLAN-interface 100 to advertise only a default route.

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ripng default-route only
```

Configure RIPng on VLAN-interface 101 to advertise a default route and other routes.

```
<Switch> system-view
[Switch] interface vlan-interface 101
[Switch-Vlan-interface101] ripng default-route originate
```

8.1.18. ripng enable

Use **ripng enable** to enable RIPng on an interface.

Use **undo ripng enable** to disable RIPng on an interface.

Syntax

ripng *process-id* **enable**

undo ripng enable

Default

RIPng is disabled on an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

process-id: Specifies a RIPng process by its ID in the range of 1 to 65535.

Examples

Enable RIPng 100 on VLAN-interface 100.

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ripng 100 enable
```

8.1.19. ripng metricin

Use **ripng metricin** to configure an interface to add a metric to inbound RIPng routes.

Use **undo ripng metricin** to restore the default.

Syntax

ripng metricin *value*

undo ripng metricin

Default

The additional metric of an inbound route is 0.

Views

Interface view

Predefined user roles

network-admin

Parameters

value: Adds an additional metric to inbound routes, in the range of 0 to 16.

Examples

Configure VLAN-interface 100 to add a metric of 12 to inbound RIPng routes.

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ripng metricin 12
```

8.1.20. ripng metricout

Use **ripng metricout** to configure an interface to add a metric to outbound RIPng routes.

Use **undo ripng metricout** to restore the default.

Syntax

ripng metricout *value*

undo ripng metricout

Default

The additional metric of outbound routes is 1.

Views

Interface view

Predefined user roles

network-admin

Parameters

value: Adds an additional metric to outbound routes, in the range of 1 to 16.

Examples

Configure RIPng on VLAN-interface 100 to add a metric of 12 to outbound routes.

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ripng metricout 12
```

8.1.21. ripng poison-reverse

Use **ripng poison-reverse** to enable poison reverse.

Use **undo ripng poison-reverse** to disable poison reverse.

Syntax

ripng poison-reverse

undo ripng poison-reverse

Default

Poison reverse is disabled.

Views

Interface view

Predefined user roles

network-admin

Examples

Enable poison reverse for RIPng update messages on VLAN-interface 100.

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ripng poison-reverse
```

8.1.22. ripng split-horizon

Use **ripng split-horizon** to enable split horizon.

Use **undo ripng split-horizon** to disable split horizon.

Syntax

ripng split-horizon

undo ripng split-horizon

Default

Split horizon is enabled.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

Split horizon prevents routing loops. If you want to disable this feature, make sure the operation is indispensable.

If both poison reverse and split horizon are enabled, only poison reverse takes effect.

Examples

Enable split horizon on VLAN-interface 100.

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ripng split-horizon
```

8.1.23. ripng summary-address

Use **ripng summary-address** to configure a summary network to be advertised through an interface.

Use **undo ripng summary-address** to remove a summary network.

Syntax

ripng summary-address *ipv6-address prefix-length*

undo ripng summary-address *ipv6-address prefix-length*

Default

No summary network is configured to be advertised through an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies the destination IPv6 address of the summary route.

prefix-length: Specifies the prefix length of the destination IPv6 address of the summary route, in the range of 0 to 128. It indicates the number of consecutive 1s of the prefix, which defines the network ID.

Usage guidelines

Networks on the summary network will not be advertised. The cost of the summary route is the lowest cost among summarized routes.

Examples

Assign an IPv6 address with the 64-bit prefix to VLAN-interface 100 and configure a summary with the 35-bit prefix.

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ipv6 address 2001:200::3EFF:FE11:6770/64
[Switch-Vlan-interface100] ripng summary-address 2001:200:: 35
```

8.1.24. timers

Use **timers** to set RIPng timers.

Use **undo timers** to restore the default.

Syntax

timers { **garbage-collect** *garbage-collect-value* | **suppress** *suppress-value* | **timeout** *timeout-value* | **update** *update-value* } *

undo timers { **garbage-collect** | **suppress** | **timeout** | **update** } *

Default

The garbage-collect timer is 120 seconds, the suppress timer is 120 seconds, the timeout timer is 180 seconds, and the update timer is 30 seconds.

Views

RIPng view

Predefines user roles

network-admin

Parameters

garbage-collect-value: Sets the garbage-collect timer in the range of 1 to 86400 seconds.

suppress-value: Sets the suppress timer in the range of 0 to 86400 seconds.

timeout-value: Sets the timeout timer in the range of 1 to 86400 seconds.

update-value: Sets the update timer in the range of 1 to 86400 seconds.

Usage guidelines

RIPng has the following timers:

- **Update timer**—Interval between update messages.
- **Timeout timer**—Route aging time. If no update for a route is received before the timer expires, RIPng sets the metric of the route to 16.
- **Suppress timer**—How long a RIPng route stays in suppressed state. When the metric of a route becomes 16, the route enters the suppressed state. If RIPng receives an update for the route from the same neighbor and the route in the update has a metric less than 16, RIPng uses the route to replace the suppressed route.
- **Garbage-collect timer**—Interval from when the metric of a route becomes 16 to when it is deleted from the routing table. During the garbage-collect timer length, RIPng advertises the route with a metric of 16. If no update is announced for that route before the garbage-collect timer expires, RIPng deletes the route from the routing table.

As a best practice, do not change the default values of these timers.

The timer lengths must be kept consistent on all routers in the network.

Examples

Set the update, timeout, suppress, and garbage-collect timers to 5 seconds, 15 seconds, 15 seconds, and 30 seconds.

```
<Switch> system-view
[Switch] ripng 1
[Switch-ripng-1] timers update 5 timeout 15 suppress 15 garbage-collect 30
```

Contents

A page of this section is **5-x-x**

9. OSPFv3 commands ····· 9-1
9.1. OSPFv3 commands ····· 9-1
9.1.1. abr-summary (OSPFv3 area view) ····· 9-1
9.1.2. area ····· 9-2
9.1.3. bandwidth-reference (OSPFv3 view) ····· 9-2
9.1.4. default-cost (OSPFv3 area view) ····· 9-3
9.1.5. default-route-advertise (OSPFv3 view) ····· 9-4
9.1.6. display ospfv3 ····· 9-5
9.1.7. display ospfv3 abr-asbr ····· 9-12
9.1.8. display ospfv3 abr-summary ····· 9-13
9.1.9. display ospfv3 asbr-summary ····· 9-15
9.1.10. display ospfv3 graceful-restart ····· 9-17
9.1.11. display ospfv3 interface ····· 9-21
9.1.12. display ospfv3 lsdb ····· 9-24
9.1.13. display ospfv3 nexthop ····· 9-28
9.1.14. display ospfv3 peer ····· 9-29
9.1.15. display ospfv3 request-queue ····· 9-33
9.1.16. display ospfv3 retrans-queue ····· 9-34
9.1.17. display ospfv3 routing ····· 9-35
9.1.18. display ospfv3 statistics ····· 9-37
9.1.19. display ospfv3 vlink ····· 9-39
9.1.20. filter (OSPFv3 area view) ····· 9-40
9.1.21. filter-policy export (OSPFv3 view) ····· 9-41
9.1.22. filter-policy import (OSPFv3 view) ····· 9-43
9.1.23. graceful-restart enable ····· 9-44
9.1.24. graceful-restart helper enable ····· 9-45
9.1.25. graceful-restart helper strict-lsa-checking ····· 9-46
9.1.26. graceful-restart interval ····· 9-47
9.1.27. import-route (OSPFv3 view) ····· 9-47
9.1.28. log-peer-change ····· 9-49
9.1.29. lsa-generation-interval ····· 9-50
9.1.30. maximum load-balancing (OSPFv3 view) ····· 9-51
9.1.31. non-stop-routing ····· 9-51
9.1.32. ospfv3 ····· 9-52
9.1.33. ospfv3 area ····· 9-53
9.1.34. ospfv3 bfd enable ····· 9-54
9.1.35. ospfv3 cost ····· 9-54
9.1.36. ospfv3 dr-priority ····· 9-55
9.1.37. ospfv3 mtu-ignore ····· 9-56
9.1.38. ospfv3 network-type ····· 9-57
9.1.39. ospfv3 peer ····· 9-58
9.1.40. ospfv3 timer dead ····· 9-59
9.1.41. ospfv3 timer hello ····· 9-59
9.1.42. ospfv3 timer poll ····· 9-60
9.1.43. ospfv3 timer retransmit ····· 9-61
9.1.44. ospfv3 trans-delay ····· 9-62
9.1.45. preference ····· 9-63
9.1.46. reset ospfv3 process ····· 9-64
9.1.47. reset ospfv3 redistribution ····· 9-64
9.1.48. reset ospfv3 statistics ····· 9-65
9.1.49. router-id ····· 9-65
9.1.50. silent-interface(OSPFv3 view) ····· 9-66

9.1.51. snmp-agent trap enable ospfv3 ····· 9-67
9.1.52. spf-schedule-interval ····· 9-68
9.1.53. stub (OSPFv3 area view) ····· 9-69
9.1.54. vlink-peer (OSPFv3 area view) ····· 9-70

9. OSPFv3 commands

9.1. OSPFv3 commands

9.1.1. abr-summary (OSPFv3 area view)

Use **abr-summary** to configure route summarization on an ABR.

Use **undo abr-summary** to remove the configuration.

Syntax

abr-summary *ipv6-address prefix-length* [**not-advertise**] [**cost** *cost-value*]

undo abr-summary *ipv6-address prefix-length*

Default

Route summarization is not configured on an ABR.

Views

OSPFv3 area view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies the destination IPv6 address of the summary route.

prefix-length: Specifies the prefix length of the destination IPv6 address, in the range of 0 to 128. This argument specifies the number of consecutive 1s of the prefix, which defines the network ID.

not-advertise: Specifies not to advertise the summary IPv6 route. If you do not specify this keyword, the command advertises the IPv6 summary route.

cost *cost-value*: Specifies the cost of the summary route, in the range of 1 to 16777215. The default cost is the largest cost value among routes that are summarized.

Usage guidelines

This command applies only to an ABR to summarize multiple contiguous networks into one network.

To enable ABR to advertise specific routes that have been summarized, use the **undo abr-summary** command.

Examples

Summarize networks 2000:1:1:1::/64 and 2000:1:1:2::/64 in Area 1 into 2000:1:1::/48.

```
<Switch> system-view
[Switch] ospfv3 1
[Switch-ospfv3-1] area 1
[Switch-ospfv3-1-area-0.0.0.1] abr-summary 2000:1:1:: 48
```

9.1.2. area

Use **area** to create an OSPFv3 area and enter OSPFv3 area view.

Use **undo area** to remove an OSPFv3 area.

Syntax

area *area-id*

undo area *area-id*

Default

No OSPFv3 areas exist.

Views

OSPFv3 view

Predefined user roles

network-admin

Parameters

area-id: Specifies an area by its ID, an IPv4 address or a decimal integer in the range of 0 to 4294967295 that is translated into the IPv4 address format.

Examples

Create OSPFv3 Area 0 and enter its view.

```
<Switch> system-view
[Switch] ospfv3 1
[Switch-ospfv3-1] area 0
[Switch-ospfv3-1-area-0.0.0.0]
```

9.1.3. bandwidth-reference (OSPFv3 view)

Use **bandwidth-reference** to set a reference bandwidth value for link cost calculation.

Use **undo bandwidth-reference** to restore the default.

Syntax

bandwidth-reference *value*

undo bandwidth-reference

Default

The reference bandwidth value is 100 Mbps for link cost calculation.

Views

OSPFv3 view

Predefined user roles

network-admin

Parameters

value: Specifies the reference bandwidth value for link cost calculation, in the range of 1 to 4294967 Mbps.

Usage guidelines

You can configure an OSPFv3 cost for an interface with one of the following methods:

- Configure the cost value in interface view.
- Configure a bandwidth reference value. OSPFv3 computes the cost automatically based on the bandwidth reference value by using the following formula: Interface OSPFv3 cost = Bandwidth reference value / Interface bandwidth.
  - If the calculated cost is greater than 65535, the value of 65535 is used.
  - If the calculated cost is smaller than 1, the value of 1 is used.

If no cost value is configured for an interface, OSPFv3 computes the interface cost value automatically.

Examples

Set the reference bandwidth value to 1000 Mbps.

```
<Switch> system-view
[Switch] ospfv3 1
[Switch-ospfv3-1] bandwidth-reference 1000
```

9.1.4. default-cost (OSPFv3 area view)

Use **default-cost** to set a cost for the default route advertised to the stub area or NSSA area.

Use **undo default-cost** to restore the default.

Syntax

default-cost *cost*

undo default-cost

Default

The cost is 1.

Views

OSPFv3 area view

Predefined user roles

network-admin

Parameters

value: Specifies a cost for the default route advertised to the stub area or NSSA area, in the range of 0 to 16777214.

Usage guidelines

This command takes effect only on the ABR of a stub area or the ABR or ASBR of an NSSA area.

Examples

Configure Area 1 as a stub area, and set the cost of the default route advertised to the stub area to 60.

```
<Switch> system-view
[Switch] ospfv3 1
[Switch-ospfv3-1] area 1
[Switch-ospfv3-1-area-0.0.0.1] stub
[Switch-ospfv3-1-area-0.0.0.1] default-cost 60
```

Related commands

stub (OSPFv3 area view)

9.1.5. default-route-advertise (OSPFv3 view)

Use **default-route-advertise** to redistribute a default route into the OSPFv3 routing domain.

Use **undo default-route-advertise** to restore the default.

Syntax

default-route-advertise [[**always** | **permit-calculate-other**] | **cost** *cost-value* | **route-policy** *route-policy-name* | **tag** *tag* | **type** *type*] *

undo default-route-advertise

Default

No default route is redistributed into the OSPFv3 routing domain.

Views

OSPFv3 view

Predefined user roles

network-admin

Parameters

always: Redistributes a default route in an AS-external-LSA into the OSPFv3 routing domain regardless of whether a default route exists in the routing table. If you do not specify this keyword, the router redistributes a default route in an AS-external-LSA into the OSPFv3 routing domain only when the default route exists in the routing table.

permit-calculate-other: Enables OSPFv3 to calculate default routes received from other routers. If you do not specify this keyword, OSPFv3 does not calculate default routes from other routers. If the router does not redistribute any default route in an AS-external-LSA into the OSPFv3 routing domain, the router calculates default routes from other routers. It calculates these routes regardless of whether this keyword is specified.

cost *cost-value*: Specifies a cost for the default route, in the range of 0 to 16777214. The default is 1.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters. When the routing policy is matched and one of the following conditions is met, the command redistributes a default route in an AS-external-LSA into the OSPFv3 routing domain:

- A default route exists in the routing table.
- The **always** keyword is specified.

The routing policy modifies values in the AS-external-LSA.

tag *tag*: Specifies a tag for the default route, in the range of 0 to 4294967295. If you do not specify this option, the tag specified to 1.

type *type*: Specifies a type for the AS-external-LSA, 1 or 2. The default is 2.

Usage guidelines

This command redistributes a default route in an AS-external-LSA, which cannot be redistributed with the **import-route** command. If the local routing table has no default route, you must provide the **always** keyword for the command.

Examples

Redistribute a default route into the OSPFv3 routing domain. (The default route does not exist in the local router.)

```
<Switch> system-view
[Switch] ospfv3 1
[Switch-ospfv3-1] default-route-advertise always
```

Related commands

import-route (OSPFv3 view)

9.1.6. display ospfv3

Use **display ospfv3** to display OSPFv3 process information.

Syntax

display ospfv3 [*process-id*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies an OSPFv3 process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays information about all OSPFv3 processes.

verbose: Displays detailed OSPFv3 process information. If you do not specify this keyword, the command displays brief OSPFv3 process information.

Examples

Display detailed information about all OSPFv3 processes.

```
<Switch> display ospfv3 verbose

              OSPFv3 Process 1 with Router ID 1.1.1.1

 RouterID: 1.1.1.1          Router type:  ABR  ASBR  NSSA
 Route tag: 0
 Route tag check: Disabled
 Multi-VPN-Instance: Disabled
 Type value of extended community attributes:
    Domain ID : 0x0005
    Route type: 0x0306
    Router ID : 0x0107
 Domain-id: 0.0.0.0
 DN-bit check: Enabled
 DN-bit set: Enabled
 Originating router-LSAs with maximum metric
    Condition: On startup for 600 seconds, State: Inactive
    Advertise summary-LSAs with metric 16711680
    Advertise external-LSAs with metric 16711680
    Advertise intra-area-prefix-LSAs with maximum metric
 SPF-schedule-interval: 5 50 200
 LSA generation interval: 5
 LSA arrival interval: 1000
 Transmit pacing: Interval: 20 Count: 3
 Default ASE parameters: Tag: 1
 Route preference: 10
 ASE route preference: 150
 FRR backup mode: LFA
 SPF calculation count: 0
 External LSA count: 0
 LSA originated count: 0
 LSA received count: 0
 Area count: 2  Stub area count: 0  NSSA area count: 1
 ExChange/Loading neighbors: 0
```

```
Max equal cost paths: 32
Up interfaces: 1
Full neighbors: 1
Normal areas with up interfaces: 1
Calculation trigger type: Full
Current calculation type: SPF calculation
Current calculation phase: Calculation area topology
Redistribute timer: Off
Redistribute schedule type: RIB
Redistribute route count: 0
Process reset state: N/A
Current reset type: N/A
Next reset type: N/A
Reset prepare message replied: -/-/-/-
Reset process message replied: -/-/-/-
Reset phase of module:
  M-N/A, P-N/A, S-N/A, C-N/A, R-N/A

Area: 0.0.0.0
Area flag: Normal
SPF scheduled count: 0
ExChange/Loading neighbors: 0
LSA count: 0
Up interfaces: 0
MTU: 1440
Default cost: 1
Created by Vlink
Process reset state: N/A
Current reset type: N/A
Reset prepare message replied: -/-/-/-
Reset process message replied: -/-/-/-
Reset phase of module:
  M-N/A, P-N/A, S-N/A, C-N/A, R-N/A

Area: 0.0.0.2
Area flag: Normal
SPF scheduled count: 0
ExChange/Loading neighbors: 0
LSA count: 0
IPsec profile name: Profile000
Keychain authentication: Enabled (test)
Up interfaces: 1
MTU: 1500
Default cost: 1
Process reset state: N/A
Current reset type: N/A
Reset prepare message replied: -/-/-/-
Reset process message replied: -/-/-/-
```

```
Reset phase of module:
  M-N/A, P-N/A, S-N/A, C-N/A, R-N/A

Area: 0.0.0.3
Area flag: NSSA
7/5 translator state: Disabled
7/5 translate stability timer interval: 0
SPF Scheduled Count: 0
ExChange/Loading neighbors: 0
LSA Count: 0
Up interfaces: 0
MTU: 1440
Default cost: 1
Process reset flag: N/A
Current reset type: N/A
Reset prepare message replied: -/-/-/-
Reset process message replied: -/-/-/-
Reset phase of module:
  M-N/A, P-N/A, S-N/A, C-N/A, R-N/A
```

Table 9-1 Command output

Field	Description
OSPFv3 Process 1 with Router ID 1.1.1.1	OSPFv3 process is 1, and router ID is 1.1.1.1.
Router type	Router type: • ABR. • ASBR. • NSSA. • Null.
Route tag	Tag of the routes redistributed into the OSPFv3 process.
Route tag check	Whether the check is enabled for the route tag in OSPFv3 LSAs of the OSPFv3 process.
Multi-VPN-Instance	Whether the OSPFv3 process supports PE or multiple VPN instances: • **Multi-VPN-Instance: Disabled**—The process does not support multiple VPN instances. • **Multi-VPN-Instance: Enabled**—The process supports multiple VPN instances. • **PE Router, Multi-VPN-Instance: Enabled**—The local device is a PE.
DN-bit check	Whether the check is enabled for the DN bit in OSPFv3 LSAs of the OSPFv3 process.
DN-bit set	Whether the DN bit is set for OSPFv3 LSAs in the OSPFv3 process.
Condition	Time when the router acts as a stub router: • Always.

Field	Description
	• On startup while BGP is converging for *xxx* seconds, where *xxx* is specified by the user. • On startup for *xxx* seconds, where *xxx* is specified by the user.
State	State of the stub router: • Active. • Inactive.
SPF-schedule-interval	Interval for SPF calculations.
Transmit pacing	LSU advertisement rate: • **Interval**—Specifies the interval for sending LSUs. • **Count**—Specifies the maximum number of LSUs sent at each interval.
Default ASE parameters	Default parameters of redistributed routes. **Tag** represents the route tag of the redistributed routes.
Route preference	Internal route preference.
ASE route preference	AS-external route preference.
FRR backup mode	FRR backup mode: • **LFA**—Uses the LFA algorithm to calculate a backup next hop for all routes. **LFA ABR-only** indicates that only the next hop of the route to the ABR can be used as the backup next hop. • **route-policy** *route-policy-name*—Specifies a backup next hop by using a routing policy.
LSA originated count	Number of originated LSAs.
LSA received count	Number of received LSAs.
Area count	Total number of areas.
Stub area count	Number of stub areas.
NSSA area count	Number of NSSA areas.
ExChange/Loading neighbors	Neighbors in ExChange/Loading state.
Calculation trigger type	Route calculation trigger type: • **Full**—Calculation of all routes is triggered. • **Area topology change**—Topology change in an area. • **Intra router change**—Incremental intra-area route change. • **ASBR change**—Incremental ASBR route change. • **Full IP prefix**—Calculation of all IP prefixes is triggered. • **Full intra AS**—Calculation of all intra-AS prefixes is triggered. • **Inc intra AS**—Calculation of incremental intra-AS prefixes is triggered. • **Full inter AS**—Calculation of all AS-external prefixes is triggered. • **Inc inter AS**—Calculation of incremental AS-external prefixes is triggered.

Field	Description
	• **Nexthop calculation**—Calculation of next hops is triggered. • **N/A**—Route calculation is not triggered.
Current calculation type	Current route calculation type: • SPF calculation. • **Intra router calculation**—Intra-area route calculation. • **ASBR calculation**—Inter-area ASBR route calculation. • **Inc intra router**—Incremental intra-area route calculation. • **Inc ASBR calculation**—Incremental inter-area ASBR route calculation. • **Full intra AS**—Calculation of all intra-AS prefixes. • **Inc intra AS**—Calculation of incremental intra-AS prefixes. • **Full inter AS**—Calculation of all AS-external prefixes. • **Inc inter AS**—Calculation of incremental AS-external prefixes. • **N/A**—Route calculation is not triggered.
Current calculation phase	Current route calculation phase: • **Calculation area topology**—Calculating area topology. • **Calculation router**—Calculating routes on routers. • **Calculation intra AS**—Calculating intra-AS routes. • **Calculation ASBR**—Calculating routes on ASBRs. • **Calculation inter AS**—Calculating AS-external routes. • **Calculation end**—Ending phase of calculation. • **N/A**—Route calculation is not triggered.
Redistribute timer	Route redistribution timer status: on or off.
Redistribute schedule type	Route redistribution scheduling type: • **RIB**—Redistribute routes through the RIB table. • **Self**—Redistribute routes through the routing table. • **N/A**—Route redistribution is not triggered.
Redistribute route count	Number of redistributed routes.
Process reset state	Process reset state: • **N/A**—The process is not reset. • **Under reset**—The process is in the reset progress. • **Under RIB smooth**—The process is synchronizing RIB routes.
Current reset type	Current process reset type:

Field	Description
	• **N/A**—The process is not reset. • **GR quit**—Normal reset when GR quits abnormally. • **Delete**—Delete OSPFv3 process. • **Undo router-id**—Delete router ID. • **Set router-id**—Set router ID.
Next reset type	Next process reset type: • **N/A**—The process is not reset. • **GR quit**—Normal reset when GR quits abnormally. • **Delete**—Delete OSPFv3 process. • **Undo router-id**—Delete router ID. • **Set router-id**—Set router ID.
Reset prepare message replied	Modules that reply reset prepare messages: • **P**—Neighbor maintenance module. • **S**—LSDB synchronization module. • **C**—Route calculation module. • **R**—Route redistribution module.
Reset process message replied	Modules that reply reset process messages: • **P**—Neighbor maintenance module. • **S**—LSDB synchronization module. • **C**—Route calculation module. • **R**—Route redistribution module.

Reset phase of module	Reset phase of each module:
	• LSDB synchronization (S) module:
	  ○ **N/A**—Not reset.
	  ○ **Delete ASE**—Delete all ASE LSAs.
	  ○ **Delete area LSA**—Delete LSAs from an area.
	  ○ **Delete area IF**—Delete interfaces from an area.
	• Route calculation (C) module:
	  ○ **N/A**—Not reset.
	  ○ **Delete topology**—Delete area topology.
	  ○ **Delete router**—Delete routes of routers.
	  ○ **Delete intra AS**—Delete intra-AS routes
	  ○ **Delete inter AS**—Delete AS-external routes.
	  ○ **Delete ASBR**—Delete ASBR routes.
	• Route redistribution (R) module:
	  ○ **N/A**—Not reset.
	  ○ **Delete import**—Delete redistributed routes.

IPsec profile name	IPsec profile applied to the interface.
Keychain authentication: Enabled (test)	Keychain authentication is enabled for the area, and the keychain **test** is used.
Created by Vlink	The area is created through virtual link.
7/5 translator state	State of the translator that translates Type-7 LSAs to Type-5 LSAs:

Field	Description
	• **Enabled**—The translator is specified through commands. • **Elected**—The translator is designated through election. • **Disabled**—The device is not a translator.
7/5 translate stability timer interval	Stability interval (in seconds) for Type-7 LSA-to-Type-5 LSA translation.

9.1.7. display ospfv3 abr-asbr

Use **display ospfv3 abr-asbr** to display information about the routes to OSPFv3 ABR and ASBR.

Syntax

display ospfv3 [*process-id*] **abr-asbr**

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies an OSPFv3 process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays information about all the routes to the OSPFv3 ABR and ASBR.

Examples

Display information about all the routes to the OSPFv3 ABR and ASBR.

```
<Switch> display ospfv3 abr-asbr

                OSPFv3 Process 1 with Router ID 1.1.1.1

 Destination : 1.1.1.2                                  Rtr Type : ABR
 Area        : 0.0.0.0                                  Path Type: Intra
 Interface   : Vlan102                                BkInterface: Vlan101
 NextHop     : FE80:1:1::1
 BkNexthop   : FE80:1:2::2
 Cost        : 1

 Destination : 1.1.1.3                                  Rtr Type : ASBR
 Area        : 0.0.0.0                                  Path Type: Intra
 Interface   : Vlan103                                BkInterface: Vlan104
 BkNexthop   : FE80:1:2::4
```

```
NextHop      : FE80:2:1::1
Cost         : 1
```

Table 9-2 Command output

Field	Description
OSPFv3 Process 1 with Router ID 1.1.1.1	OSPFv3 process is 1, and router ID is 1.1.1.1.
Destination	Router ID of an ABR or ASBR.
Rtr Type	Router type: ABR or ASBR.
Area	Area ID of the next hop.
Path Type	Type of the route to the ABR or ASBR: • **Intra**—Intra-area route. • **Inter**—Inter-area route.
Interface	Output interface.
BkInterface	Backup output interface.
NextHop	Next hop address.
BkNexthop	Backup next hop address.
Cost	Cost from the router to the ABR or ASBR.

9.1.8. display ospfv3 abr-summary

Use **display ospfv3 abr-summary** to display ABR summary route information.

Syntax

display ospfv3 [*process-id*] [**area** *area-id*] **abr-summary** [*ipv6-address prefix-length*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies an OSPFv3 process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays information about ABR summary routes for all OSPFv3 processes.

area *area-id*: Specifies an OSPFv3 area by its ID. The area ID is an IP address or a decimal integer in the range of 0 to 4294967295 that is translated into the IP address format. If you do not specify this option, the command displays information about ABR summary routes for all OSPFv3 areas.

ipv6-address prefix-length: Specifies an IPv6 address. The *ipv6-address* argument specifies an IPv6 prefix. The *prefix-length* argument specifies a prefix length in the range of 0 to 128. If you do not specify this argument, the command displays information about all summary routes on the ABR.

verbose: Displays detailed ABR summary route information. If you do not specify this keyword, the command displays brief ABR summary route information.

Examples

Display brief ABR summary route information in OSPFv3 process 1.

```
<Switch> display ospfv3 1 abr-summary

            OSPFv3 Process 1 with Router ID 2.2.2.2

                    Area: 1.1.1.1
 Total summary addresses: 1

 Prefix       : 1000:4::/32
 Status       : Advertise
 NULL0        : Active
 Cost         : 1 (Configured)
 Routes count: 2
```

Table 9-3 Command output

Field	Description
Area	Area to which the summary routes belong.
Total summary addresses	Total number of summary routes.
Prefix	Prefix of the summary route.
Status	Advertisement status of the summary route.
NULL0	Null 0 route.
Cost	Cost of the summary route.
Routes count	Number of summarized routes.

Display detailed ABR summary route information in OSPFv3 process 1.

```
<Switch> display ospfv3 1 abr-summary verbose

            OSPFv3 Process 1 with Router ID 2.2.2.2

                      Area: 1.1.1.1
Total summary addresses: 1

 Prefix       : 1000:4::/32
 Status       : Advertise
 NULL0        : Active
 Cost         : 1 (Configured)
```

```
Routes count: 2
  Destination                                     Metric
  1000:4:10:3::/96                                1
  1000:4:11:3::/96                                1
```

Table 9-4 Command output

Field	Description
Destination	Destination address of a summarized route.
Metric	Metric of a summarized route.

9.1.9. display ospfv3 asbr-summary

Use **display ospfv3 asbr-summary** to display ASBR summary route information.

Syntax

display ospfv3 [*process-id*] **asbr-summary** [*ipv6-address prefix-length*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies an OSPFv3 process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays information about ASBR summary routes for all OSPFv3 processes.

ipv6-address prefix-length: Specifies an IPv6 address. The *ipv6-address* argument specifies an IPv6 prefix. The *prefix-length* argument specifies a prefix length in the range of 0 to 128. If you do not specify this argument, the command displays information about all ASBR summary routes.

verbose: Displays detailed ASBR summary route information. If you do not specify this keyword, the command displays brief ASBR summary route information.

Examples

Display brief ASBR summary route information in OSPFv3 process 1.

```
<Switch> display ospfv3 1 asbr-summary

                OSPFv3 Process 1 with Router ID 2.2.2.2

 Total summary addresses: 1
```

```
Prefix      : 1000:4::/32
Status      : Advertise
NULL0       : Active
Cost        : 1 (Configured)
Tag         : (Not configured)
Nssa-only   : (Not configured)
Routes count: 2
```

Table 9-5 Command output

Field	Description
Total summaryaddresses	Total number of summaryroutes.
Prefix	Prefix and prefix length of the summaryroute.
Status	Advertisement status of the summaryroute: • **Advertise**—The summaryroute has been advertised. • **Not-advertise**—The summaryroute has not been advertised.
NULL0	Status of the Null 0 route: • Active. • Inactive.
Cost	Cost of the summaryroute: • Configured. • Not configured.
Tag	Tag of the summaryroute: • Configured. • Not configured.
Nssa-only	Whether the **nssa-only** attribute is configured: • Configured. • Not configured.
Routes count	Number of summarized routes.

Display detailed ASBR summary route information in OSPFv3 process 1.

```
<Switch> display ospfv3 1 asbr-summary verbose

              OSPFv3 Process 1 with Router ID 2.2.2.2

 Total summary addresses: 1

 Prefix      : 1000:4::/32
 Status      : Advertise
 NULL0       : Active
 Cost        : 1 (Configured)
 Tag         : (Not configured)
 Nssa-only   : (Not configured)
 Routes count: 2
  Destination                              Protocol Process Type Metric
```

```
1000:4:10:3::/96                        Static   0       2     1
1000:4:11:3::/96                        Static   0       2     1
```

Table 9-6 Command output

Field	Description
Destination	Prefix and prefix length of the summarized route.
Protocol	Routing protocol from which the route was redistributed.
Process	Process of the routing protocol from which the route was redistributed.
Type	Type of the summarized route.
Metric	Metric of the summarized route.

9.1.10. display ospfv3 graceful-restart

Use **display ospfv3 graceful-restart** to display GR information.

Syntax

display ospfv3 [*process-id*] **graceful-restart** [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies an OSPFv3 process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays GR information for all processes.

verbose: Displays detailed GR information. If you do not specify this keyword, the command displays brief GR information.

Examples

Display brief GR information for all OSPFv3 processes (GR restarter).

```
<Switch> display ospfv3 graceful-restart

                OSPFv3 Process 1 with Router ID 3.3.3.3

 Graceful-restart capability      : Enable
 Graceful-restart support         : Planned and un-planned, Partial
 Helper capability                : Enable
 Helper support                   : Planned and un-planned
 Current GR state                 : Normal
```

```
Graceful-restart period         : 120 seconds
Number of neighbors under helper: 0
Number of restarting neighbors  : 0
Last exit reason:
  Restarter: None
  Helper   : None
```

Table 9-7 Command output

Field	Description
OSPFv3 Process 1 with Router ID 3.3.3.3	The GR status of OSPFv3 process 1 with router ID 3.3.3.3 is displayed.
Graceful-restart capability	Whether OSPFv3 GR is enabled: • Enabled. • Disabled.
Graceful-restart support	GR modes that the process supports (displayed only when GR is enabled): • **Planned and un-planned**—Supports both planned and unplanned GR. • **Planned only**—Supports only planned GR. • **Partial**—Supports partial GR. • **Global**—Supports global GR.
Helper capability	Whether OSPFv3 GR helper is enabled: • Enabled. • Disabled.
Helper support	Policies and GR modes that the GR helper supports (displayed only when GR helper is enabled): • **Strict LSA check**—The GR helper supports strict LSA checking. • **Planned and un-planned**—The GR helper supports both planned and unplanned GR. • **Planned only**—The GR helper supports only planned GR.
Current GR state	GR status: • **Normal**—GR is not in progress or has completed. • **Under GR**—GR is in progress. • **Under Helper**—The process is acting as GR helper.
Graceful-restart period	GR restart interval.
Number of neighbors under helper	Number of neighbors in GR helper status.
Number of restarting neighbors	Number of neighbors in GR restarter status.

Last exit reason	Last exit reason:
	• **Restarter**—Reason that the restarter exited most recently:
	  ○ None.
	  ○ **Completed**—GR is completed.
	  ○ **Interval timer is fired**—The GR timer expires.

Field	Description
	○ **Interface state change**—An interface state change occurs. ○ **Received 1-way hello**—The device receives 1-way hello packets from the neighbor. ○ **Reset neighbor**—The neighbor is reset. ○ **DR or BDR change**—The DR or BDR changes. • **Helper**—Reason that the helper exited most recently: ○ None. ○ **Completed**—GR is completed. ○ **Received 1-way hello**—The device receives 1-way hello packets from the neighbor. ○ **Grace Period timer is fired**—The GR timer expires. ○ **Lsa check failed**—An LSA change on the GR helper is detected. ○ **Reset neighbor**—The neighbor is reset. ○ **Received MAXAGE gracelsa but neighbor is not full**—The device receives Grace-LSAs that reached the maximum age, but the neighbor is not in Full state.

Display detailed GR information for all OSPFv3 processes (GR restarter).

```
<Switch> display ospfv3 graceful-restart verbose

               OSPFv3 Process 1 with Router ID 3.3.3.3

 Graceful-restart capability     : Enable
 Graceful-restart support        : Planned and un-planned, Partial
 Helper capability               : Enable
 Helper support                  : Planned and un-planned
 Current GR state                : Normal
 Graceful-restart period         : 120 seconds
 Number of neighbors under helper: 0
 Number of restarting neighbors  : 0
 Last exit reason:
   Restarter: None
   Helper   : None

 Area: 0.0.0.0
 Area flag: Normal
 Area up interface count: 1

 Virtual-link Neighbor-ID: 100.1.1.1, Neighbor-state: Full
 Restarter state: Normal   State: P-2-P    Type: Virtual
```

```
Interface: 6696 (Vlan-interface200), Instance-ID: 0
Local  IPv6 address: 200:1:FFFF::1
Remote IPv6 address: 201:FFFF::2
Transit area: 0.0.0.1
Last exit reason:
  Restarter: None
  Helper   : None
Neighbor       GR state       Last helper exit reason
100.1.1.1      Normal         None

Area: 0.0.0.1
Area flag: Transit
Area up interface count: 3

Interface: 5506 (Vlan-interface3), Instance-ID: 0
Restarter state: Normal   State: DR       Type: Broadcast
Last exit reason:
  Restarter: None
  Helper   : None
Neighbor count of this interface: 0
Number of neighbors under helper: 0

Interface: 6696 (Vlan-interface200), Instance-ID: 0
Restarter state: Normal   State: DR       Type: Broadcast
Last exit reason:
  Restarter: None
  Helper   : None
Neighbor count of this interface: 1
Number of neighbors under helper: 0
Neighbor       GR state       Last helper exit reason
100.1.1.1      Normal         None

Area: 0.0.0.5
Area flag: NSSANoSummaryNoImportRoute
7/5 translator state: Disabled
7/5 translate stability timer interval: 0
Area up interface count: 0
```

Table 9-8 Command output

Field	Description
Area	Area ID.
Area flag	Type of the area: • Normal. • Transit. • Stub. • **StubNoSummary**—Totally stub area. • NSSA.

Field	Description
	• **NSSANoSummary**—Totally NSSA area. • **NSSANoSummaryNoImportRoute**—Totally NSSA area with the **no-import-route** keyword configured.
7/5 translator state	State of the translator that translates Type-7 LSAs to Type-5 LSAs: • **Enabled**—The translator is specified through commands. • **Elected**—The translator is designated through election. • **Disabled**—The device is not a translator.
7/5 translate stability timer interval	Stability interval (in seconds) for Type-7 LSA-to-Type-5 LSA translation.
Area up interface count	Number of up interfaces in the area.
Interface	Interface in the area, or the output interface of the virtual link.
Restarter state	Restarter state on the interface.
State	Interface state.
Type	Interface network type.
Neighbor count of this interface	Number of neighbors on the interface.
Neighbor	Neighbor router ID.
GR state	Neighbor GR state: • **Normal**—GR is not in progress or has completed. • **Under GR**—GR is in process. • **Under Helper**—The process is acting as GR helper.
Last helper exit reason	Reason that the helper exited most recently.
Virtual-link Neighbor-ID	Router ID of the virtual link's neighbor.
Neighbor-State	Neighbor or virtual link state: Down, Init, 2-Way, ExStart, Exchange, Loading, and Full.
Local IPv6 address	Local IPv6 address of the neighbor relationship.
Remote IPv6 address	Peer IPv6 address of the neighbor relationship.
Transit area	Transit area ID.

9.1.11. display ospfv3 interface

Use **display ospfv3 interface** to display OSPFv3 interface information.

Syntax

display ospfv3 [*process-id*] **interface** [*interface-type interface-number* | **verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies an OSPFv3 process by its ID in the range of 1 to 65535.

interface-type interface-number: Specifies an interface by its type and number.

verbose: Displays detailed information about all OSPFv3 interfaces.

Usage guidelines

If you do not specify a process, this command displays brief OSPFv3 interface information for all processes.

If you do not specify the *interface-type interface-number* argument or the **verbose** keyword, this command displays brief information about all OSPFv3 interfaces.

Examples

Display OSPFv3 information about VLAN-interface 1.

```
<Switch> display ospfv3 interface vlan-interface 1

               OSPFv3 Process 1 with Router ID 1.1.1.1

 Area: 0.0.0.0
----------------------------------------------------------------------------
 Vlan-interface1 is up, line protocol is up
  Interface ID 65697        Instance ID 0
  IPv6 prefixes
    fe80::200:12ff:fe34:1  (Link-Local address)
    2001::1
  Cost: 1       State: BDR       Type: Broadcast    MTU: 1500
  Priority: 1
  Designated router: 2.2.2.2
  Backup designated router: 1.1.1.1
  Timers: Hello 10, Dead 40, Poll 40, Retransmit 5, Transmit delay 1
  FRR backup: Enabled
  Neighbor count is 1, Adjacent neighbor count is 1
  Primary path detection mode: BFD echo
  IPsec profile name: profile001
  Keychain authentication: Enabled (test), inherited
  Exchanging/Loading neighbors: 0
  Wait timer: Off,  LsAck timer: Off
  Prefix-suppression is enabled
```

Table 9-9 Command output

Field	Description
Area	Area ID that the interface belongs to.
Interface ID	Interface ID.
Instance ID	Instance ID.
IPv6 prefixes	IPv6 prefix.
Cost	Cost value of the interface.
State	Interface state: • **DOWN**—No protocol traffic can be sent or received on the interface. • **Waiting**—The interface starts sending and receiving Hello packets. The router is trying to determine the identity of the (Backup) designated router for the network. • **P-2-P**—The interface will send Hello packets at the hello interval, and try to establish an adjacency with the neighbor. • **DR**—The router is the designated router on the network. • **BDR**—The router is the backup designated router on the network. • **DROther**—The router is a DR Other router on the attached network.
Type	Network type of the interface: PTP (P2P), PTMP (P2MP), Broadcast, or NBMA.
MTU	MTU value of the interface.
Priority	DR priority of the interface.
Designated router	DR on this link.
Backup designated router	BDR on this link.
Timers	Time intervals in seconds configured on the interface: • **Hello**—Hello interval. • **Dead**—Dead interval. • **Poll**—Polling interval on an NBMA network. • **Retransmit**—LSA retransmission interval.
Transmit Delay	LSA transmission delay on the interface, in seconds.
FRR backup	Whether LFA calculation is enabled on an interface: • **Enabled**. • **Disabled**.
Neighbor count	Number of neighbors on the interface.
Primary path detection mode	Primary link detection mode: • **BFD ctrl**—BFD control packet mode. • **BFD echo**—BFD echo packet mode.
Adjacent neighbor count	Number of adjacencies on the interface.
IPsec profile name	IPsec profile applied to the interface.

Field	Description
Keychain authentication: Enabled (test), inherited	Keychain authentication is enabled for the interface, and the keychain **test** is used. The **inherited** attribute indicates that the interface is using the authentication mode specified for the area to which the interface belongs.

9.1.12. display ospfv3 lsdb

Use **display ospfv3 lsdb** to display OSPFv3 LSDB information.

Syntax

display ospfv3 [*process-id*] **lsdb** [{ **external** | **grace** | **inter-prefix** | **inter-router** | **intra-prefix** | **link** | **network** | **router** | **unknown** [*type*] } [*link-state-id*] [**originate-router** *router-id* | **self-originate**] | **statistics** | **total** | **verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies an OSPFv3 process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays LSDB information for all processes.

external: Displays AS external LSAs (Type-5 LSAs).

grace: Displays Grace-LSAs (Type-11 LSAs).

inter-prefix: Displays Inter-area-prefix LSAs (Type-3 LSAs).

inter-router: Displays Inter-area-router LSAs (Type-4 LSAs).

intra-prefix: Displays Intra-area-prefix LSAs (Type-9 LSAs).

link: Displays Link-LSAs (Type-8 LSAs).

network: Displays Network-LSAs (Type-2 LSAs).

router: Displays Router-LSAs (Type-1 LSAs).

unknown: Displays unknown LSAs.

type: Specifies an LSA type, a hexadecimal string of 0 to ffff. If you do not specify this argument, the command displays all unknown LSAs.

link-state-id: Specifies a link state ID in IPv4 address format.

originate-router *router-id*: Specifies an advertising router by its ID.

self-originate: Displays locally originated LSAs.

statistics: Displays LSA statistics.

total: Displays the total number of LSAs in the LSDB.

verbose: Displays detailed information. If you do not specify this keyword, the command displays brief information.

Examples

Display OSPFv3 LSDB information.

```
<Switch> display ospfv3 lsdb

                OSPFv3 Process 1 with Router ID 1.1.1.1

                    Link-LSA (Interface Vlan-interface100)
------------------------------------------------------------------------------
 Link State ID   Origin Router    Age   SeqNum     CkSum  Prefix
 0.15.0.8        2.2.2.2          0691  0x80000041 0x8315      1
 0.0.0.3         1.1.1.1          0623  0x80000001 0x0fee      1

                    Router-LSA (Area 0.0.0.1)
------------------------------------------------------------------------------
 Link State ID   Origin Router    Age   SeqNum     CkSum    Link
 0.0.0.0         1.1.1.1          0013  0x80000068 0x5d5f      2
 0.0.0.0         2.2.2.2          0024  0x800000ea 0x1e22      0

                    Network-LSA (Area 0.0.0.1)
------------------------------------------------------------------------------
 Link State ID   Origin Router    Age   SeqNum     CkSum
 0.15.0.8        2.2.2.2          0019  0x80000007 0x599e

                    Intra-Area-Prefix-LSA (Area 0.0.0.1)
------------------------------------------------------------------------------
 Link State ID   Origin Router    Age   SeqNum     CkSum  Prefix  Reference
 0.0.0.2         2.2.2.2          3600  0x80000002 0x2eed      2 Network-LSA
 0.0.0.1         2.2.2.2          0018  0x80000001 0x1478      1 Network-LSA
```

Table 9-10 Command output

Field	Description
Origin Router	Originating router.
Age	Age of LSAs.
SeqNum	LSA sequence number.
CkSum	LSA checksum.
Prefix	Number of prefixes.

Field	Description
Link	Number of links.
Reference	Type of referenced LSA.

Display Link LSA information in the LSDB.

```
<Switch> display ospfv3 lsdb link

               OSPFv3 Process 1 with Router ID 1.1.1.1
                  Link-LSA (Interface Vlan-interface100)
------------------------------------------------------------------------------
  LS age             : 833
  LS Type            : Link-LSA
  Link State ID      : 0.15.0.8
  Originating Router: 2.2.2.2
  LS Seq Number      : 0x80000041
  Checksum           : 0x8315
  Length             : 56
  Priority           : 1
  Options            : 0x000013 (-|R|-|x|E|V6)
  Link-Local Address: fe80::200:5eff:fe00:100
  Number of Prefixes: 1
      Prefix         : 1001::/64
      Prefix Options: 0 (-|-|x|-|-)
```

Table 9-11 Command output

Field	Description
LS age	Age of LSA.
LS Type	Type of LSA.
Link State ID	Link state ID.
Originating Router	Originating router.
LS Seq Number	LSA sequence number.
Checksum	LSA checksum.
Length	LSA length.
Priority	Router priority.
Options	Options.
Link-Local Address	Link-local address.
Number of Prefixes	Number of prefixes.
Prefix	Address prefix.
Prefix Options	Prefix options.

Display LSA statistics.

```
<System> display ospfv3 lsdb statistics
```

```
              OSPFv3 Process 1 with Router ID 1.1.1.1
--------------------------------------------------------------------------
 Area ID         Router Network IntePre  InteRou IntraPre NSSA
 0.0.0.1         2      0       0        0       2        0
 0.0.0.3         1      0       0        0       1        1
 Total           3      0       0        0       3        1
--------------------------------------------------------------------------
                 Link   Grace   ASE
 Total           4      0       0
```

Table 9-12 Command output

Field	Description
Area ID	Area ID.
Router	Number of Type-1 LSAs.
Network	Number of Type-2 LSAs.
IntePre	Number of Type-3 LSAs.
InteRou	Number of Type-4 LSAs.
IntraPre	Number of Type-9 LSAs.
NSSA	Number of Type-7 LSAs.
Link	Total number of Type-8 LSAs.
Grace	Number of Type-11 LSAs.
ASE	Total number of Type-5 LSAs.

Display detailed OSPFv3 LSDB information.

```
<Switch> display ospfv3 lsdb verbose

              OSPFv3 Process 1 with Router ID 1.1.1.1

                 Link-LSA (Interface Vlan-interface100)
--------------------------------------------------------------------------
 Link State ID   Origin Router    Age   SeqNum     CkSum  Prefix
 0.15.0.8        2.2.2.2          0691  0x80000041 0x8315      1
                 SendCnt: 0       RxmtCnt: 0       Status: Stale
 0.0.0.3         1.1.1.1          0623  0x80000001 0x0fee      1
                 SendCnt: 0       RxmtCnt: 0       Status: Stale

                 Router-LSA (Area 0.0.0.1)
--------------------------------------------------------------------------
 Link State ID   Origin Router    Age   SeqNum     CkSum    Link
 0.0.0.0         1.1.1.1          0013  0x80000068 0x5d5f      2
                 SendCnt: 0       RxmtCnt: 0       Status: Stale
 0.0.0.0         2.2.2.2          0024  0x800000ea 0x1e22      0
                 SendCnt: 0       RxmtCnt: 0       Status: Stale
```

```
                  Network-LSA (Area 0.0.0.1)
-------------------------------------------------------------------------
 Link State ID   Origin Router    Age   SeqNum     CkSum
 0.15.0.8        2.2.2.2          0019  0x80000007 0x599e
                 SendCnt: 0       RxmtCnt: 0       Status: Stale

                  Intra-Area-Prefix-LSA (Area 0.0.0.1)
-------------------------------------------------------------------------
 Link State ID   Origin Router    Age   SeqNum     CkSum  Prefix  Reference
 0.0.0.2         2.2.2.2          3600  0x80000002 0x2eed      2 Network-LSA
                 SendCnt: 0       RxmtCnt: 0       Status: Stale
 0.0.0.1         2.2.2.2          0018  0x80000001 0x1478      1 Network-LSA
                 SendCnt: 0       RxmtCnt: 0       Status: Stale
```

Table 9-13 Command output

Field	Description
SendCnt	Number of interfaces to send the LSA.
RxmtCnt	Number of LSAs in the link state retransmission list.
Status	LSA status: • Normal. • Delayed. • **Maxage routed**—The LSA has reached its maximum age. • Self originated. • **Stale**—A self-originated LSAis received during the GR process.

9.1.13. display ospfv3 nexthop

Use **display ospfv3 nexthop** to display OSPFv3 next hop information.

Syntax

display ospfv3 [*process-id*] **nexthop**

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies an OSPFv3 process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays next hop information for all OSPFv3 processes.

Examples

Display next hop information for OSPFv3 process 1.

```
<Switch> display ospfv3 1 nexthop

                OSPFv3 Process 1 with Router ID 1.1.1.1

 Nexthop : FE80::20C:29FF:FED7:F308              Interface: Vlan102
 RefCount: 4                                     Status   : Valid
 NbrID   : 1.1.1.1                               NbrIntID : 21

 Nexthop : FE80::20C:29FF:FED7:F312              Interface: Vlan103
 RefCount: 3                                     Status   : Valid
 NbrID   : 1.1.1.1                               NbrIntID : 38
```

Table 9-14 Command output

Field	Description
Nexthop	Next hop address.
Interface	Output interface.
RefCount	Reference count (routes that use the next hop).
Status	Next hop status: valid or invalid.
NbrId	Neighbor router ID.
NbrIntID	Neighbor interface ID.

9.1.14. display ospfv3 peer

Use **display ospfv3 peer** to display information about OSPFv3 neighbors.

Syntax

display ospfv3 [*process-id*] [**area** *area-id*] **peer** [[*interface-type interface-number*] [**verbose**] | *peer-router-id* | **statistics**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies an OSPFv3 process by its ID in the range of 1 to 65535. If you do not specify a process, this command displays neighbor information for all processes.

area *area-id*: Specifies an area by its ID, an IPv4 address or a decimal integer in the range of 0 to 4294967295 that is translated into the IPv4 address format. If you do not specify an area, this command displays neighbor information for all areas.

interface-type interface-number: Specifies an interface by its type and number.

verbose: Displays detailed neighbor information.

peer-router-id: Specifies a neighbor.

statistics: Displays OSPFv3 neighbor statistics.

Usage guidelines

If you do not specify an interface and a neighbor, this command displays neighbor information for all interfaces.

Examples

Display neighbor information for OSPFv3 process 1.

```
<Switch> display ospfv3 1 peer vlan-interface 1

              OSPFv3 Process 1 with Router ID 1.1.1.1

 Area: 0.0.0.1
----------------------------------------------------------------------------
 Router ID       Pri State             Dead-Time InstID Interface
 2.2.2.2         1   Init/ -           00:00:36  0      Vlan1
```

Table 9-15 Command output

Field	Description
Router ID	Neighbor router ID.
Pri	Neighboring router priority.
State	Neighbor state.
Dead-Time	Dead time remained.
Inst ID	Instance ID.
Interface	Interface connected to the neighbor.

Display detailed neighbor information for OSPFv3 process 1.

```
<Switch> display ospfv3 1 peer vlan-interface 1 verbose

              OSPFv3 Process 1 with Router ID 1.1.1.1

 Area 0.0.0.1 interface Vlan1's neighbors
 Router ID: 2.2.2.2          Address: fe80::200:5eff:fe00:100
   State: ExStart  Mode: None  Priority: 1
   DR: 2.2.2.2  BDR: None   MTU: 1500
   Options is 0x000413 (AT|-|-|-|-|R|-|x|E|V6)
   Dead timer due in 00:00:33
```

```
Neighbor is up for 00:24:19
Authentication sequence: (high) 0, (low) 59755
Neighbor state change count: 205
Database Summary List 0
Link State Request List 0
Link State Retransmission List 0
Neighbor interface ID: 8037
GR state: Normal
Grace period: 0           Grace period timer: Off
DD Rxmt Timer: Off        LS Rxmt Timer: On
```

Table 9-16 Command output

Field	Description
Router ID	Neighbor router ID.
Address	Link-local address of the interface.
State	Neighbor state.
Mode	Neighbor mode for LSDB synchronization.
Priority	Neighboring router priority.
DR	DR on the interface's network segment.
BDR	BDR on the interface's network segment.
MTU	Interface MTU.
Options	LSA options: • **AT**—Whether the Authentication Trailer option is carried in packets. • **DC**—The originating router supports OSPFv3 over on-demand circuits. • **R**—Whether the originating router is an active router. • **N**—Whether the originating router supports NSSA LSAs. • **x**—Reserved. • **E**—Whether the originating router can receive AS External LSAs. • **V6**—Whether the originating router takes part in IPv6 route calculation.
Dead timer due in 33 sec	This dead timer will expire in 33 seconds.
Neighbor is up for 00:24:19	The neighbor has been up for 00:24:19.
Authentication sequence: (high) 0, (low) 59755	Authentication sequence number carried in the received packets. The high 32-bit value is 0, and the low 32-bit value is 59755.
Neighbor state change count	Count of neighbor state changes.
Database Summary List	Number of LSAs sent in DD packet.
Link State Request List	Number of LSAs in the link state request list.
Link State Retransmission List	Number of LSAs in the link state retransmission list.
Neighbor interface ID	Interface ID of the neighbor.

Field	Description
GR state	GR state: • **Normal**—GR is not in progress. • **Doing GR**—Acting as the GR restarter. • Complete GR. • **Helper**—Acting as the GR helper.
Grace period	Grace-LSA sending interval.
Grace period timer	Grace-LSA sending interval timer.
DD Rxmt Timer	DD packet retransmission timer.
LS Rxmt Timer	LSU retransmission timer.

Display OSPFv3 neighbor statistics.

```
<Switch> display ospfv3 peer statistics

                OSPFv3 Process 1 with Router ID 1.1.1.1
----------------------------------------------------------------------------
 Area ID          Down Attempt Init 2-Way ExStart Exchange Loading Full Total
 0.0.0.0          0    0       0    0      0       0        0       1    1
 Total            0    0       0    0      0       0        0       1    1
```

Table 9-17 Command output

Field	Description
Area ID	Area ID.
Down	In this state, neighbor initial state, the router has not received any information from a neighboring router for a period of time.
Attempt	This state is available only in an NBMA network. In this state, the OSPFv3 router has not received any information from a neighbor for a period. The router can send Hello packets at a longer interval to keep the neighbor relationship.
Init	In this state, the device received a Hello packet from the neighbor but the packet contains no router ID of the neighbor. Mutual communication is not setup.
2-Way	Mutual communication between the router and its neighbor is available. DR/BDR election is finished under this state (or higher).
ExStart	In this state, the router decides on the initial DD sequence number and active/standby relationship of the two parties.
Exchange	In this state, the router exchanges DD packets with the neighbor.
Loading	In this state, the router sends LSRs to request the neighbor for needed LSAs.
Full	LSDB synchronization has been accomplished between neighbors.
Total	Total number of neighbors under the same state.

9.1.15. display ospfv3 request-queue

Use **display ospfv3 request-queue** to display OSPFv3 request list information.

Syntax

display ospfv3 [*process-id*] [**area** *area-id*] **request-queue** [*interface-type interface-number*] [*neighbor-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies an OSPFv3 process by its ID in the range of 1 to 65535. If you do not specify an OSPFv3 process, this command displays OSPFv3 request list information for all OSPFv3 processes.

area *area-id*: Specifies an area by its ID, an IPv4 address or a decimal integer in the range of 0 to 4294967295 that is translated into the IPv4 address format. If you do not specify an OSPFv3 area, this command displays OSPFv3 request list information for all areas.

interface-type interface-number: Specifies an interface by its type and number. If you do not specify an interface, this command displays OSPFv3 request list information for all interfaces.

neighbor-id: Specifies a neighbor's router ID. If you do not specify a neighbor, this command displays OSPFv3 request list information for all OSPFv3 neighbors.

Examples

Display OSPFv3 request list information.

```
<Switch> display ospfv3 request-queue

                OSPFv3 Process 1 with Router ID 1.1.1.1

                    Area: 0.0.0.0
                    Interface Vlan-interface100
----------------------------------------------------------------------------
                    Nbr-ID 1.3.3.3 Request List
 Type     LinkState ID     AdvRouter        SeqNum       Age   CkSum
 0x4005   0.0.34.127       1.3.3.3          0x80000001   0027  0x274d
 0x4005   0.0.34.128       1.3.3.3          0x80000001   0027  0x2d45
 0x4005   0.0.34.129       1.3.3.3          0x80000001   0027  0x333d
 0x4005   0.0.34.130       1.3.3.3          0x80000001   0027  0x3935
```

Table 9-18 Command output

Field	Description
Area	Area ID.
Interface	Interface type and sequence number.
Nbr-ID	Neighbor ID.
Request list	Request list information.
Type	LSA type.
LinkState ID	Link state ID.
AdvRouter	Advertising router.
SeqNum	LSA sequence number.
Age	LSA age.
CkSum	Checksum.

9.1.16. display ospfv3 retrans-queue

Use **display ospfv3 retrans-queue** to display retransmission list information.

Syntax

display ospfv3 [*process-id*] [**area** *area-id*] **retrans-queue** [*interface-type interface-number*] [*neighbor-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies an OSPFv3 process by its ID in the range of 1 to 65535. If you do not specify an OSPFv3 process, this command displays retransmission list information for all OSPFv3 processes.

area *area-id*: Specifies an area by its ID, an IPv4 address or a decimal integer in the range of 0 to 4294967295 that is translated into the IPv4 address format. If you do not specify an OSPFv3 area, this command displays retransmission list information for all OSPFv3 areas.

interface-type interface-number: Specifies an interface by its type and number. If you do not specify an interface, this command displays retransmission list information for all interfaces.

neighbor-id: Specifies a neighbor's router ID. If you do not specify a neighbor, this command displays retransmission list information for all neighbors.

Examples

Display OSPFv3 retransmission list information.

```
<Switch> display ospfv3 retrans-queue

                OSPFv3 Process 1 with Router ID 1.1.1.1

                    Area: 0.0.0.0
                    Interface Vlan-interface100
----------------------------------------------------------------------------
                    Nbr-ID 1.2.2.2 Retransmit List
 Type     LinkState ID     AdvRouter        SeqNum       Age    CkSum
 0x2009   0.0.0.0         1.3.3.3          0x80000001   3600   0x49fb
```

Table 9-19 Command output

Field	Description
Area	Area ID.
Interface	Interface type and sequence number.
Nbr-ID	Neighbor ID.
Retransmit List	Retransmission list information.
Type	LSA type.
LinkState ID	Link state ID.
AdvRouter	Advertising router.
SeqNum	LSA sequence number.
Age	LSA age.
CkSum	Checksum.

9.1.17. display ospfv3 routing

Use **display ospfv3 routing** to display OSPFv3 route information.

Syntax

display ospfv3 [*process-id*] **routing** [*ipv6-address prefix-length*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies an OSPFv3 process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays the OSPFv3 route information for all processes.

ipv6-address prefix-length: Specifies an IPv6 address. The *ipv6-address* argument specifies an IPv6 prefix. The *prefix-length* argument specifies a prefix length in the range of 0 to 128.

Examples

Display OSPFv3 routing information.

```
<Switch> display ospfv3 routing

                OSPFv3 Process 1 with Router ID 9.9.9.9
--------------------------------------------------------------------------
 I  - Intra area route,  E1 - Type 1 external route,  N1 - Type 1 NSSA route
 IA - Inter area route,  E2 - Type 2 external route,  N2 - Type 2 NSSA route
 *  - Selected route

*Destination: 3::3/128
  Type       : I                                  Area       : 0.0.0.1
  AdvRouter  : 1.1.1.1                            Preference : 0
  NibID      : 0x130000001                        Cost       : 10
  Interface  : Vlan101                            BkInterface: Vlan102
  Nexthop    : FE80::20C:29FF:FED4:7171
  BkNexthop  : FE80:1:1:1

*Destination: 3::4/128
  Type       : I                                  Area       : 0.0.0.1
  AdvRouter  : 1.1.1.1                            Preference : 0
  NibID      : 0x130000001                        Cost       : 10
  Interface  : Vlan101                            BkInterface: Vlan102
  Nexthop    : FE80::10C:29AF:FE97:1210
  BkNexthop  : FE80:1:1:1

*Destination: 3::5/128
  Type       : I                                  Area       : 0.0.0.1
  AdvRouter  : 1.1.1.1                            Preference : 0
  NibID      : 0x130000001                        Cost       : 10
  Interface  : Vlan101                            BkInterface: Vlan102
  Nexthop    : FE80::10BC:28AF:FE97:1008
  BkNexthop  : FE80:1:1:1

Total: 3
 Intra area: 3         Inter area: 0         ASE: 0         NSSA: 0
```

Table 9-20 Command output

Field	Description
Destination	Destination network segment.
Type	Route type.
Area	Area ID.

Field	Description
AdvRouter	Advertising router.
Preference	OSPFv3 route preference.
NibID	Next hop ID.
Cost	Route cost value.
Interface	Output interface.
BkInterface	Backup output interface.
Nexthop	Primary next hop IP address.
BkNexthop	Backup next hop IP address.
Nexthop	Next hop address.
Interface	Output interface.
AdvRouter	Advertising router.
Area	Area ID.
Tag	Tag of external routes.
Preference	Route preference.
Total	Total number of routes.
Intra area	Number of intra-area routes.
Inter area	Number of inter-area routes.
ASE	Number of Type-5 external routes.
NSSA	Number of Type-7 external routes.

9.1.18. display ospfv3 statistics

Use **display ospfv3 statistics** to display OSPFv3 statistics.

Syntax

display ospfv3 [*process-id*] **statistics**

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies an OSPFv3 process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays OSPFv3 statistics for all processes.

Examples

Display OSPFv3 statistics.

```
<Switch> display ospfv3 statistics

              OSPFv3 Process 1 with Router ID 1.1.1.1
                  Packet Statistics
------------------------------------------------------------
 Type                          Recv              Send
 Hello                         1746              1284
 DB Description                505               941
 Ls Req                        252               136
 Ls Upd                        851               1553
 Ls Ack                        416               450

            Local Originated LSAs Statistics
------------------------------------------------------------
 Type                                           Count
 Router-LSA                                     192
 Network-LSA                                    0
 Inter-Area-Prefix-LSA                          0
 Inter-Area-Router-LSA                          0
 AS-external-LSA                                0
 NSSA-LSA                                       0
 Link-LSA                                       10
 Intra-Area-Prefix-LSA                          112
 Grace-LSA                                      0
 Unknown-LSA                                    0
 Total                                          314

                  Routes Statistics
------------------------------------------------------------
 Type                                           Count
 Intra Area                                     0
 Inter Area                                     0
 ASE                                            0
 NSSA                                           0
```

Table 9-21 Command output

Field	Description
Packet Statistics	Statistics about inbound and outbound packets.
Hello	Hello packet.
DB Description	DB description packet.
Ls Req	Link state request packet.
Ls Upd	Link state update packet.
Ls Ack	Link state acknowledgment packet.

Field	Description
Local Originated LSAs Statistics	Statistics about generated LSAs.
Router-LSA	Number of Type-1 LSAs.
Network-LSA	Number of Type-2 LSAs.
Inter-Area-Prefix-LSA	Number of Type-3 LSAs.
Inter-Area-Router-LSA	Number of Type-4 LSAs.
AS-external-LSA	Number of Type-5 LSAs.
NSSA-LSA	Number of Type-7 LSAs.
Link-LSA	Number of Type-8 LSAs.
Intra-Area-Prefix-LSA	Number of Type-9 LSAs.
Grace-LSA	Number of Type-11 LSAs.
Unknown-LSA	Number of Unknown-LSAs.
Total	Total number.
Routes Statistics	Number of routes.
Intra Area	Intra-area routes.
Inter Area	Inter-area routes.
ASE	Type-5 external routes.
NSSA	Type-7 external routes.

9.1.19. display ospfv3 vlink

Use **display ospfv3 vlink** to display OSPFv3 virtual link information.

Syntax

display ospfv3 [*process-id*] **vlink**

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies an OSPFv3 process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays the OSPFv3 virtual link information for all OSPFv3 processes.

Examples

Display OSPFv3 virtual link information.

```
<Switch> display ospfv3 vlink
```

```
                OSPFv3 Process 1 with Router ID 1.1.1.1

Virtual-link Neighbor-id: 12.2.2.2, Neighbor-state: Full
Interface: 2348 (Vlan-interface12), Instance-ID: 0
Local  IPv6 address: 3:3333::12
Remote IPv6 address: 2:2222::12
Cost: 1  State: P-2-P  Type: Virtual
Transit area: 0.0.0.1
Timers: Hello 10, Dead 40, Retransmit 5, Transmit Delay 1
IPsec profile name: profile001
Keychain authentication: Enabled (test), inherited
```

Table 9-22 Command output

Field	Description
Virtual-link Neighbor-ID	ID of the neighbor on the virtual link.
Neighbor-State	Neighbor state: Down, Init, 2-Way, ExStart, Exchange, Loading, or Full.
Interface	Number and name of the local interface on the virtual link.
Cost	Interface route cost.
State	Interface state.
Type	Virtual link.
Transit Area	Transit area ID. This field is displayed when a virtual link is present on the interface.
Timers	Values of OSPFv3 timers (in seconds): **Hello**, **Dead**, and **Retransmit**.
Transmit Delay	LSA transmission delay on the interface, in seconds.
IPsec profile name	IPsec profile applied to the virtual link.
Keychain authentication: Enabled (test), inherited	Keychain authentication is enabled for the virtual link, and the keychain **test** is used. The **inherited** attribute indicates that the virtual link is using the authentication mode specified for the backbone area.

9.1.20. filter (OSPFv3 area view)

Use **filter** to configure inbound/outbound Inter-Area-Prefix-LSA filtering on an ABR.

Use **undo filter** to remove the configuration.

Syntax

filter { *ipv6-acl-number* | **prefix-list** *prefix-list-name* | **route-policy** *route-policy-name* } { **export** | **import** }

undo filter { **export** | **import** }

Default

Inter-Area-Prefix-LSAs are not filtered.

Views

OSPFv3 area view

Predefined user roles

network-admin

Parameters

ipv6-acl-number: Specifies an IPv6 ACL by its number in the range of 2000 to 3999 to filter inbound/outbound Inter-Area-Prefix-LSAs.

prefix-list *prefix-list-name*: Specifies an IPv6 prefix list by its name, a case-sensitive string of 1 to 63 characters, to filter inbound/outbound Inter-Area-Prefix-LSAs.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters, to filter inbound/outbound Inter-Area-Prefix-LSAs.

export: Filters Inter-Area-Prefix-LSAs advertised to other areas.

import: Filters Inter-Area-Prefix-LSAs advertised into the local area.

Usage guidelines

This command applies only to an ABR.

Examples

Use IPv6 prefix list **my-prefix-list** to filter inbound Inter-Area-Prefix-LSAs. Use IPv6 basic ACL 2000 to filter outbound Inter-Area-Prefix-LSAs in OSPFv3 Area 1.

```
<Switch> system-view
[Switch] ospfv3 1
[Switch-ospfv3-1] area 1
[Switch-ospfv3-1-area-0.0.0.1] filter prefix-list my-prefix-list import
[Switch-ospfv3-1-area-0.0.0.1] filter 2000 export
```

9.1.21. filter-policy export (OSPFv3 view)

Use **filter-policy export** to configure OSPFv3 to filter redistributed routes.

Use **undo filter-policy export** to remove the configuration.

Syntax

filter-policy { *ipv6-acl-number* | **prefix-list** *prefix-list-name* } **export** [*protocol* [*process-id*]]

undo filter-policy export [*protocol* [*process-id*]]

Default

Redistributed routes are not filtered.

Views

OSPFv3 view

Predefined user roles

network-admin

Parameters

ipv6-acl-number: Specifies an IPv6 ACL by its number in the range of 2000 to 3999 to filter redistributed routes by destination address.

prefix-list *prefix-list-name*: Specifies an IPv6 prefix list by its name, a case-sensitive string of 1 to 63 characters, to filter redistributed routes by destination address.

protocol: Filters routes redistributed from the specified routing protocol. If you do not specify this argument, the command filters all redistributed routes.

process-id: Specifies a process by its ID in the range of 1 to 65535. This argument is available only when the *protocol* argument is **ripng**, or **ospfv3**.

Usage guidelines

To use an advanced ACL (with a number from 3000 to 3999) in the command, configure the ACL in one of the following ways:

- To deny/permit a route with the specified destination, use **rule** [*rule-id*] { **deny** | **permit** } **ipv6 source** *sour sour-prefix*.
- To deny/permit a route with the specified destination and prefix, use **rule** [*rule-id*] { **deny** | **permit** } **ipv6 source** *sour sour-prefix* **destination** *dest dest-prefix*.

The **source** keyword specifies the destination address of a route, and the **destination** keyword specifies the prefix of the route. For the configuration to take effect, specify a contiguous prefix.

Using the **filter-policy export** command filters only routes redistributed by the **import-route** command. If the **import-route** command is not configured to redistribute routes from other protocols and other OSPFv3 processes, the **filter-policy export** command does not take effect.

Examples

Use IPv6 prefix list **abc** to filter redistributed routes.

```
<Switch> system-view
[Switch] ipv6 prefix-list abc permit 2002:1:: 64
[Switch] ospfv3
[Switch-ospfv3-1] filter-policy prefix-list abc export
```

Configure IPv6 advanced ACL 3000 to permit only route 2001::1/128. Use ACL 3000 to filter redistributed routes.

```
<Switch> system-view
[Switch] acl ipv6 advanced 3000
```

```
[Switch-acl-ipv6-adv-3000] rule 10 permit ipv6 source 2001::1 128 destination
ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff 128
[Switch-acl-ipv6-adv-3000] rule 100 deny ipv6
[Switch-acl-ipv6-adv-3000] quit
[Switch] ospfv3
[Switch-ospfv3-1] filter-policy 3000 export
```

9.1.22. filter-policy import (OSPFv3 view)

Use **filter-policy import** to configure OSPFv3 to filter routes calculated using received LSAs.

Use **undo filter-policy import** to remove the configuration.

Syntax

filter-policy { *ipv6-acl-number* [**gateway** *prefix-list-name*] | **prefix-list** *prefix-list-name* [**gateway** *prefix-list-name*] | **gateway** *prefix-list-name* | **route-policy** *route-policy-name* } **import**

undo filter-policy import

Default

Routes calculated using received LSAs are not filtered.

Views

OSPFv3 view

Predefined user roles

network-admin

Parameters

ipv6-acl-number: Specifies an IPv6 ACL by its number in the range of 2000 to 3999 to filter routes by destination.

gateway *prefix-list-name*: Specifies an IPv6 prefix list by its name, a case-sensitive string of 1 to 63 characters, to filter routes by next hop. If you do not specify this option, the command does not filter routes by next hop.

prefix-list *prefix-list-name*: Specifies an IPv6 prefix list by its name, a case-sensitive string of 1 to 63 characters, to filter routes by destination.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters, to filter received routes.

Usage guidelines

To use an advanced ACL (with a number from 3000 to 3999) in the command, configure the ACL in one of the following ways:

- To deny/permit a route with the specified destination, use **rule** [*rule-id*] { **deny** | **permit** } **ipv6 source** *sour sour-prefix*.
- To deny/permit a route with the specified destination and prefix, use **rule** [*rule-id*] { **deny** | **permit** } **ipv6 source** *sour sour-prefix* **destination** *dest dest-prefix*.

The **source** keyword specifies the destination address of a route, and the **destination** keyword specifies the prefix of the route. For the configuration to take effect, specify a contiguous prefix.

Using the **filter-policy import** command filters only routes computed by OSPFv3. Routes that fail to pass the filter are not added to the routing table.

Examples

Use IPv6 prefix list **abc** to filter received routes.

```
<Switch> system-view
[Switch] ipv6 prefix-list abc permit 2002:1:: 64
[Switch] ospfv3
[Switch-ospfv3-1] filter-policy prefix-list abc import
```

Configure IPv6 advanced ACL 3000 to permit only route 2001::1/128 to pass. Use ACL 3000 to filter received routes.

```
<Switch> system-view
[Switch] acl ipv6 advanced 3000
[Switch-acl-ipv6-adv-3000] rule 10 permit ipv6 source 2001::1 128 destination
ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff 128
[Switch-acl-ipv6-adv-3000] rule 100 deny ipv6
[Switch-acl-ipv6-adv-3000] quit
[Switch] ospfv3
[Switch-ospfv3-1] filter-policy 3000 import
```

9.1.23. graceful-restart enable

Use **graceful-restart enable** to enable the GR capability for OSPFv3.

Use **undo graceful-restart enable** to disable the GR capability for OSPFv3.

Syntax

graceful-restart enable

undo graceful-restart enable

Default

The GR capability for OSPFv3 is disabled.

Views

OSPFv3 view

Predefined user roles

network-admin

Usage guidelines

GR includes planned GR and unplanned GR.

- **Planned GR**—Manually restarts OSPFv3 or performs an active/standby switchover. Before OSPFv3 restart or active/standby switchover, the GR restarter sends Grace-LSAs to GR helpers.
- **Unplanned GR**—OSPFv3 restarts or an active/standby switchover occurs because of device failure. Before OSPFv3 restart or active/standby switchover, the GR restarter does not send Grace-LSAs to GR helpers.

To prevent service interruption after a master/backup switchover, a GR restarter running OSPFv3 must perform the following tasks:

- Keep the GR restarter forwarding entries stable during reboot.
- Establish all adjacencies and obtain complete topology information after reboot.

Examples

Enable the GR capability for OSPFv3 process 1.

```
<Switch> system-view
[Switch] ospfv3 1
[Switch-ospfv3-1] graceful-restart enable
```

Related commands

graceful-restart helper enable

9.1.24. graceful-restart helper enable

Use **graceful-restart helper enable** to enable the GR helper capability for OSPFv3.

Use **undo graceful-restart helper enable** to disable the GR helper capability for OSPFv3.

Syntax

graceful-restart helper enable

undo graceful-restart helper enable

Default

The GR helper capability for OSPFv3 is enabled.

Views

OSPFv3 view

Predefined user roles

network-admin

Usage guidelines

Upon receiving the Grace-LSA, the neighbors with the GR helper capability enter the helper mode (and are called GR helpers). Then, the GR restarter retrieves its adjacencies and LSDB with the help of the GR helpers.

Examples

Enable the GR helper capability for OSPFv3 process 1.

```
<Switch> system-view
[Switch] ospfv3 1
[Switch-ospfv3-1] graceful-restart helper enable
```

Related commands

graceful-restart enable

9.1.25. graceful-restart helper strict-lsa-checking

Use **graceful-restart helper strict-lsa-checking** to enable strict LSA checking for the GR helper.

Use **undo graceful-restart helper strict-lsa-checking** to disable strict LSA checking for the GR helper.

Syntax

graceful-restart helper strict-lsa-checking

undo graceful-restart helper strict-lsa-checking

Default

Strict LSA checking for the GR helper is disabled.

Views

OSPFv3 view

Predefined user roles

network-admin

Usage guidelines

With GR helper enabled, when an LSA change on the GR helper is detected, the GR helper device exits the GR helper mode.

Examples

Enable strict LSA checking for the GR helper in OSPFv3 process 1.

```
<Switch> system-view
[Switch] ospfv3 1
[Switch-ospfv3-1] graceful-restart helper strict-lsa-checking
```

Related commands

graceful-restart helper enable

9.1.26. graceful-restart interval

Use **graceful-restart interval** to set the GR restart interval.

Use **undo graceful-restart interval** to restore the default.

Syntax

graceful-restart interval *interval*

undo graceful-restart interval

Default

The GR restart interval is 120 seconds.

Views

OSPFv3 view

Predefined user roles

network-admin

Parameters

interval: Specifies GR restart interval in the range of 40 to 1800 seconds.

Usage guidelines

For GR restart to succeed, the value of the GR restart interval cannot be smaller than the maximum OSPFv3 neighbor dead time of all the OSPFv3 interfaces.

Examples

Set the GR restart interval for OSPFv3 process 1 to 100 seconds.

```
<Switch> system-view
[Switch] ospfv3 1
[Switch-ospfv3-1] graceful-restart interval 100
```

Related commands

ospfv3 timer dead

9.1.27. import-route (OSPFv3 view)

Use **import-route** to redistribute routes.

Use **undo import-route** to disable route redistribution.

Syntax

import-route bgp4+ [**allow-ibgp**] [**cost** *cost-value* | **route-policy** *route-policy-name* | **type** *type*] *

undo import-route bgp4+

import-route { **direct** | **static** } [**cost** *cost-value* | **route-policy** *route-policy-name* | **type** *type*] *

undo import-route { **direct** | **static** }

import-route { **ospfv3** | **ripng** } [*process-id* | **all-processes**]

undo import-route { **ospfv3** | **ripng** } [*process-id* | **all-processes**]

Default

OSPFv3 route redistribution is disabled.

Views

OSPFv3 view

Predefined user roles

network-admin

Parameters

bgp4+: Redistributes IPv6 BGP routes.

direct: Redistributes direct routes.

static: Redistributes static routes.

ospfv3: Redistributes OSPFv3 routes.

ripng: Redistributes RIPng routes.

process-id: Specifies the process ID of a routing protocol, in the range of 1 to 65536. The default is 1.

all-processes: Redistributes routes from all the processes of the specified routing protocol.

allow-ibgp: Redistributes IBGP routes.

cost *cost-value*: Specifies a cost for redistributed routes, in the range of 1 to 16777214. The default is 1.

route-policy *route-policy-name*: Specifies a routing policy to filter redistributed routes. The *route-policy-name* argument is a case-sensitive string of 1 to 63 characters.

type *type*: Specifies the type for redistributed routes, 1 or 2. The default is 2.

Usage guidelines

An external route is a route to a destination outside the OSPFv3 AS. External routes include the following types:

- **Type-1 external routes**—Have high credibility. The cost of Type-1 external routes is comparable with the cost of OSPFv3 internal routes. The cost of a Type-1 external route equals the cost from the router to the ASBR plus the cost from the ASBR to the external route's destination.

- **Type-2 external routes**—Have low credibility. OSPFv3 considers the cost from the ASBR to a Type-2 external route is much bigger than the cost from the ASBR to an OSPFv3 internal router. The cost of a Type-2 external route equals the cost from the ASBR to the Type-2 external route's destination.

The **import-route** command cannot redistribute default routes.

The **import-route bgp4+** command redistributes only EBGP routes. The **import-route bgp4+ allow-ibgp** command redistributes both EBGP and IBGP routes, and might cause routing loops. Therefore, use it with caution.

Examples

Configure OSPFv3 process 1 to redistribute routes from RIPng and specify the type as type 2 and cost as 50.

```
<Switch> system-view
[Switch] ospfv3
[Switch-ospfv3-1] import-route ripng 10 type 2 cost 50
```

Configure OSPFv3 process 100 to redistribute the routes discovered by OSPFv3 process 160.

```
<Switch> system-view
[Switch] ospfv3 100
[Switch-ospfv3-100] import-route ospfv3 160
```

Related commands

default-route-advertise (OSPFv3 view)

9.1.28. log-peer-change

Use **log-peer-change** to enable logging for neighbor state changes.

Use **undo log-peer-change** to disable logging for neighbor state changes.

Syntax

log-peer-change

undo log-peer-change

Default

Logging for neighbor state changes is enabled.

Views

OSPFv3 view

Predefined user roles

network-admin

Usage guidelines

This feature enables the device to deliver logs about neighbor state changes to its information center. The information center processes logs according to user-defined output rules (whether

and where to output logs). For more information about the information center, see *Network Management and Monitoring Configuration Guide*.

Examples

Disable logging for neighbor state changes for OSPFv3 process 100.

```
<Switch> system-view
[Switch] ospfv3 100
[Switch-ospfv3-100] undo log-peer-change
```

9.1.29. lsa-generation-interval

Use **lsa-generation-interval** to set the OSPFv3 LSA generation interval.

Use **undo lsa-generation-interval** to restore the default.

Syntax

lsa-generation-interval *maximum-interval* [*minimum-interval* [*incremental-interval*]]

undo lsa-generation-interval

Default

The maximum interval is 5 seconds, the minimum interval is 0 milliseconds, and the incremental interval is 0 milliseconds.

Views

OSPFv3 view

Predefined user roles

network-admin

Parameters

maximum-interval: Specifies the maximum OSPFv3 LSA generation interval in the range of 1 to 60 seconds.

minimum-interval: Specifies the minimum OSPFv3 LSA generation interval in the range of 10 to 60000 milliseconds. The default is 0, which indicates that the minimum interval can be any value.

incremental-interval: Specifies the OSPFv3 LSA generation incremental interval in the range of 10 to 60000 milliseconds.

Usage guidelines

When network changes are infrequent, LSAs are generated at the minimum interval. If network changes become frequent, the LSA generation interval is incremented by the incremental interval × 2^{n-2} for each generation until the maximum interval is reached. The value *n* is the number of generation times.

The minimum interval and the incremental interval cannot be greater than the maximum interval.

Examples

Set the maximum LSA generation interval to 2 seconds, minimum interval to 100 milliseconds, and incremental interval to 100 milliseconds.

```
<Switch> system-view
[Switch] ospfv3 100
[Switch-ospfv3-100] lsa-generation-interval 2 100 100
```

Related commands

lsa-arrival-interval

9.1.30. maximum load-balancing (OSPFv3 view)

Use **maximum load-balancing** to set the maximum number of equal-cost multi-path (ECMP) routes.

Use **undo maximum load-balancing** to restore the default.

Syntax

maximum load-balancing *number*

undo maximum load-balancing

Default

8

Views

OSPFv3 view

Predefined user roles

network-admin

Parameters

number: Specifies the maximum number of ECMP routes in the range of 1 to 8. When the maximum number is 1, OSPFv3 does not perform load balancing.

Examples

Set the maximum number of ECMP routes to 2.

```
<Switch> system-view
[Switch] ospfv3 100
[Switch-ospfv3-100] maximum load-balancing 2
```

9.1.31. non-stop-routing

MEMO:

non-stop-routing command is supported from later software, including Version 7.2.16.

Use **non-stop-routing** to enable OSPFv3 NSR.

Use **undo non-stop-routing** to disable OSPFv3 NSR.

Syntax

non-stop-routing

undo non-stop-routing

Default

OSPFv3 NSR is disabled.

Views

OSPFv3 view

Predefined user roles

network-admin

Usage guidelines

This command takes effect only for the current process. As a best practice, enable OSPFv3 NSR for each process if multiple OSPFv3 processes exist.

OSPFv3 NSR and OSPFv3 GR are mutually exclusive. Do not configure the **non-stop-routing** command and the **graceful-restart enable** command at the same time.

Examples

Enable NSR for OSPFv3 process 100.

```
<Switch> system-view
[Switch] ospfv3 100
[Switch-ospfv3-100] non-stop-routing
```

9.1.32. ospfv3

Use **ospfv3** to enable an OSPFv3 process and enter OSPFv3 view.

Use **undo ospfv3** to disable an OSPFv3 process.

Syntax

ospfv3 [*process-id* | **vpn-instance** *vpn-instance-name*] *

undo ospfv3 [*process-id*]

Default

No OSPFv3 process is enabled.

Views

System view

Predefined user roles

network-admin

Parameters

process-id: Specifies an OSPFv3 process by its ID in the range of 1 to 65535. The default process ID is 1.

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the OSPFv3 process runs on the public network.

Usage guidelines

Specify a router ID for the OSPFv3 process. Otherwise, the OSPFv3 process cannot generate LSAs.

Examples

Enable OSPFv3 process 120 and set the router ID to 1.1.1.1.

```
<Switch> system-view
[Switch] ospfv3 120
[Switch-ospfv3-120] router-id 1.1.1.1
```

9.1.33. ospfv3 area

Use **ospfv3 area** to enable an OSPFv3 process on an interface and specify an area for the interface.

Use **undo ospfv3 area** to disable an OSPFv3 process on an interface.

Syntax

ospfv3 *process-id* **area** *area-id* [**instance** *instance-id*]

undo ospfv3 *process-id* **area** *area-id* [**instance** *instance-id*]

Default

No OSPFv3 processes are enabled on an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

process-id: Specifies an OSPFv3 process by its ID in the range of 1 to 65535.

area-id: Specifies an area by its ID, an IPv4 address or a decimal integer in the range of 0 to 4294967295 that is translated into the IPv4 address format.

instance *instance-id*: Specifies an instance by its ID in the range of 0 to 255. The default is 0.

Examples

Configure VLAN-interface 10 to run instance 1 of OSPFv3 process 1 in Area 1.

```
<Switch> system-view
[Switch] interface vlan-interface 10
[Switch-Vlan-interface10] ospfv3 1 area 1 instance 1
```

9.1.34. ospfv3 bfd enable

Use **ospfv3 bfd enable** to enable BFD on an OSPFv3 interface.

Use **undo ospfv3 bfd enable** to disable BFD on an OSPFv3 interface.

Syntax

ospfv3 bfd enable [**instance** *instance-id*]

undo ospfv3 bfd enable [**instance** *instance-id*]

Default

BFD is disabled on an OSPFv3 interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

instance *instance-id*: Specifies an instance by its ID in the range of 0 to 255. The default is 0.

Usage guidelines

BFD provides a mechanism to quickly detect the connectivity of links between OSPFv3 neighbors, improving the convergence speed of OSPFv3.

OSPFv3 uses BFD to implement bidirectional control detection.

Examples

Enable BFD on VLAN-interface 11 in instance 1.

```
<Switch> system-view
[Switch] interface vlan-interface 11
[Switch-Vlan-interface11] ospfv3 bfd enable instance 1
```

9.1.35. ospfv3 cost

Use **ospfv3 cost** to set an OSPFv3 cost for an interface in an instance.

Use **undo ospfv3 cost** to remove the configuration.

Syntax

ospfv3 cost *cost-value* [**instance** *instance-id*]

undo ospfv3 cost [**instance** *instance-id*]

Default

The cost is 1 for a VLAN interface, is 0 for a loopback interface, and is computed according to the interface bandwidth for other interfaces.

Views

Interface view

Predefined user roles

network-admin

Parameters

cost-value: Specifies an OSPFv3 cost in the range of 0 to 65535 for a loopback interface, and in the range of 1 to 65535 for other interfaces.

instance *instance-id*: Specifies an instance by its ID in the range of 0 to 255. The default is 0.

Examples

Set the OSPFv3 cost to 33 for VLAN-interface 10 in instance 1.

```
<Switch> system-view
[Switch] interface vlan-interface 10
[Switch-Vlan-interface10] ospfv3 cost 33 instance 1
```

9.1.36. ospfv3 dr-priority

Use **ospfv3 dr-priority** to set the router priority for an interface in an instance.

Use **undo ospfv3 dr-priority** to remove the configuration.

Syntax

ospfv3 dr-priority *priority* [**instance** *instance-id*]

undo ospfv3 dr-priority [**instance** *instance-id*]

Default

An interface has a router ID of 1.

Views

Interface view

Predefined user roles

network-admin

Parameters

priority: Specifies a router priority in the range of 0 to 255.

instance *instance-id*: Specifies an instance by its ID in the range of 0 to 255. The default is 0.

Usage guidelines

An interface's router priority determines its privilege in DR/BDR selection.

Examples

Set the router priority for VLAN-interface 10 in instance 1 to 8.

```
<Switch> system-view
[Switch] interface vlan-interface 10
[Switch-Vlan-interface10] ospfv3 dr-priority 8 instance 1
```

9.1.37. ospfv3 mtu-ignore

Use **ospfv3 mtu-ignore** to configure an interface to ignore MTU check during DD packet exchange.

Use **undo ospfv3 mtu-ignore** to remove the configuration.

Syntax

ospfv3 mtu-ignore [**instance** *instance-id*]

undo ospfv3 mtu-ignore [**instance** *instance-id*]

Default

An interface performs MTU check during DD packet exchange.

Views

Interface view

Predefined user roles

network-admin

Parameters

instance *instance-id*: Specifies an instance by its ID in the range of 0 to 255. The default is 0.

Usage guidelines

A neighbor relationship can be established only if the interface's MTU is the same as that of the peer.

Examples

Configure VLAN-interface 10 that belongs to instance 1 to ignore MTU check during DD packet exchange.

```
<Switch> system-view
```

```
[Switch] interface vlan-interface 10
[Switch-Vlan-interface10] ospfv3 mtu-ignore instance 1
```

9.1.38. ospfv3 network-type

Use **ospfv3 network-type** to specify the network type for an OSPFv3 interface.

Use **undo ospfv3 network-type** to remove the configuration.

Syntax

ospfv3 network-type { **broadcast** | **nbma** | **p2mp** [**unicast**] | **p2p** } [**instance** *instance-id*]

undo ospfv3 network-type [**instance** *instance-id*]

Default

The network type of an OSPFv3 interface is broadcast.

Views

Interface view

Predefined user roles

network-admin

Parameters

broadcast: Specifies the network type as broadcast.

nbma: Specifies the network type as NBMA.

p2mp: Specifies the network type as P2MP.

unicast: Specifies the P2MP interface to unicast OSPFv3 packets. By default, a P2MP interface multicasts OSPFv3 packets.

p2p: Specifies the network type as P2P.

instance *instance-id*: Specifies an instance by its ID in the range of 0 to 255. The default is 0.

Usage guidelines

If a router on a broadcast network does not support multicast, configure the network type for the connected interfaces as NBMA.

When the network type of an interface is NBMA or P2MP unicast, you must use the **peer** command to specify the neighbor.

When the network type of an interface is P2MP unicast, all OSPFv3 packets are unicast by the interface.

Examples

Specify the OSPFv3 network type for VLAN-interface 20 as NBMA.

```
<Switch> system-view
[Switch] interface vlan-interface 20
[Switch-Vlan-interface20] ospfv3 network-type nbma
```

Related commands

ospfv3 dr-priority

9.1.39. ospfv3 peer

Use **ospfv3 peer** to specify a neighbor and the DR priority of the neighbor.

Use **undo ospfv3 peer** to remove the configuration.

Syntax

ospfv3 peer *ipv6-address* [**cost** *cost-value* | **dr-priority** *priority*] [**instance** *instance-id*]

undo ospfv3 peer *ipv6-address* [**instance** *instance-id*]

Default

No link-local address is specified for the neighbor interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies the link-local IPv6 address of the neighbor.

cost *cost-value*: Specifies the cost of the neighbor, in the range of 1 to 65535.

dr-priority *priority*: Specifies the DR priority of the neighbor, in the range of 0 to 255. The default is 1.

instance *instance-id:* Specifies an instance by its ID in the range of 0 to 255. The default is 0.

Usage guidelines

For NBMA and P2MP interfaces (only when in unicast mode), you must specify the link-local IPv6 addresses of their neighbors because these interfaces cannot find neighbors through broadcasting hello packets. For NBMA interfaces, you can also specify DR priorities for their neighbors.

Examples

On VLAN-interface 10, specify the link-local address of its neighbor as FE80::1111.

```
<Switch> system-view
[Switch] interface vlan-interface 10
```

```
[Switch-Vlan-interface10] ospfv3 peer fe80::1111
```

9.1.40. ospfv3 timer dead

Use **ospfv3 timer dead** to set the OSPFv3 neighbor dead time.

Use **undo ospfv3 timer dead** to remove the configuration.

Syntax

ospfv3 timer dead *seconds* [**instance** *instance-id*]

undo ospfv3 timer dead [**instance** *instance-id*]

Default

The OSPFv3 neighbor dead time is 40 seconds for P2P and broadcast interfaces, and is 120 seconds for P2MP and NBMA interfaces.

Views

Interface view

Predefined user roles

network-admin

Parameters

seconds: Specifies the dead time in the range of 1 to 65535 seconds.

instance *instance-id*: Specifies an instance by its ID in the range of 0 to 255. The default is 0.

Usage guidelines

If an interface receives no hello packet from a neighbor within the dead time, the interface determines that the neighbor is down.

The dead time must be a minimum of four times the hello time and must be identical on interfaces attached to the same network segment.

Examples

Set the OSPFv3 neighbor dead time to 60 seconds for VLAN-interface 10.

```
<Switch> system-view
[Switch] interface vlan-interface 10
[Switch-Vlan-interface10] ospfv3 timer dead 60
```

Related commands

ospfv3 timer hello

9.1.41. ospfv3 timer hello

Use **ospfv3 timer hello** to set the hello interval for an interface.

Use **undo ospfv3 timer hello** to remove the configuration.

Syntax

ospfv3 timer hello *seconds* [**instance** *instance-id*]

undo ospfv3 timer hello [**instance** *instance-id*]

Default

The hello interval is 10 seconds for P2P and broadcast interfaces, and is 30 seconds for P2MP or NBMA interfaces.

Views

Interface view

Predefined user roles

network-admin

Parameters

seconds: Specifies the hello interval in the range of 1 to 65535 seconds.

instance *instance-id*: Specifies an instance by its ID in the range of 0 to 255. The default is 0.

Usage guidelines

The shorter the hello interval is, the faster the topology converges and the more resources are consumed. Make sure the hello interval on two neighboring interfaces is the same.

Examples

Set the hello interval to 20 seconds for VLAN-interface 10.

```
<Switch> system-view
[Switch] interface vlan-interface 10
[Switch-Vlan-interface10] ospfv3 timer hello 20
```

Related commands

ospfv3 timer dead

9.1.42. ospfv3 timer poll

Use **ospfv3 timer poll** to set the poll interval on an NBMA interface.

Use **undo ospfv3 timer poll** to remove the configuration.

Syntax

ospfv3 timer poll *seconds* [**instance** *instance-id*]

undo ospfv3 timer poll [**instance** *instance-id*]

Default

The poll interval is 120 seconds on an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

seconds: Specifies the poll interval in the range of 1 to 65535 seconds.

instance *instance-id*: Specifies an interface instance by its ID in the range of 0 to 255. The default is 0.

Usage guidelines

When an NBMA interface finds its neighbor is down, it sends hello packets at the poll interval.

The poll interval must be a minimum of four times the hello interval.

Examples

Set the poll interval on VLAN-interface 10 to 120 seconds.

```
<Switch> system-view
[Switch] interface vlan-interface 10
[Switch-Vlan-interface10] ospfv3 timer poll 120
```

Related commands

ospfv3 timer hello

9.1.43. ospfv3 timer retransmit

Use **ospfv3 timer retransmit** to set the LSA retransmission interval for an interface.

Use **undo ospfv3 timer retransmit** to remove the configuration.

Syntax

ospfv3 timer retransmit *seconds* [**instance** *instance-id*]

undo ospfv3 timer retransmit [**instance** *instance-id*]

Default

The interval is 5 seconds.

Views

Interface view

Predefined user roles

network-admin

Parameters

seconds: Specifies the LSA retransmission interval in the range of 1 to 3600 seconds.

instance *instance-id*: Specifies an instance by its ID in the range of 0 to 255. The default is 0.

Usage guidelines

After the device sends an LSA to its neighbor, it waits for an acknowledgment. If the device receives no acknowledgment after the LSA retransmission interval elapses, it will retransmit the LSA.

To avoid unnecessary retransmissions, set an appropriate retransmission interval. For example, you can set a large retransmission interval value on a low-speed link.

Examples

Set the LSA retransmission interval to 12 seconds on VLAN-interface10 in instance 1.

```
<Switch> system-view
[Switch] interface vlan-interface 10
[Switch-Vlan-interface10] ospfv3 timer retransmit 12 instance 1
```

9.1.44. ospfv3 trans-delay

Use **ospfv3 trans-delay** to set the transmission delay for an interface.

Use **undo ospfv3 trans-delay** to remove the configuration.

Syntax

ospfv3 trans-delay *seconds* [**instance** *instance-id*]

undo ospfv3 trans-delay [**instance** *instance-id*]

Default

The transmission delay is 1 second.

Views

Interface view

Predefined user roles

network-admin

Parameters

seconds: Specifies the transmission delay in the range of 1 to 3600 seconds.

instance *instance-id*: Specifies an instance by its ID in the range of 0 to 255. The default is 0.

Usage guidelines

Each LSA in the LSDB has an age that is incremented by 1 every second, but the age does not change during transmission. Adding a transmission delay into the age time is important in low speed networks.

Examples

Set the transmission delay to 3 seconds for VLAN-interface 10 in instance 1.

```
<Switch> system-view
[Switch] interface vlan-interface 10
[Switch-Vlan-interface10] ospfv3 trans-delay 3 instance 1
```

9.1.45. preference

Use **preference** to set a preference for OSPFv3 routes.

Use **undo preference** to remove the configuration.

Syntax

preference [**ase**] { *preference* | **route-policy** *route-policy-name* } *

undo preference [**ase**]

Default

The preference is 10 for OSPFv3 internal routes and 150 for OSPFv3 external routes.

Views

OSPFv3 view

Predefined user roles

network-admin

Parameters

ase: Specifies a preference for OSPFv3 external routes. If you do not specify this keyword, the command sets a preference for OSPFv3 internal routes.

preference: Specifies the preference value in the range of 1 to 255. A smaller value represents a higher preference.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters, to set a preference for matching routes.

Usage guidelines

If multiple routing protocols find multiple routes to the same destination, the router uses the route found by the protocol with the highest preference.

Examples

Set a preference of 150 for OSPFv3 routes.

```
<Switch> system-view
[Switch] OSPFv3
[Switch-OSPFv3-1] preference 150
```

9.1.46. reset ospfv3 process

Use **reset ospfv3 process** to restart OSPFv3 processes.

Syntax

reset ospfv3 [*process-id*] **process** [**graceful-restart**]

Views

User view

Predefined user roles

network-admin

Parameters

process-id: Specifies an OSPFv3 process by its ID in the range of 1 to 65535. If you do not specify this argument, the command restarts all OSPFv3 processes.

graceful-restart: Restarts the OSPFv3 process by using GR.

Usage guidelines

The **reset ospfv3 process** command performs the following actions:

- Clears all invalid LSAs without waiting for their timeouts.
- Starts a new DR/BDR election.
- Keeps previous OSPFv3 configurations.

The system prompts you to select whether to restart OSPFv3 process upon execution of this command.

Examples

Restart all OSPFv3 processes.

```
<Switch> reset ospfv3 process
Reset OSPFv3 process? [Y/N]:y
```

9.1.47. reset ospfv3 redistribution

Use **reset ospfv3 redistribution** to restart route redistribution.

Syntax

reset ospfv3 [*process-id*] **redistribution**

Views

User view

Predefined user roles

network-admin

Parameters

process-id: Specifies an OSPFv3 process by its ID in the range of 1 to 65535. If you do not specify this argument, the command restarts route redistribution for all OSPFv3 processes.

Examples

Restart route redistribution.

```
<Switch> reset ospfv3 redistribution
```

9.1.48. reset ospfv3 statistics

Use **reset ospfv3 statistics** to clear OSPFv3 statistics.

Syntax

reset ospfv3 [*process-id*] **statistics**

Views

User view

Predefined user roles

network-admin

Parameters

process-id: Specifies an OSPFv3 process by its ID in the range of 1 to 65535. If you do not specify this argument, the command clears statistics for all OSPFv3 processes.

Examples

Clear statistics for all OSPFv3 processes.

```
<Switch> reset ospfv3 statistics
```

9.1.49. router-id

Use **router-id** to configure a router ID.

Use **undo router-id** to restore the default.

Syntax

router-id *router-id*

undo router-id

Default

No router ID is configured.

Views

OSPFv3 view

Predefined user roles

network-admin

Parameters

router-id: Specifies a router ID in IPv4 address format.

Usage guidelines

The router ID is the unique identifier for the device to run OSPFv3 in the AS. An OSPFv3 process cannot run without a router ID.

You must specify a unique router ID for each OSPFv3 process in an AS and on a router.

Examples

Configure the router ID 10.1.1.3 for OSPFv3 process 1.

```
<Switch> system-view
[Switch] ospfv3 1
[Switch-ospfv3-1] router-id 10.1.1.3
```

Related commands

ospfv3

9.1.50. silent-interface(OSPFv3 view)

Use **silent-interface** to disable the specified interface from receiving and sending OSPFv3 packets.

Use **undo silent-interface** to remove the configuration.

Syntax

silent-interface { *interface-type interface-number* | **all** }

undo silent-interface { *interface-type interface-number* | **all** }

Default

An interface can receive and send OSPFv3 packets.

Views

OSPFv3 view

Predefined user roles

network-admin

Parameters

interface-type interface-number: Specifies an interface by its type and number.

all: Specifies all interfaces.

Usage guidelines

Multiple processes can disable the same interface from receiving and sending OSPFv3 packets. However, the **silent-interface** command takes effect only on interfaces enabled with the current process.

Examples

Disable VLAN-interface 10 from receiving and sending OSPFv3 packets in OSPFv3 processes 100 and 200.

```
<Switch> system-view
[Switch] ospfv3 100
[Switch-ospfv3-100] router-id 10.100.1.9
[Switch-ospfv3-100] silent-interface vlan-interface 10
[Switch-ospfv3-100] quit
[Switch] ospfv3 200
[Switch-ospfv3-200] router-id 20.100.1.9
[Switch-ospfv3-200] silent-interface vlan-interface 10
```

9.1.51. snmp-agent trap enable ospfv3

Use **snmp-agent trap enable ospfv3** to enable SNMP notifications for OSPFv3.

Use **undo snmp-agent trap enable ospfv3** to disable SNMP notifications for OSPFv3.

Syntax

snmp-agent trap enable ospfv3 [**grrestarter-status-change** | **grhelper-status-change** | **if-state-change** | **if-cfg-error** | **if-bad-pkt** | **neighbor-state-change** | **nssatranslator-status-change** | **virtif-bad-pkt** | **virtif-cfg-error** | **virtif-state-change** | **virtgrhelper-status-change** | **virtneighbor-state-change**] *

undo snmp-agent trap enable ospfv3 [**grrestarter-status-change** | **grhelper-status-change** | **if-state-change** | **if-cfg-error** | **if-bad-pkt** | **neighbor-state-change** | **nssatranslator-status-change** | **virtif-bad-pkt** | **virtif-cfg-error** | **virtif-state-change** | **virtgrhelper-status-change** | **virtneighbor-state-change**] *

Default

SNMP notifications for OSPFv3 are enabled.

Views

System view

Predefined user roles

network-admin

Parameters

grrestarter-status-change: Specifies notifications about GR restarter state changes.

grhelper-status-change: Specifies notifications about GR helper state changes.

if-state-change: Specifies notifications about interface state changes.

if-cfg-error: Specifies notifications about error configuration of an interface.

if-bad-pkt: Specifies notifications about error messages received on an interface.

neighbor-state-change: Specifies notifications about neighbor state changes.

nssatranslator-status-change: Specifies notifications about NSSA translator state changes.

virtif-bad-pkt: Specifies notifications about error messages received on a virtual interface.

virtif-cfg-error: Specifies notifications about error configuration of a virtual interface.

virtif-state-change: Specifies notifications about virtual interface state changes.

virtgrhelper-status-change: Specifies notifications about neighbor GR helper state changes of a virtual interface.

virtneighbor-state-change: Specifies notifications about the neighbor state changes of a virtual interface.

Examples

Disable SNMP notifications for OSPFv3.

```
<Switch> system-view
[Switch] undo snmp-agent trap enable ospfv3
```

9.1.52. spf-schedule-interval

Use **spf-schedule-interval** to set the OSPFv3 SPF calculation interval.

Use **undo spf-schedule-interval** to restore the default.

Syntax

spf-schedule-interval *maximum-interval* [*minimum-interval* [*incremental-interval*]]

undo spf-schedule-interval

Default

The maximum SPF calculation interval is 5 seconds, the minimum interval is 50 milliseconds, and the incremental interval is 200 milliseconds.

Views

OSPFv3 view

Predefined user roles

network-admin

Parameters

maximum-interval: Specifies the maximum OSPFv3 route calculation interval in the range of 1 to 60 seconds.

minimum-interval: Specifies the minimum OSPFv3 route calculation interval in the range of 10 to 60000 milliseconds.

incremental-interval: Specifies the incremental OSPFv3 route calculation interval in the range of 10 to 60000 milliseconds.

Usage guidelines

Based on the LSDB, an OSPFv3 router uses SPF to calculate a shortest path tree with itself being the root. OSPFv3 uses the shortest path tree to determine the next hop to a destination. By adjusting the SPF calculation interval, you can prevent overconsumption of bandwidth and router resources due to frequent topology changes.

For a stable network, the minimum interval is used. If network changes become frequent, the SPF calculation interval is incremented by the incremental interval × 2^{n-2} for each calculation until the maximum interval is reached. The value *n* is the number of calculation times.

The minimum interval and the incremental interval cannot be greater than the maximum interval.

Examples

Set the maximum SPF calculation interval to 10 seconds, minimum interval to 500 milliseconds, and incremental interval to 300 milliseconds.

```
<Switch> system-view
[Switch] ospfv3 100
[Switch-ospfv3-100] spf-schedule-interval 10 500 300
```

9.1.53. stub (OSPFv3 area view)

Use **stub** to configure an area as a stub area.

Use **undo stub** to restore the default.

Syntax

stub [**default-route-advertise-always** | **no-summary**] *

undo stub

Default

No area is configured as a stub area.

Views

OSPFv3 area view

Predefined user roles

network-admin

Parameters

default-route-advertise-always: Enables the ABR to always advertise a default route into the stub area.

no-summary: Enables the ABR to advertise only a default route in an Inter-Area-Prefix-LSA into the stub area. No AS-external-LSA, Inter-Area-Prefix-LSA, or other Inter-Area-Router-LSA is advertised in the area. The area is a totally stub area.

Usage guidelines

To remove the **no-summary** configuration on an ABR, execute the **stub** command again to overwrite it.

To configure an area as a stub area, execute the **stub** command on all routers attached to the area.

Examples

Configure OSPFv3 area 1 as a stub area.

```
<Switch> system-view
[Switch] ospfv3 1
[Switch-ospfv3-1] area 1
[Switch-ospfv3-1-area-0.0.0.1] stub
```

Related commands

default-cost (OSPFv3 area view)

9.1.54. vlink-peer (OSPFv3 area view)

Use **vlink-peer** to configure a virtual link.

Use **undo vlink-peer** to remove a virtual link.

Syntax

vlink-peer *router-id* [**dead** *seconds* | **hello** *seconds* | **instance** *instance-id* | **retransmit** *seconds* | **trans-delay** *seconds*] *

undo vlink-peer *router-id* [**dead** | **hello** | **retransmit** | **trans-delay**] *

Default

No virtual links exist.

Views

OSPFv3 area view

Predefined user roles

network-admin

Parameters

router-id: Specifies the router ID of the neighbor on the virtual link.

dead *seconds*: Specifies the dead interval in the range of 1 to 32768 seconds. The default is 40. The dead interval must be identical with that on the virtual link neighbor, and must be a minimum of four times the hello interval.

hello *seconds*: Specifies the hello interval in the range of 1 to 8192 seconds. The default is 10. It must be identical with the hello interval on the virtual link neighbor.

instance *instance-id*: Specifies the instance ID of a virtual link, in the range of 0 to 255. The default is 0.

retransmit *seconds*: Specifies the retransmission interval in the range of 1 to 3600 seconds. The default is 5.

trans-delay *seconds*: Specifies the transmission delay interval in the range of 1 to 3600 seconds. The default is 1.

Usage guidelines

You can configure a virtual link to maintain connectivity between a non-backbone area and the backbone, or maintain connectivity within the backbone. A virtual link is similar to an interface with OSPFv3 enabled. You can configure parameters such as **hello**, **dead**, **retransmit** and **trans-delay** for the virtual link.

Both ends of a virtual link must be ABRs that are configured with the **vlink-peer** command.

The following guidelines apply to parameters:

- The smaller the hello interval is, the faster the network converges, and the more network resources are consumed.
- For a low speed link, set a large retransmission interval to avoid unnecessary retransmissions.
- Specify a transmission delay with the **trans-delay** keyword depending on the interface delay.

OSPFv3 supports only the HMAC-SHA-256 authentication algorithm.

The ID of keys used for authentication can only be in the range of 0 to 65535.

Examples

Configure a virtual link to 10.10.0.3.

```
<Switch> system-view
[Switch] ospfv3 1
[Switch-ospfv3-1] area 1
[Switch-ospfv3-1-area-0.0.0.1] vlink-peer 10.10.0.3
```

Related commands

display ospfv3 vlink

Contents

A page of this section is **5-x-x**

10. IPv6 policy-based routing commands ····· 10-1
10.1. IPv6 policy-based routing commands ····· 10-1
10.1.1. apply next-hop ····· 10-1
10.1.2. display ipv6 policy-based-route ····· 10-2
10.1.3. display ipv6 policy-based-route interface ····· 10-3
10.1.4. display ipv6 policy-based-route setup ····· 10-4
10.1.5. if-match acl ····· 10-5
10.1.6. ipv6 policy-based-route (interface view) ····· 10-6
10.1.7. ipv6 policy-based-route (system view) ····· 10-7
10.1.8. reset ipv6 policy-based-route statistics ····· 10-8

10. IPv6 policy-based routing commands

10.1. IPv6 policy-based routing commands

10.1.1. apply next-hop

Use **apply next-hop** to set next hops.

Use **undo apply next-hop** to remove next hops.

Syntax

apply next-hop [**vpn-instance** *vpn-instance-name*] { *ipv6-address* [**direct**] [**track** *track-entry-number*] } &<1-2>

undo apply next-hop [[**vpn-instance** *vpn-instance-name*] *ipv6-address*&<1-2>]

Default

No next hop is set.

Views

IPv6 policy node view

Predefined user roles

network-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. The specified VPN instance must already exist.

ipv6-address: Specifies the IPv6 address of the next hop. If you do not specify the **vpn-instance** *vpn-instance-name* option or the **inbound-vpn** keyword, the next hop belongs to the public network.

direct: Specifies that the next hop must be directly connected to take effect.

track *track-entry-number*: Specifies a track entry by its number in the range of 1 to 1024.

&<1-2>: Indicates that the argument before it can be entered up to two times.

Usage guidelines

You can specify multiple next hops for backup in one command line or by executing this command multiple times.

With a next hop specified, the **undo apply next-hop** command removes the next hop.

Without any next hop specified, the **undo apply next-hop** command removes all next hops.

Examples

Set a directly-connected next hop of 1::1.

```
<Switch> system-view
[Switch] ipv6 policy-based-route aa permit node 11
[Switch-pbr6-aa-11] apply next-hop 1::1
```

10.1.2. display ipv6 policy-based-route

Use **display ipv6 policy-based-route** to display IPv6 PBR policy information.

Syntax

display ipv6 policy-based-route [**policy** *policy-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

policy *policy-name*: Specifies a policy by its name, a case-sensitive string of 1 to 19 characters. If you do not specify a policy, this command displays information for all IPv6 PBR policies.

Examples

Display all IPv6 policy information.

```
<Switch> display ipv6 policy-based-route
Policy name: aaa
  node 1 permit:
    if-match acl 2000
    apply next-hop 1000::1
```

Table 10-1 Command output

Field	Description
node 1 permit	The match mode of Node 1 is **permit**.
if-match acl	Compares IPv6 packets with IPv6 ACL.
apply next-hop	Specifies a next hop for permitted IPv6 packets.

Related commands

ipv6 policy-based-route (system view)

10.1.3. display ipv6 policy-based-route interface

Use **display ipv6 policy-based-route interface** to display IPv6 interface PBR configuration and statistics.

Syntax

display ipv6 policy-based-route interface *interface-type interface-number*

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number: Specifies an interface by its type and number.

Examples

Display IPv6 PBR configuration and statistics on VLAN-interface 2.

```
<Switch> display ipv6 policy-based-route interface vlan-interface 2
Policy based routing information for interface Vlan-inerface2(failed):
Policy name: aaa
  node 0 deny:
  Matched: 0
  node 1 permit:
    if-match acl 3999
  Matched: 0
  node 2 permit:
    if-match acl 2000
    apply next-hop 1000::1
  Matched: 0
  node 5 permit:
    if-match acl 3101
    apply next-hop 1000::1
  Matched: 0
Total matched: 0
<Switch> display ipv6 policy-based-route interface Vlan-inerface2
Policy based routing information for interface Vlan-inerface2:
Policy name: aaa
  node 0 deny(not support):
  Matched: 0
  node 1 permit:
    if-match acl 3999
  Matched: 0
```

```
  node 2 permit(no resource):
    if-match acl 2000
    apply next-hop 1000::1
  Matched: 0
  node 5 permit:
    if-match acl 3101
    apply next-hop 1000::1
  Matched: 0 (no statistics resource)
Total matched: 0
```

Table 10-2 Command output

Field	Description
Policy based routing information for interface *XXXX*(failed)	IPv6 PBR configuration and statistics on the interface. **failed** indicates the policy (including all its nodes) failed to be assigned to the driver. For a global interface (with only one-dimensional interface number, for example, VLAN-interface 10), **failed** can be displayed only when you specify the slot information for the command.
node 0 deny(not support) node 2 permit(no resource)	Match mode of the node, **permit** or **deny**. **not support** means the device does not support the match criteria configured on the node. **no resource** means the device has insufficient ACL resources, and failed to assign ACL resources to the node. For a global interface (with only one-dimensional interface number, for example, VLAN-interface 10), **not support** and **no resource** can be displayed only when you specify the slot information for the command.
if-match acl	Compares IPv6 packets with the IPv6 ACL.
apply next-hop	Specifies a next hop for permitted IPv6 packets.
Matched: 0 (no statistics resource)	Number of successful matches on the node (**no statistics resource** indicates insufficient statistics resources). For a global interface (with only one-dimensional interface number, for example, VLAN-interface 10), **no statistics resource** can be displayed only when you specify the slot information for the command.
Total matched	Total number of successful matches on all nodes.

Related commands

reset ipv6 policy-based-route statistics

10.1.4. display ipv6 policy-based-route setup

Use **display ipv6 policy-based-route setup** to display IPv6 PBR configuration.

Syntax

display ipv6 policy-based-route setup

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display IPv6 PBR configuration.

```
<Switch> display ipv6 policy-based-route setup
Policy name              Type              Interface
pr01                     Forward           Vlan-interface 2
pr02                     Local             N/A
```

Table 10-3 Command output

Field	Description
Policy name	Policy name.
Type	Type of the PBR: • **Forward**—Interface PBR. • **Local**—Local PBR.
Interface	Interface where the policy is applied.

Related commands

ipv6 policy-based-route (interface view)

10.1.5. if-match acl

Use **if-match acl** to set an ACL match criterion.

Use **undo if-match acl** to restore the default.

Syntax

if-match acl { *ipv6-acl-number* | **name** *ipv6-acl-name* }

undo if-match acl

Default

No ACL match criterion is set.

Views

IPv6 policy node view

Predefined user roles

network-admin

Parameters

ipv6-acl-number: Specifies an IPv6 ACL by its number in the range of 2000 to 3999. The value range of a basic ACL is 2000 to 2999 and that of an advanced ACL is 3000 to 3999.

name *ipv6-acl-name*: Specifies an IPv6 ACL by its name, a case-insensitive string of 1 to 63 characters starting with a letter. The ACL name cannot be **all**. For the command to take effect, make sure the specified IPv6 ACL is a basic or advanced ACL.

Examples

Configure Node 10 of policy **aa** to permit the packets matching ACL 2000.

```
<Switch> system-view
[Switch] ipv6 policy-based-route aa permit node 10
[Switch-pbr6-aa-10] if-match acl 2000
```

Configure Node 10 of policy **aa** to permit the packets matching ACL **aaa**.

```
<Switch> system-view
[Switch] ipv6 policy-based-route aa permit node 10
[Switch-pbr6-aa-10] if-match acl name aaa
```

10.1.6. ipv6 policy-based-route (interface view)

Use **ipv6 policy-based-route** to configure IPv6 interface PBR by applying an IPv6 policy to an interface.

Use **undo ipv6 policy-based-route** to restore the default.

Syntax

ipv6 policy-based-route *policy-name*

undo ipv6 policy-based-route

Default

No IPv6 is applied to an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

policy-name: Specifies a policy by its name, a case-sensitive string of 1 to 19 characters. The specified policy must already exist.

Examples

Apply policy **aaa** to VLAN-interface 2.

```
<Switch> system-view
[Switch] interface vlan-interface 2
```

```
[Switch-Vlan-interface2] ipv6 policy-based-route aaa
```

Related commands

display ipv6 policy-based-route setup

ipv6 policy-based-route (system view)

10.1.7. ipv6 policy-based-route (system view)

Use **ipv6 policy-based-route** to create an IPv6 policy node and enter its view, or enter the view of an existing IPv6 policy node.

Use **undo ipv6 policy-based-route** to delete an IPv6 policy or IPv6 policy node.

Syntax

ipv6 policy-based-route *policy-name* [**deny** | **permit**] **node** *node-number*

undo ipv6 policy-based-route *policy-name* [**deny** | **node** *node-number* | **permit**]

Default

No IPv6 policy nodes exist.

Views

System view

Predefined user roles

network-admin

Parameters

policy-name: Specifies a policy name, a case-sensitive string of 1 to 19 characters.

deny: Specifies the match mode for the policy node as **deny**.

permit: Specifies the match mode for the policy node as **permit** (default mode).

node *node-number*: Specifies the number of the IPv6 policy node. A smaller number has a higher priority. The value range for the *node-number* argument is 0 to 255.

Usage guidelines

To delete an IPv6 policy that has already applied to an interface, you must delete the policy from the interface first.

If a policy node is specified, the **undo ipv6 policy-based-route** command deletes the specified policy node. If a match mode is specified, the command deletes all nodes configured with the match mode. If no node is specified, the command deletes the whole policy.

Examples

Create permit-mode Node 10 for IPv6 policy **aaa** and enter its view.

```
<Switch> system-view
```

```
[Switch] ipv6 policy-based-route aaa permit node 10
[Switch-pbr6-aaa-10]
```

Related commands

display ipv6 policy-based-route

10.1.8. reset ipv6 policy-based-route statistics

Use **reset ipv6 policy-based-route statistics** to clear IPv6 PBR statistics.

Syntax

reset ipv6 policy-based-route statistics [**policy** *policy-name*]

Views

User view

Predefined user roles

network-admin

Parameters

policy *policy-name*: Specifies a policy by its name, a case-sensitive string of 1 to 19 characters. If you do not specify a policy, this command clears IPv6 PBR statistics for all policies.

Examples

Clear all IPv6 PBR statistics.

```
<Switch> reset ipv6 policy-based-route statistics
```

Related commands

display ipv6 policy-based-route interface

Contents

A page of this section is **5-x-x**

11. Routing policy commands ····· 11-1
11.1. Common routing policy commands ····· 11-1
11.1.1. apply as-path ····· 11-1
11.1.2. apply comm-list delete ····· 11-2
11.1.3. apply community ····· 11-2
11.1.4. apply cost ····· 11-4
11.1.5. apply cost-type ····· 11-4
11.1.6. apply extcommunity ····· 11-5
11.1.7. apply local-preference ····· 11-6
11.1.8. apply origin ····· 11-7
11.1.9. apply preference ····· 11-7
11.1.10. apply preferred-value ····· 11-8
11.1.11. apply tag ····· 11-9
11.1.12. display ip as-path ····· 11-9
11.1.13. display ip community-list ····· 11-10
11.1.14. display ip extcommunity-list ····· 11-11
11.1.15. display route-policy ····· 11-12
11.1.16. if-match as-path ····· 11-13
11.1.17. if-match community ····· 11-14
11.1.18. if-match cost ····· 11-15
11.1.19. if-match extcommunity ····· 11-15
11.1.20. if-match interface ····· 11-16
11.1.21. if-match route-type ····· 11-17
11.1.22. if-match tag ····· 11-18
11.1.23. ip as-path ····· 11-18
11.1.24. ip community-list ····· 11-19
11.1.25. ip extcommunity-list ····· 11-21
11.1.26. route-policy ····· 11-22
11.2. IPv4 routing policy commands ····· 11-23
11.2.1. apply ip-address next-hop ····· 11-23
11.2.2. display ip prefix-list ····· 11-24
11.2.3. if-match ip ····· 11-25
11.2.4. ip prefix-list ····· 11-26
11.2.5. reset ip prefix-list ····· 11-28
11.3. IPv6 routing policy commands ····· 11-28
11.3.1. apply ipv6 next-hop ····· 11-28
11.3.2. display ipv6 prefix-list ····· 11-29
11.3.3. if-match ipv6 ····· 11-30
11.3.4. ipv6 prefix-list ····· 11-31
11.3.5. reset ipv6 prefix-list ····· 11-33

11. Routing policy commands

11.1. Common routing policy commands

11.1.1. apply as-path

Use **apply as-path** to set the AS_PATH attribute for BGP routes.

Use **undo apply as-path** to restore the default.

Syntax

apply as-path *as-number*&<1-32> [**replace**]

undo apply as-path

Default

No AS_PATH attribute is set.

Views

Routing policy node view

Predefined user roles

network-admin

Parameters

as-number&<1-32>: Specifies an AS by its number in the range of 1 to 4294967295. &<1-32> indicates that you can specify a maximum of 32 AS numbers.

replace: Replaces the original AS numbers. If you do not specify this keyword, the command adds the specified AS numbers before the original AS_PATH attribute.

Examples

Configure node 10 in **permit** mode for routing policy **policy1** to add AS number 200 before the original AS_PATH attribute of BGP routes matching AS path list 1.

```
<Switch> system-view
[Switch] route-policy policy1 permit node 10
[Switch-route-policy-policy1-10] if-match as-path 1
[Switch-route-policy-policy1-10] apply as-path 200
```

Related commands

display ip as-path

if-match as-path

ip as-path

11.1.2. apply comm-list delete

Use **apply comm-list delete** to delete the COMMUNITY attributes from BGP routes.

Use **undo apply comm-list** to restore the default.

Syntax

apply comm-list { *comm-list-number* | *comm-list-name* } **delete**

undo apply comm-list

Default

No COMMUNITY attributes are deleted from BGP routes.

Views

Routing policy node view

Predefined user roles

network-admin

Parameters

comm-list-number: Specifies a basic community list by its number in the range of 1 to 99 or an advanced community list by its number in the range of 100 to 199.

comm-list-name: Specifies a community list by its name, a case-sensitive string of 1 to 63 characters that cannot contain only numbers.

Examples

Configure node 10 in **permit** mode for routing policy **policy1** to delete the COMMUNITY attributes specified in community list 1 from BGP routes.

```
<Switch> system-view
[Switch] route-policy policy1 permit node 10
[Switch-route-policy-policy1-10] apply comm-list 1 delete
```

Related commands

ip community-list

11.1.3. apply community

Use **apply community** to set the COMMUNITY attribute for BGP routes.

Use **undo apply community** to remove the specified COMMUNITY attribute for BGP routes.

Syntax

apply community { **none** | **additive** | { *community-number*&<1-32> | *aa:nn*&<1-32> | **internet** | **no-advertise** | **no-export** | **no-export-subconfed** } * [**additive**] }

undo apply community [**none** | **additive** | { *community-number*&<1-32> | *aa:nn*&<1-32> | **internet** | **no-advertise** | **no-export** | **no-export-subconfed** } * [**additive**]]

Default

No COMMUNITY attribute is set for BGP routes.

Views

Routing policy node view

Predefined user roles

network-admin

Parameters

none: Removes the COMMUNITY attributes of BGP routes.

community-number&<1-32>: Specifies a community sequence number in the range of 1 to 4294967295. &<1-32> indicates that you can specify a maximum of 32 community sequence numbers.

aa:nn&<1-32>: Specifies a community number. Both *aa* and *nn* are in the range of 0 to 65535. &<1-32> indicates that you can specify a maximum of 32 community numbers.

internet: Sets the INTERNET community attribute for BGP routes. Routes with this attribute can be advertised to all BGP peers. By default, all routes have this attribute.

no-advertise: Sets the NO_ADVERTISE community attribute for BGP routes. Routes with this attribute cannot be advertised to any peers.

no-export: Sets the NO_EXPORT community attribute for BGP routes. Routes with this attribute cannot be advertised out of the AS or confederation, but can be advertised to other sub-ASs in the confederation.

no-export-subconfed: Sets the NO_EXPORT_SUBCONFED community attribute for BGP routes. Routes with this attribute cannot be advertised out of the local AS or to other sub-ASs in the confederation.

additive: Adds the specified COMMUNITY attribute to the original COMMUNITY attribute of BGP routes.

Examples

Configure node 16 in **permit** mode for routing policy **setcommunity** to set the NO_EXPORT community attribute for BGP routes.

```
<Switch> system-view
[Switch] route-policy setcommunity permit node 16
[Switch-route-policy-setcommunity-16] apply community no-export
```

Related commands

if-match community

ip community-list

11.1.4. apply cost

Use **apply cost** to set a cost for routes.

Use **undo apply cost** to restore the default.

Syntax

apply cost [**+** | **-**] *cost-value*

undo apply cost

Default

No cost is set for routes.

Views

Routing policy node view

Predefined user roles

network-admin

Parameters

+: Increases a cost value.

-: Decreases a cost value.

cost-value: Specifies a cost in the range of 0 to 4294967295.

Examples

Configure node 10 in **permit** mode for routing policy **policy1** to set a cost of 120 for OSPF external routes.

```
<Switch> system-view
[Switch] route-policy policy1 permit node 10
[Switch-route-policy-policy1-10] if-match route-type external-type1or2
[Switch-route-policy-policy1-10] apply cost 120
```

11.1.5. apply cost-type

Use **apply cost-type** to set a cost type for routes.

Use **undo apply cost-type** to restore the default.

Syntax

apply cost-type { **internal** | **type-1** | **type-2** }

undo apply cost-type

Default

No cost type is set for routes.

Views

Routing policy node view

Predefined user roles

network-admin

Parameters

internal: Sets the MED value for a matching BGP route to the IGP metric of the route's next hop.

type-1: Sets the cost type to OSPF Type-1 external route.

type-2: Sets the cost type to OSPF Type-2 external route.

Usage guidelines

The **apply cost-type internal** command sets the MED for a matching BGP route learned from an IBGP peer to the IGP metric of the route's next hop. The MED is modified when BGP advertises the route to an EBGP peer.

Examples

Configure node 10 in **permit** mode for routing policy **policy1** to set the cost type for routes that have a tag of 8 to OSPF Type-1 external routes.

```
<Switch> system-view
[Switch] route-policy policy1 permit node 10
[Switch-route-policy-policy1-10] if-match tag 8
[Switch-route-policy-policy1-10] apply cost-type type-1
```

11.1.6. apply extcommunity

Use **apply extcommunity** to set the extended community attribute for BGP routes.

Use **undo apply extcommunity** to remove the extended community attribute for BGP routes.

Syntax

apply extcommunity { **rt** *route-target* }&<1-32> [**additive**]

undo apply extcommunity [{ **rt** *route-target* }&<1-32>]

Default

No extended community attribute is set for BGP routes.

Views

Routing policy node view

Predefined user roles

network-admin

Parameters

{ **rt** *route-target* }&<1-32>: Sets the RT extended community attribute, a string of 3 to 21 characters. &<1-32> indicates that you can specify a maximum of 32 RT extended community attributes.

An RT attribute has the following forms:

- *16-bit AS number*:*32-bit self-defined number*. For example, 101:3. The AS number is in the range of 0 to 65535, and the self-defined number is in the range of 0 to 4294967295.
- *32-bit IP address*:*16-bit self-defined number*. For example, 192.168.122.15:1. The self-defined number is in the range of 0 to 65535.
- *32-bit AS number*:*16-bit self-defined number*. For example, 70000:3. The AS number is in the range of 65536 to 4294967295, and the self-defined number is in the range of 0 to 65535.

additive: Adds the specified attribute to the original extended community attribute.

Examples

Configure node 10 in **permit** mode for routing policy **policy1** to add the RT extended community attribute 100:2 to BGP routes matching AS path list 1.

```
<Switch> system-view
[Switch] route-policy policy1 permit node 10
[Switch-route-policy-policy1-10] if-match as-path 1
[Switch-route-policy-policy1-10] apply extcommunity rt 100:2 additive
```

11.1.7. apply local-preference

Use **apply local-preference** to set a local preference for BGP routes.

Use **undo apply local-preference** to restore the default.

Syntax

apply local-preference *preference*

undo apply local-preference

Default

No local preference is set for BGP routes.

Views

Routing policy node view

Predefined user roles

network-admin

Parameters

preference: Specifies a local preference in the range of 0 to 4294967295.

Examples

Configure node 10 in **permit** mode for routing policy **policy1** to set a local preference of 130 for BGP routes matching AS path list 1.

```
<Switch> system-view
[Switch] route-policy policy1 permit node 10
[Switch-route-policy-policy1-10] if-match as-path 1
[Switch-route-policy-policy1-10] apply local-preference 130
```

11.1.8. apply origin

Use **apply origin** to set the ORIGIN attribute for BGP routes.

Use **undo apply origin** to restore the default.

Syntax

apply origin { **egp** *as-number* | **igp** | **incomplete** }

undo apply origin

Default

No ORIGIN attribute is set for BGP routes.

Views

Routing policy node view

Predefined user roles

network-admin

Parameters

egp *as-number*: Sets the ORIGIN attribute to EGP. The *as-number* argument specifies an AS number in the range 1 to 4294967295 for EGP routes.

igp: Sets the ORIGIN attribute to IGP.

incomplete: Sets the ORIGIN attribute to UNKNOWN.

Examples

Configure node 10 in **permit** mode for routing policy **policy1** to set the ORIGIN attribute to IGP for BGP routes matching AS path list 1.

```
<Switch> system-view
[Switch] route-policy policy1 permit node 10
[Switch-route-policy-policy1-10] if-match as-path 1
[Switch-route-policy-policy1-10] apply origin igp
```

11.1.9. apply preference

Use **apply preference** to set a preference for a routing protocol.

Use **undo apply preference** to restore the default.

Syntax

apply preference *preference*

undo apply preference

Default

No preference is set for a routing protocol.

Views

Routing policy node view

Predefined user roles

network-admin

Parameters

preference: Specifies a preference in the range of 1 to 255.

Usage guidelines

If you have set preferences for routing protocols by using the **preference** command, the **apply preference** command sets a new preference for the matching routing protocol. Unmatched routing protocols still use the preferences set by using the **preference** command.

Examples

Configure node 10 in **permit** mode for routing policy **policy1** to set the preference for OSPF external routes to 90.

```
<Switch> system-view
[Switch] route-policy policy1 permit node 10
[Switch-route-policy-policy1-10] if-match route-type external-type1or2
[Switch-route-policy-policy1-10] apply preference 90
```

11.1.10. apply preferred-value

Use **apply preferred-value** to set a preferred value for BGP routes.

Use **undo apply preferred-value** to restore the default.

Syntax

apply preferred-value *preferred-value*

undo apply preferred-value

Default

No preferred value is set for BGP routes.

Views

Routing policy node view

Predefined user roles

network-admin

Parameters

preferred-value: Specifies a preferred value in the range of 0 to 65535.

Examples

Configure node 10 in **permit** mode for routing policy **policy1** to set a preferred value of 66 for BGP routes matching AS path list 1.

```
<Switch> system-view
[Switch] route-policy policy1 permit node 10
[Switch-route-policy-policy1-10] if-match as-path 1
[Switch-route-policy-policy1-10] apply preferred-value 66
```

11.1.11. apply tag

Use **apply tag** to set a tag for IGP routes.

Use **undo apply tag** to restore the default.

Syntax

apply tag *tag-value*

undo apply tag

Default

No routing tag is set for IGP routes.

Views

Routing policy node view

Predefined user roles

network-admin

Parameters

tag-value: Specifies the tag value in the range of 0 to 4294967295.

Examples

Configure node 10 in **permit** mode for routing policy **policy1** to set a tag of 100 for IGP routes.

```
<Switch> system-view
[Switch] route-policy policy1 permit node 10
[Switch-route-policy-policy1-10] apply tag 100
```

11.1.12. display ip as-path

Use **display ip as-path** to display BGP AS path list information.

Syntax

display ip as-path [*as-path-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

as-path-number: Specifies an AS path list by its number in the range of 1 to 256. If you do not specify this argument, the command displays information about all BGP AS path lists.

Examples

Display information about BGP AS path list 1.

```
<Switch> display ip as-path 1
ListID    Mode      Expression
1         Permit    2
```

Table 11-1 Command output

Field	Description
ListID	AS path list ID.
Mode	Match mode: • **Permit**. • **Deny**.
Expression	Regular expression used to match routes.

11.1.13. display ip community-list

Use **display ip community-list** to display BGP community list information.

Syntax

display ip community-list [*basic-community-list-number* | *adv-community-list-number* | **name** *comm-list-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

basic-community-list-number: Specifies a basic community list by its number in the range of 1 to 99.

adv-community-list-number: Specifies an advanced community list by its number in the range of 100 to 199.

name *comm-list-name*: Specifies a community list by its name, a case-sensitive string of 1 to 63 characters that cannot contain only numbers.

Usage guidelines

If no community list is specified, this command displays information about all BGP community lists.

Examples

Display information about all BGP community lists.

```
<Switch> display ip community-list
Community List Basic aaa
        Permit
Community List Advanced bbb
        Permit  3333
```

Table 11-2 Command output

Field	Description
Community List Basic	Basic community list.
Community List Advanced	Advanced community list.
permit	Match mode: • **Permit**. • **Deny**.

11.1.14. display ip extcommunity-list

Use **display ip extcommunity-list** to display BGP extended community list information.

Syntax

display ip extcommunity-list [*ext-comm-list-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ext-comm-list-number: Specifies an extended community list by its number in the range of 1 to 199. If you do not specify this argument, the command displays information about all BGP extended community lists.

Examples

Display information about BGP extended community list 1.

```
<Switch> display ip extcommunity-list 1
Extended Community List Number 1
         Permit rt: 9:6
         Permit soo: 9:6
```

Table 11-3 Command output

Field	Description
Extended Community List Number	Extended community list.
permit	Match mode: • **Permit**. • **Deny**.
rt	Route Target (RT) extended community attribute.
soo	Site of Origin (SoO) extended community attribute.

11.1.15. display route-policy

Use **display route-policy** to display routing policy information.

Syntax

display route-policy [**name** *route-policy-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

name *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters. If you do not specify this option, the command displays information about all routing policies.

Examples

Display information about routing policy **policy1**.

```
<Switch> display route-policy name policy1
```

```
Route-policy: policy1
  Permit : 1
          if-match cost 10
          continue: next node 11
          apply preference 10
```

Table 11-4 Command output

Field	Description
Route-policy	Routing policy name.
permit	Match mode: • **Permit**. • **Deny**.
if-match	Match criterion.
continue	Specify the next node to be matched.
apply	Action.

11.1.16. if-match as-path

Use **if-match as-path** to match BGP routes whose AS_PATH attribute matches a specified AS path list.

Use **undo if-match as-path** to remove the specified AS path list match criterion.

Syntax

if-match as-path *as-path-number*&<1-32>

undo if-match as-path [*as-path-number*&<1-32>]

Default

No AS path list match criterion is configured.

Views

Routing policy node view

Predefined user roles

network-admin

Parameters

as-path-number&<1-32>: Specifies an AS path list by its number in the range of 1 to 256. &<1-32> indicates that you can specify a maximum of 32 AS path lists.

Examples

Configure AS path list 2 to permit BGP routes containing AS number 200 or 300 to pass. Configure node 10 in **permit** mode for routing policy **test** to match AS path list 2.

```
<Switch> system-view
[Switch] ip as-path 2 permit _*200.*300
```

```
[Switch] route-policy test permit node 10
[Switch-route-policy-policy1-10] if-match as-path 2
```

Related commands

apply as-path

ip as-path

11.1.17. if-match community

Use **if-match community** to match BGP routes whose COMMUNITY attribute matches a specified community list.

Use **undo if-match community** to remove the specified community list match criterion.

Syntax

if-match community { { *basic-community-list-number* | **name** *comm-list-name* } [**whole-match**] | *adv-community-list-number* }&<1-32>

undo if-match community [{ *basic-community-list-number* | **name** *comm-list-name* } [**whole-match**] | *adv-community-list-number*]&<1-32>

Default

No community list match criterion is configured.

Views

Routing policy node view

Predefined user roles

network-admin

Parameters

basic-community-list-number: Specifies a basic community list by its number in the range of 1 to 99.

adv-community-list-number: Specifies an advanced community list by its number in the range of 100 to 199.

comm-list-name: Specifies a community list by its name, a case-sensitive string of 1 to 63 characters that cannot contain only numbers.

whole-match: Exactly matches the specified community list. All of the communities and only those communities specified must be present.

&<1-32>: Indicates that you can specify a maximum of 32 community lists.

Examples

Configure community list 1 to permit BGP routes with community number 100 or 200. Then configure node 10 in **permit** mode for routing policy **test** to use community list 1 to match BGP routes.

```
<Switch> system-view
[Switch] ip community-list 1 permit 100 200
[Switch] route-policy test permit node 10
[Switch-route-policy-test-10] if-match community 1
```

Related commands

apply community

ip community-list

11.1.18. if-match cost

Use **if-match cost** to match routes that have the specified cost.

Use **undo if-match cost** to restore the default.

Syntax

if-match cost *cost-value*

undo if-match cost

Default

No cost match criterion is configured.

Views

Routing policy node view

Predefined user roles

network-admin

Parameters

cost-value: Specifies a cost in the range of 0 to 4294967295.

Examples

Configure node 10 in **permit** mode for routing policy **policy1** to permit routes with a cost of 8.

```
<Switch> system-view
[Switch] route-policy policy1 permit node 10
[Switch-route-policy-policy1-10] if-match cost 8
```

11.1.19. if-match extcommunity

Use **if-match extcommunity** to match BGP routes whose extended community attribute matches a specified extended community list.

Use **undo if-match extcommunity** to remove the specified extended community list match criterion.

Syntax

if-match extcommunity *ext-comm-list-number*&<1-32>

undo if-match extcommunity [*ext-comm-list-number*&<1-32>]

Default

No extended community list match criterion is configured.

Views

Routing policy node view

Predefined user roles

network-admin

Parameters

ext-comm-list-number&<1-32>: Specifies an extended community list by its number in the range of 1 to 199. &<1-32> indicates that you can specify a maximum of 32 extended community lists.

Examples

Configure node 10 in **permit** mode for routing policy **policy1** to match BGP routes whose extended community attribute matches extended community lists 100 and 150.

```
<Switch> system-view
[Switch] ip extcommunity-list 100 permit rt 100:100
[Switch] ip extcommunity-list 150 permit rt 150:150
[Switch] route-policy policy1 permit node 10
[Switch-route-policy-policy1-10] if-match extcommunity 100 150
```

Related commands

apply extcommunity

ip extcommunity-list

11.1.20. if-match interface

Use **if-match interface** to match routes that have the specified output interfaces.

Use **undo if-match interface** to remove the specified output interface match criterion.

Syntax

if-match interface { *interface-type interface-number* }&<1-16>

undo if-match interface [*interface-type interface-number*]&<1-16>

Default

No output interface match criterion is configured.

Views

Routing policy node view

Predefined user roles

network-admin

Parameters

interface-type interface-number: Specifies an interface by its type and number.

&<1-16>: Indicates that you can specify a maximum of 16 interfaces.

Usage guidelines

BGP does not support criteria for matching the output interfaces of routes.

Examples

Configure node 10 in **permit** mode for routing policy **policy1** to permit routes with the output interface VLAN-interface 1.

```
<Switch> system-view
[Switch] route-policy policy1 permit node 10
[Switch-route-policy-policy1-10] if-match interface vlan-interface 1
```

11.1.21. if-match route-type

Use **if-match route-type** to set a route-type match criterion.

Use **undo if-match route-type** to remove the specified route-type match criterion.

Syntax

if-match route-type { **external-type1** | **external-type1or2** | **external-type2** | **internal** | **nssa-external-type1** | **nssa-external-type1or2** | **nssa-external-type2** } *

undo if-match route-type [**external-type1** | **external-type1or2** | **external-type2** | **internal** | **nssa-external-type1** | **nssa-external-type1or2** | **nssa-external-type2**] *

Default

No route-type match criterion is set.

Views

Routing policy node view

Predefined user roles

network-admin

Parameters

external-type1: Matches OSPF Type 1 external routes.

external-type1or2: Matches OSPF Type 1 and Type 2 external routes.

external-type2: Matches OSPF Type 2 external routes.

internal: Matches OSPF internal routes (including OSPF intra-area and inter-area routes).

nssa-external-type1: Matches OSPF NSSA Type 1 external routes.

nssa-external-type1or2: Matches OSPF NSSA Type 1 and 2 external routes.

nssa-external-type2: Matches OSPF NSSA Type 2 external routes.

Examples

Configure node 10 in **permit** mode for routing policy **policy1** to match OSPF internal routes.

```
<Switch> system-view
[Switch] route-policy policy1 permit node 10
[Switch-route-policy-policy1-10] if-match route-type internal
```

11.1.22. if-match tag

Use **if-match tag** to match IGP routes that have the specified tag.

Use **undo if-match tag** to restore the default.

Syntax

if-match tag *tag-value*

undo if-match tag

Default

No tag match criterion is configured.

Views

Routing policy node view

Predefined user roles

network-admin

Parameters

tag-value: Specifies a tag in the range of 0 to 4294967295.

Examples

Configure node 10 in **permit** mode for routing policy **policy1** to match IGP routes that have a tag of 8.

```
<Switch> system-view
[Switch] route-policy policy1 permit node 10
[Switch-route-policy-policy1-10] if-match tag 8
```

11.1.23. ip as-path

Use **ip as-path** to configure an AS path list.

Use **undo ip as-path** to remove an AS path list.

Syntax

ip as-path *as-path-number* { **deny** | **permit** } *regular-expression*

undo ip as-path *as-path-number* [*regular-expression* | **deny** | **permit**]

Default

No AS path lists exist.

Views

System view

Predefined user roles

network-admin

Parameters

as-path-number: Specifies an AS path list number in the range of 1 to 256.

deny: Specifies the match mode for the AS path list as **deny**.

permit: Specifies the match mode for the AS path list as **permit**.

regular-expression: Specifies an AS path regular expression, a string of 1 to 63 characters.

Usage guidelines

BGP routing updates contain an AS_PATH attribute field that identifies the ASs through which the routes have passed. An AS path regular expression, for example, ^200.*100$, matches the AS_PATH attribute that starts with AS 200 and ends with AS 100. For more information about regular expressions, see *Fundamentals Configuration Guide*.

Examples

Configure AS path list 1 to permit routes whose AS_PATH attribute starts with 10.

```
<Switch> system-view
[Switch] ip as-path 1 permit ^10
```

Related commands

apply as-path

display ip as-path

if-match as-path

11.1.24. ip community-list

Use **ip community-list** to configure a community list.

Use **undo ip community-list** to remove a community list.

Syntax

ip community-list { *basic-comm-list-num* | **basic** *basic-comm-list-name* } { **deny** | **permit** } [*community-number*&<1-32> | *aa:nn*&<1-32>] [**internet** | **no-advertise** | **no-export** | **no-export-subconfed**] *

undo ip community-list { *basic-comm-list-num* | **basic** *basic-comm-list-name* } [**deny** | **permit**] [*community-number*&<1-32> | *aa:nn*&<1-32>] [**internet** | **no-advertise** | **no-export** | **no-export-subconfed**] *

ip community-list { *adv-comm-list-num* | **advanced** *adv-comm-list-name* } { **deny** | **permit** } *regular-expression*

undo ip community-list { *adv-comm-list-num* | **advanced** *adv-comm-list-name* } [**deny** | **permit**] [*regular-expression*]

Default

No community lists exist.

Views

System view

Predefined user roles

network-admin

Parameters

basic-comm-list-num: Specifies a basic community list number in the range of 1 to 99.

basic *basic-comm-list-name*: Specifies a basic community list name, a case-sensitive string of 1 to 63 characters that cannot contain only numbers.

advanced *adv-comm-list-name*: Specifies an advanced community list name, a case-sensitive string of 1 to 63 characters that cannot contain only numbers.

adv-comm-list-num: Specifies an advanced community list number in the range of 100 to 199.

regular-expression: Specifies a regular expression for the advanced community list, a string of 1 to 63 characters. For more information about regular expressions, see *Fundamentals Configuration Guide*.

deny: Specifies the match mode for the community list as **deny**.

permit: Specifies the match mode for the community list as **permit**.

community-number&<1-32>: Specifies a community sequence number in the range of 1 to 4294967295. &<1-32> indicates that you can specify a maximum of 32 community sequence numbers.

aa:nn&<1-32>: Specifies a community number. Both *aa* and *nn* are in the range of 0 to 65535. &<1-32> indicates that you can specify a maximum of 32 community numbers.

internet: Specifies the INTERNET community attribute. Routes with this attribute can be advertised to all BGP peers. By default, all routes have this attribute.

no-advertise: Specifies the NO_ADVERTISE community attribute. Routes with this attribute cannot be advertised to other BGP peers.

no-export: Specifies the NO_EXPORT community attribute. Routes with this attribute cannot be advertised out of the local AS or the local confederation but can be advertised to other ASs in the confederation.

no-export-subconfed: Specifies the NO_EXPORT_SUBCONFED community attribute. Routes with this attribute cannot be advertised out of the local AS, or to other sub-ASs in the local confederation.

Examples

Configure basic community list 1 to permit routes with the INTERNET community attribute.

```
<Switch> system-view
[Switch] ip community-list 1 permit internet
```

Configure advanced community list 100 to permit routes with the COMMUNITY attribute starting with 10.

```
<Switch> system-view
[Switch] ip community-list 100 permit ^10
```

Related commands

apply comm-list delete

apply community

display ip community-list

if-match community

11.1.25. ip extcommunity-list

Use **ip extcommunity-list** to configure an extended community list.

Use **undo ip extcommunity-list** to remove an extended community list.

Syntax

ip extcommunity-list *ext-comm-list-number* { **deny** | **permit** } { **rt** *route-target* }&<1-32>

undo ip extcommunity-list *ext-comm-list-number* [{ **deny** | **permit** } [**rt** *route-target*]&<1-32>]

Default

No extended community lists exist.

Views

System view

Predefined user roles

network-admin

Parameters

ext-comm-list-number: Specifies an extended community list number in the range of 1 to 199.

deny: Specifies the match mode for the extended community list as **deny**.

permit: Specifies the match mode for the extended community list as **permit**.

rt *route-target*: Specifies a space-separated list of up to 32 RT extended community attribute items. Each item is a string of 3 to 21 characters.

An RT attribute has the following forms:

- *16-bit AS number*:*32-bit self-defined number*. For example, 101:3. The AS number is in the range of 0 to 65535, and the self-defined number is in the range of 0 to 4294967295.
- *32-bit IP address*:*16-bit self-defined number*. For example, 192.168.122.15:1. The self-defined number is in the range of 0 to 65535.
- *32-bit AS number*:*16-bit self-defined number*. For example, 70000:3. The AS number is in the range of 65536 to 4294967295, and the self-defined number is in the range of 0 to 65535.

Examples

Configure extended community list 1 to permit routes with RT 200:200 to pass.

```
<Switch> system-view
[Switch] ip extcommunity-list 1 permit rt 200:200
```

Related commands

apply extcommunity

display ip extcommunity-list

if-match extcommunity

11.1.26. route-policy

Use **route-policy** to create a routing policy and a node and enter routing policy node view, or enter the view of an existing routing policy node.

Use **undo route-policy** to remove a routing policy or a node of it.

Syntax

route-policy *route-policy-name* { **deny** | **permit** } **node** *node-number*

undo route-policy *route-policy-name* [**deny** | **permit**] [**node** *node-number*]

Default

No routing policies exist.

Views

System view

Predefined user roles

network-admin

Parameters

route-policy-name: Specifies a routing policy name, a case-sensitive string of 1 to 63 characters.

deny: Specifies the deny match mode for the routing policy node. If a route matches all the **if-match** clauses of the node, it is denied without being compared with the next node. If a route does not match any **if-match** clauses of the node, the route is compared with the next node.

permit: Specifies the permit match mode for the routing policy node. If a route matches all the **if-match** clauses of the node, it is handled by the **apply** clauses of the node. If a route does not match any **if-match** clauses of the node, the route is compared with the next node.

node *node-number*: Specifies a node number in the range of 0 to 65535. A node with a smaller number is matched first.

Usage guidelines

Use a routing policy to filter routing information. A routing policy can contain several nodes and each node contains a set of **if-match** and **apply** clauses. The **if-match** clauses define the match criteria of the node and the **apply** clauses define the actions to be taken on packets matching the criteria. The relation between the **if-match** clauses of a node is logical AND. All the **if-match** clauses must be met. The relation between nodes is logical OR. A packet passing a node passes the routing policy. If a packet does not pass any nodes, the packet does not pass the routing policy.

Examples

Create node 10 in **permit** mode for routing policy **policy1** and enter routing policy node view.

```
<Switch> system-view
[Switch] route-policy policy1 permit node 10
[Switch-route-policy-policy1-10]
```

Related commands

display route-policy

11.2. IPv4 routing policy commands

11.2.1. apply ip-address next-hop

Use **apply ip-address next-hop** to set a next hop for IPv4 routes.

Use **undo apply ip-address next-hop** to restore the default.

Syntax

apply ip-address next-hop *ip-address* [**public** | **vpn-instance** *vpn-instance-name*]

undo apply ip-address next-hop

Default

No next hop is set for IPv4 routes.

Views

Routing policy node view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the next hop IP address.

public: Specifies the public network.

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

If you use this command to set a next hop for redistributed routes, the configuration does not take effect.

If you do not specify the **public** keyword and the **vpn-instance** *vpn-instance-name* option, the next hop belongs to the public network.

Examples

Configure node 10 in **permit** mode for routing policy **policy1** to set next hop 193.1.1.8 for routes matching prefix list 100.

```
<Switch> system-view
[Switch] ip prefix-list 100 permit 192.168.10.1 24
[Switch] route-policy policy1 permit node 10
[Switch-route-policy-policy1-10] if-match ip address prefix-list 100
[Switch-route-policy-policy1-10] apply ip-address next-hop 193.1.1.8
```

11.2.2. display ip prefix-list

Use **display ip prefix-list** to display IPv4 prefix list statistics.

Syntax

display ip prefix-list [**name** *prefix-list-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

name *prefix-list-name*: Specifies an IP prefix list by its name, a case-sensitive string of 1 to 63 characters. If you do not specify this option, the command displays statistics for all IPv4 prefix lists.

Examples

Display the statistics for IPv4 prefix list **abc**.

```
<Switch> display ip prefix-list name abc
Prefix-list: abc
 Permitted 0
 Denied 0
        index: 10        Deny   6.6.6.0/24              ge  26  le  28
```

Table 11-5 Command output

Field	Description
Prefix-list	Name of the IPv4 prefix list.
Permitted	Number of routes matching the criterion.
Denied	Number of routes not matching the criterion.
index	Index of an item.
deny	Match mode of the item: • **Permit**. • **Deny**.
6.6.6.0/24	IP address and mask.
ge	Greater-equal, the lower mask length limit.
le	Less-equal, the upper mask length limit.

Related commands

ip prefix-list

reset ip prefix-list

11.2.3. if-match ip

Use **if-match ip** to match IPv4 routes whose destination, next hop, or source address matches an ACL or IPv4 prefix list.

Use **undo if-match ip** to remove the specified ACL or IPv4 prefix list match criterion.

Syntax

if-match ip { **address** | **next-hop** | **route-source** } { **acl** *ipv4-acl-number* | **prefix-list** *prefix-list-name* }

undo if-match ip { **address** | **next-hop** | **route-source** } [**acl** | **prefix-list**]

Default

No ACL or IPv4 prefix list match criterion is configured.

Views

Routing policy node view

Predefined user roles

network-admin

Parameters

address: Matches the destination address of IPv4 routes.

next-hop: Matches the next hop of IPv4 routes.

route-source: Matches the source address of BGP routes. This keyword corresponds to the **Neighbor** field in the output from the **display ip routing-table verbose** command.

acl *ipv4-acl-number*: Specifies an ACL by its number. The value range for the *ipv4-acl-number* argument is 2000 to 3999 for the **address** keyword, and 2000 to 2999 for the **next-hop** keyword and **route-source** keyword.

prefix-list *prefix-list-name*: Specifies an IP prefix list by its name, a case-sensitive string of 1 to 63 characters.

Examples

Configure node 10 of routing policy **policy1** to match IPv4 routes whose next hop matches IP prefix list **p1**.

```
<Switch> system-view
[Switch] route-policy policy1 permit node 10
[Switch-route-policy-policy1-10] if-match ip next-hop prefix-list p1
```

11.2.4. ip prefix-list

Use **ip prefix-list** to configure an IPv4 prefix list or an item for the list.

Use **undo ip prefix-list** to remove an IPv4 prefix list or an item of it.

Syntax

ip prefix-list *prefix-list-name* [**index** *index-number*] { **deny** | **permit** } *ip-address mask-length* [**greater-equal** *min-mask-length*] [**less-equal** *max-mask-length*]

undo ip prefix-list *prefix-list-name* [**index** *index-number*]

Default

No IPv4 prefix lists exist.

Views

System view

Predefined user roles

network-admin

Parameters

prefix-list-name: Specifies an IPv4 prefix list name, a case-sensitive string of 1 to 63 characters.

index *index-number*: Specifies an index number for an IPv4 prefix list item, in the range of 1 to 65535. An item with a smaller index number is matched first. If you do not specify this option, the index number starts from 10 and increments by 10 for each of the consecutive prefix list items.

deny: Specifies the deny mode. If a route matches the item, the route is denied without being compared with the next item. If a route does not match the item, the route is compared with the next item.

permit: Specifies the permit mode. If a route matches the item, it passes the IPv4 prefix list. If a route does not match the item, the route is compared with the next item.

ip-address mask-length: Specifies an IPv4 prefix and mask length. The value range for the *mask-length* argument is 0 to 32.

greater-equal *min-mask-length*, **less-equal** *max-mask-length*: Specifies a prefix length range. The **greater-equal** keyword means "greater than or equal to" and the **less-equal** keyword means "less than or equal to." The prefix length range relation is *mask-length* <= *min-mask-length* <= *max-mask-length* <= 32.

- If only the *min-mask-length* argument is specified, the prefix length range is [*min-mask-length*, 32].
- If only the *max-mask-length* argument is specified, the prefix length range is [*mask-length*, *max-mask-length*].
- If both the *min-mask-length* and *max-mask-length* arguments are specified, the prefix length range is [*min-mask-length*, *max-mask-length*].

Usage guidelines

An IPv4 prefix list is used to filter IPv4 addresses. It can contain multiple items, each of which specifies a range of IPv4 prefixes. The relation between the items is logical OR. If an item is passed, the IPv4 prefix list is passed. If no item is passed, the IP prefix list cannot be passed.

If both the *ip-address* and *mask-length* arguments are specified as 0.0.0.0 0, only the default route will be matched.

To match all routes, use 0.0.0.0 0 **less-equal** 32.

Examples

Configure IP prefix list **p1** to permit routes destined for network 10.0.0.0/8 and with mask length 17 or 18.

```
<Switch> system-view
[Switch] ip prefix-list p1 permit 10.0.0.0 8 greater-equal 17 less-equal 18
```

Related commands

display ip prefix-list

reset ip prefix-list

11.2.5. reset ip prefix-list

Use **reset ip prefix-list** to clear IPv4 prefix list statistics.

Syntax

reset ip prefix-list [*prefix-list-name*]

Views

User view

Predefined user roles

network-admin

Parameters

prefix-list-name: Specifies an IP prefix list by its name, a case-sensitive string of 1 to 63 characters. If you do not specify this argument, the command clears statistics for all IPv4 prefix lists.

Examples

Clear the statistics for IPv4 prefix list **abc**.

```
<Switch> reset ip prefix-list abc
```

Related commands

display ip prefix-list

ip prefix-list

11.3. IPv6 routing policy commands

11.3.1. apply ipv6 next-hop

Use **apply ipv6 next-hop** to set a next hop for IPv6 routes.

Use **undo apply ipv6 next-hop** to restore the default.

Syntax

apply ipv6 next-hop *ipv6-address*

undo apply ipv6 next-hop

Default

No next hop is set for IPv6 routes.

Views

Routing policy node view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies the next hop IPv6 address.

Usage guidelines

If you use this command to set a next hop for redistributed routes, the configuration does not take effect.

Examples

Configure node 10 in **permit** mode for routing policy **policy1** to set next hop 3ffe:506::1 for IPv6 routes matching prefix list 100.

```
<Switch> system-view
[Switch] ipv6 prefix-list 100 permit 2::2 64
[Switch] route-policy policy1 permit node 10
[Switch-route-policy-policy1-10] if-match ipv6 address prefix-list 100
[Switch-route-policy-policy1-10] apply ipv6 next-hop 3ffe:506::1
```

11.3.2. display ipv6 prefix-list

Use **display ipv6 prefix-list** to display IPv6 prefix list statistics.

Syntax

display ipv6 prefix-list [**name** *prefix-list-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

name *prefix-list-name*: Specifies an IPv6 prefix list by its name, a case-sensitive string of 1 to 63 characters. If you do not specify this option, the command displays statistics for all IPv6 prefix lists.

Examples

Display the statistics for all IPv6 prefix lists.

```
<Switch> display ipv6 prefix-list
Prefix-list6: 666
 Permitted 0
 Denied 0
        index: 10        Permit 6::/64                  ge  66  le  88
```

Table 11-6 Command output

Field	Description
Prefix-list6	Name of the IPv6 prefix list.
Permitted	Number of routes matching the criterion.
Denied	Number of routes not matching the criterion.
index	Index number of an item.
permit	Match mode of the item: • **Permit**. • **Deny**.
6::/64	IPv6 address and prefix length for matching.
ge	Greater-equal, the lower prefix length limit.
le	Less-equal, the upper prefix length limit.

Related commands

ipv6 prefix-list

reset ipv6 prefix-list

11.3.3. if-match ipv6

Use **if-match ipv6** to match IPv6 routes whose destination, next hop, or source address matches an ACL or IPv6 prefix list.

Use **undo if-match ipv6** to remove the specified ACL or IPv6 prefix list match criterion.

Syntax

if-match ipv6 { **address** | **next-hop** | **route-source** } { **acl** *ipv6-acl-number* | **prefix-list** *prefix-list-name*

undo if-match ipv6 { **address** | **next-hop** | **route-source** } [**acl** | **prefix-list**]

Default

No ACL or IPv6 prefix list match criterion is configured.

Views

Routing policy node view

Predefined user roles

network-admin

Parameters

address: Matches the destination address of IPv6 routes.

next-hop: Matches the next hop of IPv6 routes.

route-source: Matches the source address of IPv6 routes.

acl *ipv6-acl-number*: Specifies an IPv6 ACL by its number. The value range for the *ipv6-acl-number* argument is 2000 to 3999 for the **address** keyword, and 2000 to 2999 for the **next-hop** and **route-source** keywords.

prefix-list *prefix-list-name*: Specifies an IPv6 prefix list by its name, a case-sensitive string of 1 to 63 characters.

Examples

Configure node 10 of routing policy **policy1** to permit routes whose next hop matches IPv6 prefix list **p1**.

```
<Switch> system-view
[Switch] route-policy policy1 permit node 10
[Switch-route-policy-policy1-10] if-match ipv6 next-hop prefix-list p1
```

11.3.4. ipv6 prefix-list

Use **ipv6 prefix-list** to configure an IPv6 prefix list or an item for it.

Use **undo ipv6 prefix-list** to remove an IPv6 prefix list or an item.

Syntax

ipv6 prefix-list *prefix-list-name* [**index** *index-number*] { **deny** | **permit** } *ipv6-address* { *prefix-length* [**greater-equal** *min-prefix-length*] [**less-equal** *max-prefix-length*] | **inverse** *inverse-prefix-length* }

undo ipv6 prefix-list *prefix-list-name* [**index** *index-number*]

Default

No IPv6 prefix lists exist.

Views

System view

Predefined user roles

network-admin

Parameters

prefix-list-name: Specifies an IPv6 prefix list name, a case-sensitive string of 1 to 63 characters.

index *index-number*: Specifies an index number for an IPv6 prefix list item, in the range of 1 to 65535. An item with a smaller index number is matched first. If you do not specify this option, the index number starts from 10 and increments by 10 for each of the consecutive IPv6 prefix list items.

deny: Specifies the deny mode. If a route matches the item, the route is denied without being compared with the next item. If a route does not match the item, the route is compared with the next item.

permit: Specifies the permit mode. If a route matches the item, it passes the IPv6 prefix list. If a route does not match the item, the route is compared with the next item.

ipv6-address: Specifies an IPv6 address.

prefix-length: Specifies the IPv6 prefix length. The value range for the *prefix-length* argument is 0 to 128.

greater-equal *min-mask-length*, **less-equal** *max-mask-length*: Specifies a prefix length range. The **greater-equal** keyword means "greater than or equal to" and the **less-equal** keyword means "less than or equal to."

The prefix length range relation is *mask-length* <= *min-mask-length* <= *max-mask-length* <= 128.

- If only the *min-prefix-length* argument is specified, the prefix length range is [*min-prefix-length*, 128].
- If only the *max-prefix-length* argument is specified, the prefix length range is [*prefix-length*, *max-prefix-length*].
- If both the *min-prefix-length* and *max-prefix-length* arguments are specified, the prefix length range is [*min-prefix-length*, *max-prefix-length*].

inverse *inverse-prefix-length*: Matches IPv6 addresses from the least significant bit to the specified length. The value range for the *inverse-prefix-length* argument is 1 to 128.

Usage guidelines

An IPv6 prefix list is used to filter IPv6 addresses. An IPv6 prefix list can have multiple items, and each of them specifies a range of IPv6 prefixes. The relation between the items is logical OR. A route passing an item passes the IPv6 prefix list. A route passing no item does not pass the IPv6 prefix list.

If the *ipv6-address prefix-length* argument is specified as :: 0, only the default route matches.

To match all routes, configure :: 0 **less-equal** 128.

Examples

Permit IPv6 addresses with a mask length between 32 bits and 64 bits.

```
<Switch> system-view
[Switch] ipv6 prefix-list abc permit :: 0 greater-equal 32 less-equal 64
```

Deny IPv6 addresses with a prefix 3FFE:D00::/32 and a prefix length greater than or equal to 32 bits.

```
<Switch> system-view
[Switch] ipv6 prefix-list abc deny 3FFE:D00:: 32 less-equal 128
```

Related commands

display ipv6 prefix-list

reset ipv6 prefix-list

11.3.5. reset ipv6 prefix-list

Use **reset ipv6 prefix-list** to clear IPv6 prefix list statistics.

Syntax

reset ipv6 prefix-list [*prefix-list-name*]

Views

User view

Predefined user roles

network-admin

Parameters

prefix-list-name: Specifies an IPv6 prefix list by its name, a case-sensitive string of 1 to 63 characters. If you do not specify this argument, the command clears statistics for all IPv6 prefix lists.

Examples

Clear the statistics for IPv6 prefix list **abc**.

```
<Switch> reset ipv6 prefix-list abc
```

Related commands

display ipv6 prefix-list

ipv6 prefix-list

QX-S5600G Series Ethernet Switches

Command References

6.IP Multicast

This manual is including the following chapters.

01-IGMP snooping commands

02-Multicast VLAN commands

03-Multicast routing and forwarding commands

04-IGMP commands

05-PIM commands

06-MSDP commands

07-MLD snooping commands

08-IPv6 multicast VLAN commands

09-IPv6 multicast routing and forwarding commands

10-MLD commands

11-IPv6 PIM commands

12- PIM snooping commands

13- IGMP proxy commands

Contents

A page of this section is **6-x-x**

1. IGMP snooping commands ····· 1-1
1.1. IGMP snooping commands ····· 1-1
1.1.1. display igmp-snooping ····· 1-1
1.1.2. display igmp-snooping group ····· 1-4
1.1.3. display igmp-snooping router-port ····· 1-6
1.1.4. display igmp-snooping static-group ····· 1-7
1.1.5. display igmp-snooping static-router-port ····· 1-9
1.1.6. display igmp-snooping statistics ····· 1-10
1.1.7. display l2-multicast ip ····· 1-11
1.1.8. display l2-multicast ip forwarding ····· 1-13
1.1.9. display l2-multicast mac ····· 1-14
1.1.10. display l2-multicast mac forwarding ····· 1-16
1.1.11. display mac-address [multicast] ····· 1-18
1.1.12. dot1p-priority (IGMP-snooping view) ····· 1-19
1.1.13. dscp ····· 1-19
1.1.14. entry-limit (IGMP-snooping view) ····· 1-20
1.1.15. fast-leave (IGMP-snooping view) ····· 1-21
1.1.16. group-policy (IGMP-snooping view) ····· 1-21
1.1.17. host-aging-time (IGMP-snooping view) ····· 1-23
1.1.18. igmp-snooping ····· 1-23
1.1.19. igmp-snooping dot1p-priority ····· 1-24
1.1.20. igmp-snooping drop-unknown ····· 1-25
1.1.21. igmp-snooping enable ····· 1-26
1.1.22. igmp-snooping fast-leave ····· 1-27
1.1.23. igmp-snooping general-query source-ip ····· 1-28
1.1.24. igmp-snooping group-limit ····· 1-29
1.1.25. igmp-snooping group-policy ····· 1-29
1.1.26. igmp-snooping host-aging-time ····· 1-31
1.1.27. igmp-snooping host-join ····· 1-32
1.1.28. igmp-snooping last-member-query-interval ····· 1-33
1.1.29. igmp-snooping leave source-ip ····· 1-34
1.1.30. igmp-snooping max-response-time ····· 1-35
1.1.31. igmp-snooping overflow-replace ····· 1-36
1.1.32. igmp-snooping proxy enable ····· 1-37
1.1.33. igmp-snooping querier ····· 1-38
1.1.34. igmp-snooping query-interval ····· 1-39
1.1.35. igmp-snooping report source-ip ····· 1-40
1.1.36. igmp-snooping router-aging-time ····· 1-41
1.1.37. igmp-snooping source-deny ····· 1-42
1.1.38. igmp-snooping special-query source-ip ····· 1-42
1.1.39. igmp-snooping static-group ····· 1-44
1.1.40. igmp-snooping static-router-port ····· 1-44
1.1.41. igmp-snooping version ····· 1-45
1.1.42. last-member-query-interval (IGMP-snooping view) ····· 1-46
1.1.43. mac-address multicast ····· 1-47
1.1.44. max-response-time (IGMP-snooping view) ····· 1-48
1.1.45. overflow-replace (IGMP-snooping view) ····· 1-49
1.1.46. report-aggregation (IGMP-snooping view) ····· 1-49
1.1.47. reset igmp-snooping group ····· 1-50
1.1.48. reset igmp-snooping router-port ····· 1-51
1.1.49. reset igmp-snooping statistics ····· 1-51
1.1.50. router-aging-time (IGMP-snooping view) ····· 1-52

1.1.51. source-deny (IGMP-snooping view) ····· 1-52

1. IGMP snooping commands

1.1. IGMP snooping commands

1.1.1. display igmp-snooping

Use **display igmp-snooping** to display IGMP snooping status.

Syntax

display igmp-snooping [**global** | **vlan** *vlan-id* | **vsi** *vsi-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

global: Displays the global IGMP snooping status.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094.

vsi *vsi-name*: Specifies a VSI by its name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

If you do not specify any parameters, this command displays the global IGMP snooping status and the IGMP snooping status in all VLANs and VSIs.

Examples

MEMO:

Do not care about the contents of Global-enable. Even if Global-enable is Disabled, IGMP snooping is globally enabled. If it is globally disabled, "IGMP snooping is not configured." will be displayed.

Display the global IGMP snooping status and the IGMP snooping status for all VLANs and VSIs.

```
<Switch> display igmp-snooping
IGMP snooping information: Global
 Global-enable: Disabled
 Host-aging-time: 260s
 Router-aging-time: 260s
 Max-response-time: 10s
 Last-member-query-interval: 1s
 Report-aggregation: Enabled
 Host-tracking: Disabled
 Dot1p-priority: --

IGMP snooping information: VLAN 1
 IGMP snooping: Enabled
```

```
 Drop-unknown: Disabled
 Version: 2
 Host-aging-time: 260s
 Router-aging-time: 260s
 Max-response-time: 10s
 Last-member-query-interval: 1s
 Querier: Enabled (IP: 1.1.1.1, Expires: 00:02:05)
 Querier-election: Enabled
 Query-interval: 125s
 General-query source IP: 1.1.1.1
 Special-query source IP: 2.2.2.2
 Report source IP: 3.0.0.3
 Leave source IP: 1.0.0.1
 Host-tracking: Disabled
 Dot1p-priority: 2
 Proxy: Disabled

IGMP snooping information: VLAN 10
 IGMP snooping: Enabled
 Drop-unknown: Enabled
 Version: 3
 Host-aging-time: 260s
 Router-aging-time: 260s
 Max-response-time: 10s
 Last-member-query-interval: 1s
 Querier: Enabled (IP: 1.1.1.1, Expires: 00:02:05)
 Querier-election: Enabled
 Query-interval: 125s
 General-query source IP: 1.1.1.1
 Special-query source IP: 2.2.2.2
 Report source IP: 3.0.0.3
 Leave source IP: 1.0.0.1
 Host-tracking: Disabled
 Dot1p-priority: --
 Proxy: Disabled

IGMP snooping information: VSI aaa
 IGMP snooping: Enabled
 Drop-unknown: Enabled
 Version: 2
 Host-aging-time: 260s
 Router-aging-time: 260s
 Max-response-time: 10s
 Last-member-query-interval: 1s
 Querier: Disabled
 Querier-election: Disabled
 Query-interval: 125s
 General-query source IP: 1.1.1.1
```

```
Special-query source IP: 2.2.2.2
```

Table 1-1 Command output

Field	Description
Global-enable	Do not care about the contents of Global-enable. Even if Global-enable is Disabled, IGMP snooping is globally enabled.
IGMP snooping	IGMP snooping status in a VLAN or VSI: • **Enabled**. • **Disabled**.
Drop-unknown	Status of dropping unknown multicast data: • Enabled. • Disabled.
Version	IGMP snooping version.
Host-aging-time	Aging timer for the dynamic member port.
Router-aging-time	Aging timer for the dynamic router port.
Max-response-time	Maximum response time for IGMP general queries.
Last-member-query-interval	Interval for sending IGMP group-specific queries.
Report-aggregation	Status of IGMP report suppression: • Enabled. • Disabled.
Dot1p-priority	802.1p priority for IGMP messages. If the priority is not configured, this field displays two hyphens (--).
Querier	Status of IGMP snooping querier: • Enabled. • Disabled.
(IP: 1.1.1.1, Expires: 00:02:05)	IGMP snooping querier information: • **IP**—IP address of the IGMP snooping querier. • **Expire**—Remaining aging time for the IGMP snooping querier. This field is not displayed if IGMP snooping querier election is disabled.
Querier-election	Status of IGMP snooping querier election: • Enabled. • Disabled.
Query-interval	Interval for sending IGMP general queries.
General-query source IP	Source IP address of IGMP general queries.
Special-query source IP	Source IP address of IGMP group-specific queries.
Report source IP	Source IP address of IGMP reports.
Leave source IP	Source IP address of IGMP leave messages.
Host-tracking	Status of host tracking: • Enabled • Disabled.
Proxy	Status of IGMP snooping proxying:

Field	Description
	• Enabled. • Disabled.

1.1.2. display igmp-snooping group

Use **display igmp-snooping group** to display information about dynamic IGMP snooping group entries.

Syntax

display igmp-snooping group [*group-address* | *source-address*] * [**vlan** *vlan-id* | **vsi** *vsi-name*] [**verbose**] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

group-address: Specifies a multicast group by its IP address in the range of 224.0.1.0 to 239.255.255.255. If you do not specify a multicast group, this command displays information about dynamic IGMP snooping group entries for all multicast groups.

source-address: Specifies a multicast source by its IP address. If you do not specify a multicast source, this command displays information about dynamic IGMP snooping group entries for all multicast sources.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays information about dynamic IGMP snooping group entries for all VLANs.

vsi *vsi-name*: Specifies a VSI by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VSI, this command displays information about dynamic IGMP snooping group entries for all VSIs.

verbose: Displays detailed information about dynamic IGMP snooping group entries. If you do not specify this keyword, the command displays brief information about dynamic IGMP snooping group entries.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information about dynamic IGMP snooping group entries for the master device.

Examples

Display detailed information about dynamic IGMP snooping group entries for VLAN 2.

```
<Switch> display igmp-snooping group vlan 2 verbose
Total 1 entries.

VLAN 2: Total 1 entries.
  (0.0.0.0, 224.1.1.1)
    Attribute: local port
    FSM information: dummy
```

```
    Host slots (0 in total):
    Host ports (1 in total):
      GE1/0/2                          (00:03:23)
```

Display brief information about dynamic IGMP snooping group entries for VSI **aaa**.

```
<Switch> display igmp-snooping group vsi aaa
Total 1 entries.

VSI aaa: Total 1 entries.
  (0.0.0.0, 224.1.1.1)
    Host ports (3 in total):
      GE1/0/3 (Link ID 0)              (00:03:35)
      NPW (Link ID 8)                  (00:02:35)
      UPW (Link ID 9)                  (00:01:35)
```

Display detailed information about dynamic IGMP snooping group entries for VSI **bbb**.

```
<Switch> display igmp-snooping group vsi bbb verbose
Total 1 entries.
VSI bbb: Total 1 entries.
  (0.0.0.0, 224.1.1.1)
    Attribute: global port
    FSM information: dummy
    Host slots (0 in total):
    Host ports (2 in total):
      GE1/0/3 (Link ID 0)                        (00:03:35)
        VLAN pairs (1 in total):
          Outer VLAN 5     Inner VLAN 2          (00:03:35)
      Tun0 (VXLAN ID 0)                          (00:03:35)
        VLAN pairs (1 in total):
          Outer VLAN 5     Inner VLAN 2          (00:03:35)
```

Table 1-2 Command output

Field	Description
Total 1 entries	Total number of dynamic IGMP snooping group entries.
VLAN 2: Total 1 entries	Total number of dynamic IGMP snooping group entries in VLAN 2.
VSI aaa: Total 1 entries	Total number of dynamic IGMP snooping group entries in VSI **aaa**.
(0.0.0.0, 224.1.1.1)	(S, G) entry, where **0.0.0.0** in the S position means all multicast sources.
Attribute	Entry attribute: • **global port**—The entry has a global port. • **local port**—The entry has a port that resides on the member device for which the information is displayed. • **slot**—The entry has ports that reside on other member devices except the member device for which the information is displayed.
FSM information	Finite state machine information of the entry: • **delete**—The entry attributes have been deleted.

Field	Description
	• **dummy**—The entry is a new temporary entry. • **no info**—No entry exists.
Host slots (0 in total)	Member IDs and total number of the member devices that have member ports, except for the specified member device or the master device when no member device is specified.
Host ports (1 in total)	Member ports, and the total number of member ports.
(00:03:23)	Remaining aging time for the dynamic member port. For a global port (such as Layer 2 aggregate interfaces, ACs, N-PWs, and U-PWs), this field is always displayed. For a non-global port, this field is displayed when one of the following conditions exists: • The port is on the specified member device. • The port is on the master device and no member device is specified.
GE1/0/3 (Link ID 0)	AC and its link ID.
NPW (Link ID 8)	N-PW and its link ID.
UPW (Link ID 9)	U-PW and its link ID.
Tun0 (VXLAN ID 0)	VXLAN tunnel and its VXLAN ID.
VLAN pairs (1 in total)	VLAN pairs and total number of the VLAN pairs.
Outer VLAN 5 Inner VLAN 2	Outer VLAN ID and inner VLAN ID.

Related commands

reset igmp-snooping group

1.1.3. display igmp-snooping router-port

Use **display igmp-snooping router-port** to display dynamic router port information.

Syntax

display igmp-snooping router-port [**vlan** *vlan-id* | **vsi** *vsi-name*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays dynamic router port information for all VLANs.

vsi *vsi-name*: Specifies a VSI by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VSI, this command displays dynamic router port information for all VSIs.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays dynamic router port information for the master device.

Examples

Display brief information about dynamic router ports for VLAN 2.

```
<Switch> display igmp-snooping router-port vlan 2
VLAN 2:
  Router ports (2 in total):
    GE1/0/1                                 (00:01:30)
    GE1/0/2                                 (00:00:23)
```

Table 1-3 Command output

Field	Description
VLAN 2	VLAN ID.
VSI aaa	VSI name.
Router slots (0 in total)	Member IDs and total number of the member devices that have dynamic router ports, except for the specified member device or the master device when no member device is specified.
Router ports (2 in total)	Dynamic router ports and total number of dynamic router ports.
(00:01:30)	Remaining aging time for the dynamic router port. For a global port, this field is always displayed. For a global port, this field is displayed when one of the following conditions exists: • The port is on the specified member device. • The port is on the master device and no member device is specified.
GE1/0/3 (Link ID 1)	AC and its link ID.
NPW (Link ID 8)	N-PW and its link ID.
UPW (Link ID 9)	U-PW and its link ID.
Tun0 (VXLAN ID 0)	VXLAN tunnel and its VXLAN ID.
VLAN pairs (1 in total)	VLAN pairs and total number of VLAN pairs.
Outer VLAN 5 Inner VLAN 2	Outer VLAN ID and inner VLAN ID.

Related commands

reset igmp-snooping router-port

1.1.4. display igmp-snooping static-group

Use **display igmp-snooping static-group** to display information about static IGMP snooping group entries.

Syntax

display igmp-snooping static-group [*group-address* | *source-address*] * [**vlan** *vlan-id*] [**verbose**] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

group-address: Specifies a multicast group by its IP address in the range of 224.0.1.0 to 239.255.255.255. If you do not specify a multicast group, this command displays information about static IGMP snooping group entries for all multicast groups.

source-address: Specifies a multicast source by its IP address. If you do not specify a multicast source, this command displays information about static IGMP snooping group entries for all multicast sources.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays information about static IGMP snooping group entries for all VLANs.

verbose: Displays detailed information about static IGMP snooping group entries. If you do not specify the keyword, this command displays brief information about static IGMP snooping group entries.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information about static IGMP snooping group entries for the master device.

Examples

Display detailed information about static IGMP snooping group entries for VLAN 2.

```
<Switch> display igmp-snooping static-group vlan 2 verbose
Total 1 entries.

VLAN 2: Total 1 entries.
  (0.0.0.0, 224.1.1.1)
    Attribute: local port
    FSM information: dummy
    Host slots (0 in total):
    Host ports (1 in total):
      GE1/0/2
```

Table 1-4 Command output

Field	Description
Total 1 entries	Total number of static IGMP snooping group entries.
VLAN 2: Total 1 entries	Total number of static IGMP snooping group entries in VLAN 2.
(0.0.0.0, 224.1.1.1)	(S, G) entry, where **0.0.0.0** in the S position means all multicast sources.
Attribute	Entry attribute: • **global port**—The entry has a global port. • **local port**—The entry has a port that resides on the member device for which the information is displayed. • **slot**—The entry has ports that reside on other member devices except the member device for which the information is displayed.
FSM information	Finite state machine information of the entry:

Field	Description
	• **delete**—The entry attributes have been deleted. • **dummy**—The entry is a new temporary entry. • **no info**—No entry exists.
Host slots (0 in total)	Member IDs and total number of the member devices that have member ports, except for the specified member device or the master device when no member device is specified.
Host ports (1 in total)	Member ports and total number of member ports.

1.1.5. display igmp-snooping static-router-port

Use **display igmp-snooping static-router-port** to display static router port information.

Syntax

display igmp-snooping static-router-port [**vlan** *vlan-id*] [**verbose**] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094.

verbose: Displays detailed information about static router ports. If you do not specify this keyword, the command displays brief information about static router ports.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays static router port information for the master device.

Examples

Display brief information about static router ports for VLAN 2.

```
<Switch> display igmp-snooping static-router-port vlan 2
VLAN 2:
  Router ports (2 in total):
    GE1/0/1
    GE1/0/2
```

Display detailed information about static router ports for VLAN 2.

```
<Switch> display igmp-snooping static-router-port vlan 2 verbose
VLAN 2:
  Router slots (0 in total):
  Router ports (2 in total):
    GE1/0/1
    GE1/0/2
```

Table 1-5 Command output

Field	Description
VLAN 2	VLAN ID.
Router slots (0 in total)	Member IDs and total number of the member devices that have static router ports, except for the specified member device or the master device when no member device is specified.
Router ports (2 in total)	Static router ports and total number of static router ports.

1.1.6. display igmp-snooping statistics

Use **display igmp-snooping statistics** to display statistics for the IGMP messages and PIMv2 hello messages learned through IGMP snooping.

Syntax

display igmp-snooping statistics

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display statistics for the IGMP messages and PIMv2 hello messages learned through IGMP snooping.

```
<Switch> display igmp-snooping statistics
Received IGMP general queries:  0
Received IGMPv1 reports:  0
Received IGMPv2 reports:  19
Received IGMP leaves:  0
Received IGMPv2 specific queries:  0
Sent     IGMPv2 specific queries:  0
Received IGMPv3 reports:  1
Received IGMPv3 reports with right and wrong records:  0
Received IGMPv3 specific queries:  0
Received IGMPv3 specific sg queries:  0
Sent     IGMPv3 specific queries:  0
Sent     IGMPv3 specific sg queries:  0
Received PIMv2 hello:  0
Received error IGMP messages:  19
```

Table 1-6 Command output

Field	Description
general queries	Number of IGMP general queries.
specific queries	Number of IGMP group-specific queries.
reports	Number of IGMP reports.

Field	Description
leaves	Number of IGMP leave messages.
reports with right and wrong records	Number of IGMP reports with correct and incorrect records.
specific sg queries	Number of IGMP group-and-source-specific queries.
PIMv2 hello	Number of PIMv2 hello messages.
error IGMP messages	Number of IGMP messages with errors.

Related commands

reset igmp-snooping statistics

1.1.7. display l2-multicast ip

Use **display l2-multicast ip** to display information about Layer 2 IP multicast groups.

Syntax

display l2-multicast ip [**group** *group-address* | **source** *source-address*] * [**vlan** *vlan-id* | **vsi** *vsi-name*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

group *group-address*: Specifies a multicast group by its IP address. If you do not specify a multicast group, this command displays information about all Layer 2 IP multicast groups.

source *source-address*: Specifies a multicast source by its IP address. If you do not specify a multicast source, this command displays information about Layer 2 IP multicast groups for all multicast sources.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays information about Layer 2 IP multicast groups for all VLANs.

vsi *vsi-name*: Specifies a VSI by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VSI, this command displays information about Layer 2 IP multicast groups for all VSIs.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information about Layer 2 IP multicast groups for the master device.

Examples

Display information about Layer 2 IP multicast groups for VLAN 2.

```
<Switch> display l2-multicast ip vlan 2
Total 1 entries.

VLAN 2: Total 1 entries.
  (0.0.0.0, 224.1.1.1)
    Attribute: static, success
```

```
    Host ports (1 in total):
      GE1/0/1                                 (S, SUC)
```

Display information about Layer 2 IP multicast groups for VSI **aaa**.

```
<Switch> display l2-multicast ip vsi aaa
Total 1 entries.

VSI aaa: Total 1 entries.
  (0.0.0.0, 224.1.1.1)
    Attribute: dynamic, success
    Host ports (3 in total):
      GE1/0/1 (Link ID 1)                 (D, SUC)
      NPW (Link ID 8)                     (D, SUC)
      UPW (Link ID 9)                     (D, SUC)
```

Display information about Layer 2 IP multicast groups for VSI **bbb**.

```
<Switch> display l2-multicast ip vsi bbb
Total 1 entries.

VSI bbb: Total 1 entries.
  (0.0.0.0, 224.1.1.1)
    Attribute: dynamic, success
    Host ports (2 in total):
      GE1/0/1 (Link ID 1)                 (D, SUC)
      Tun0 (VXLAN ID 0)                   (D, SUC)
```

Table 1-7 Command output

Field	Description
Total 1 entries	Total number of Layer 2 IP multicast groups.
VLAN 2: Total 1 entries	Total number of Layer 2 IP multicast groups in VLAN 2.
VSI aaa: Total 1 entries	Total number of Layer 2 IP multicast groups in VSI **aaa**.
(0.0.0.0, 224.1.1.1)	(S, G) entry, where **0.0.0.0** in the S position means all multicast sources.
Attribute	Entry attribute: • **dynamic**—The entry is created by a dynamic protocol. • **static**—The entry is created by a static protocol. • **pim**—The entry is created by PIM. • **kernel**—The entry is obtained from the kernel. • **success**—Processing has succeeded. • **fail**—Processing has failed.
Host ports (1 in total)	Member ports and total number of member ports.
(S, SUC)	Port attribute: • **D**—Dynamic port. • **S**—Static port. • **P**—PIM port. • **K**—Port obtained from the kernel. • **R**—Port learned from (*, *) entries. • **W**—Port learned from (*, G) entries.

Field	Description
	• **SUC**—Processing has succeeded. • **F**—Processing has failed.
GE1/0/1 (Link ID 1)	AC and its link ID.
NPW (Link ID 8)	N-PW and its link ID.
UPW (Link ID 9)	U-PW and its link ID.
Tun0 (VXLAN ID 0)	VXLAN tunnel and its VXLAN ID.

1.1.8. display l2-multicast ip forwarding

Use **display l2-multicast ip forwarding** to display Layer 2 multicast IP forwarding entries.

Syntax

display l2-multicast ip forwarding [**group** *group-address* | **source** *source-address*] * [**vlan** *vlan-id* | **vsi** *vsi-name*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

group *group-address*: Specifies a multicast group by its IP address. If you do not specify a multicast group, this command displays Layer 2 multicast IP forwarding entries for all multicast groups.

source *source-address*: Specifies a multicast source by its IP address. If you do not specify a multicast source, this command displays Layer 2 multicast IP forwarding entries for all multicast sources.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays Layer 2 multicast IP forwarding entries for all VLANs.

vsi *vsi-name*: Specifies a VSI by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VSI, this command displays Layer 2 multicast IP forwarding entries for all VSIs.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays Layer 2 multicast IP forwarding entries for the master device.

Examples

Display Layer 2 multicast IP forwarding entries for VLAN 2.

```
<Switch> display l2-multicast ip forwarding vlan 2
Total 1 entries.

VLAN 2: Total 1 entries.
  (0.0.0.0, 224.1.1.1)
    Host ports (3 in total):
      GigabitEthernet1/0/1
```

```
      GigabitEthernet1/0/2
      GigabitEthernet1/0/3
```

Display Layer 2 IP multicast group entries for VSI **aaa**.

```
<Switch> display l2-multicast ip forwarding vsi aaa
Total 1 entries.

VSI aaa: Total 1 entries.
  (0.0.0.0, 224.1.1.1)
    Host ports (3 in total):
      GigabitEthernet1/0/3(Link ID 0)
      NPW (Link ID 8)
      UPW (Link ID 9)
```

Display information about Layer 2 multicast IP forwarding entries for VSI **bbb**.

```
<Switch> display l2-multicast ip forwarding vsi bbb
Total 1 entries.

VSI bbb: Total 1 entries.
  (0.0.0.0, 224.1.1.1)
    Host ports (2 in total):
      GigabitEthernet1/0/3(Link ID 0)
      Tunnel0 (VXLAN ID 0)
```

Table 1-8 Command output

Field	Description
Total 1 entries	Total number of Layer 2 multicast IP forwarding entries.
VLAN 2: Total 1 entries	Total number of Layer 2 multicast IP forwarding entries in VLAN 2.
VSI aaa: Total 1 entries	Total number of Layer 2 multicast IP forwarding entries in VSI **aaa**.
(0.0.0.0, 224.1.1.1)	(S, G) entry, where **0.0.0.0** in the S position means all multicast sources.
Host ports (3 in total)	Member ports and total number of member ports.
GigabitEthernet1/0/3 (Link ID 0)	AC and its link ID.
NPW (Link ID 8)	N-PW and its link ID.
UPW (Link ID 9)	U-PW and its link ID.
Tunnel0 (VXLAN ID 0)	VXLAN tunnel and its VXLAN ID.

1.1.9. display l2-multicast mac

Use **display l2-multicast mac** to display information about Layer 2 MAC multicast groups.

Syntax

display l2-multicast mac [*mac-address*] [**vlan** *vlan-id* | **vsi** *vsi-name*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

mac-address: Specifies a MAC multicast group by its multicast MAC address. If you do not specify a MAC multicast group, this command displays information about all Layer 2 MAC multicast groups.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays information about Layer 2 MAC multicast groups for all VLANs.

vsi *vsi-name*: Specifies a VSI by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VSI, this command displays information about Layer 2 MAC multicast groups for all VSIs.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information about Layer 2 MAC multicast groups for the master device.

Examples

Display information about Layer 2 MAC multicast groups for VLAN 2.

```
<Switch> display l2-multicast mac vlan 2
Total 1 entries.

VLAN 2: Total 1 entries.
  MAC group address: 0100-5e01-0101
    Attribute: success
    Host ports (1 in total):
      GE1/0/1
```

Display information about Layer 2 MAC multicast groups for VSI **aaa**.

```
<Switch> display l2-multicast mac vsi aaa
Total 1 entries.

VSI aaa: Total 1 entries.
  MAC group address: 0100-5e01-0101
    Attribute: success
    Host ports (3 in total):
      GE1/0/3 (Link ID 0)
      NPW (Link ID 8)
      UPW (Link ID 9)
```

Display information about Layer 2 MAC multicast groups for VSI **bbb**.

```
<Switch> display l2-multicast mac vsi bbb
Total 1 entries.

VSI bbb: Total 1 entries.
  MAC group address: 0100-5e01-0101
    Attribute: success
    Host ports (2 in total):
```

```
GE1/0/3 (Link ID 0)
Tun0 (VXLAN ID 0)
```

Table 1-9 Command output

Field	Description
Total 1 entries	Total number of Layer 2 MAC multicast groups.
VLAN 2: Total 1 entries	Total number of Layer 2 MAC multicast groups in VLAN 2.
VSI aaa: Total 1 entries	Total number of Layer 2 MAC multicast groups in VSI **aaa**.
MAC group address	Address of the MAC multicast group.
Attribute	Entry attribute: • **success**—Processing has succeeded. • **fail**—Processing has failed.
Host ports (1 in total)	Member ports and total number of member ports.
GE1/0/3 (Link ID 0)	AC and its link ID.
NPW (Link ID 8)	N-PW and its link ID.
UPW (Link ID 9)	U-PW and its link ID.
Tun0 (VXLAN ID 0)	VXLAN tunnel and its VXLAN ID.

1.1.10. display l2-multicast mac forwarding

Use **display l2-multicast mac forwarding** to display Layer 2 multicast MAC forwarding entries.

Syntax

display l2-multicast mac forwarding [*mac-address*] [**vlan** *vlan-id* | **vsi** *vsi-name*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

mac-address: Specifies a MAC multicast group by its MAC address. If you do not specify a MAC multicast group, this command displays Layer 2 multicast MAC forwarding entries for all MAC multicast groups.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays Layer 2 multicast MAC forwarding entries for all VLANs.

vsi *vsi-name*: Specifies a VSI by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VSI, this command displays Layer 2 MAC forwarding entries for all VSIs.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays Layer 2 multicast MAC group entries for the master device.

Examples

Display Layer 2 multicast MAC forwarding entries for VLAN 2.

```
<Switch> display l2-multicast mac forwarding vlan 2
Total 1 entries.

VLAN 2: Total 1 entries.
  MAC group address: 0100-5e01-0101
    Host ports (3 in total):
      GigabitEthernet1/0/1
      GigabitEthernet1/0/2
      GigabitEthernet1/0/3
```

Display Layer 2 multicast MAC forwarding entries for VSI **aaa**.

```
<Switch> display l2-multicast mac forwarding vsi aaa
Total 1 entries.

VSI aaa: Total 1 entries.
  MAC group address: 0100-5e01-0101
    Host slots (0 in total):
    Host ports (3 in total):
      GigabitEthernet1/0/3 (Link ID 0)
      NPW (Link ID 8)
      UPW (Link ID 9)
```

Display Layer 2 multicast MAC forwarding entries for VSI **bbb**.

```
<Switch> display l2-multicast mac forwarding vsi bbb
Total 1 entries.

VSI bbb: Total 1 entries.
  MAC group address: 0100-5e01-0101
    Host ports (2 in total):
      GigabitEthernet1/0/3 (Link ID 0)
      Tunnel0 (VXLAN ID 0)
```

Table 1-10 Command output

Field	Description
Total 1 entries	Total number of Layer 2 multicast MAC forwarding entries.
VLAN 2: Total 1 entries	Total number of Layer 2 multicast MAC forwarding entries in VLAN 2.
VSI aaa: Total 1 entries	Total number of Layer 2 multicast MAC multicast group entries in VSI **aaa**.
MAC group address	Address of the MAC multicast group.
Host ports (3 in total)	Member ports and total number of member ports.
GigabitEthernet1/0/3 (Link ID 0)	AC and its link ID.
NPW (Link ID 8)	N-PW and its link ID.
UPW (Link ID 9)	U-PW and its link ID.
Tunnel0 (VXLAN ID 0)	VXLAN tunnel and its VXLAN ID.

1.1.11. display mac-address [multicast]

Use **display mac-address** [**multicast**] to display static multicast MAC address entries.

Syntax

display mac-address [*mac-address* [**vlan** *vlan-id*] | [**multicast**] [**vlan** *vlan-id*] [**count**]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

mac-address: Specifies a multicast MAC address. The MAC address can be any legal multicast MAC address except 0100-5Exx-xxxx and 3333-xxxx-xxxx, where "x" represents a hexadecimal number in the range of 0 to F.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays MAC address entries for all VLANs.

multicast: Specifies static multicast MAC address entries.

count: Specifies the number of MAC address entries. If you specify this keyword, the command displays the number of matching MAC address entries. If you do not specify this keyword, the command displays the contents of the matching entries rather than the entry count.

Usage guidelines

If you do not specify any parameters, this command displays all MAC address table entries, including unicast MAC address entries and static multicast MAC address entries.

Examples

Display static multicast MAC address entries for VLAN 2.

```
<Switch> display mac-address multicast vlan 2
MAC Address      VLAN ID    State            Port/NickName            Aging
0100-0001-0001   2          Multicast        GE1/0/1                  N
```

Display the number of static multicast MAC address entries.

```
<Switch> display mac-address multicast count
1 mac address(es) found.
```

Table 1-11 Command output

Field	Description
MAC address	MAC address of a multicast group.
VLAN ID	ID of the VLAN to which the network device identified by the MAC address belongs.
State	Status of the MAC address. If the multicast MAC address entry is static, this field displays **Multicast**.
Port/NickName	Outgoing ports or nickname of the Egress RB in a TRILL network for the packet that is sent to the MAC address in this MAC address entry. For more information about the nickname, TRILL, and RB, see *TRILL Configuration Guide*.

Field	Description
	TRILL is not supported in the current software version.
Aging	Aging timer state. If this entry never expires, this field displays **N**.
1 mac address(es) found	One static multicast MAC address entry is found.

Related commands

mac-address multicast

1.1.12. dot1p-priority (IGMP-snooping view)

Use **dot1p-priority** to set the 802.1p priority for IGMP messages globally.

Use **undo dot1p-priority** to restore the default.

Syntax

dot1p-priority *priority*

undo dot1p-priority

Default

The 802.1p priority for IGMP messages is not configured. For IGMP messages created by the device, the 802.1p priority is 0. For IGMP messages to be forwarded, the device does not change the 802.1p priority.

Views

IGMP-snooping view

Predefined user roles

network-admin

Parameters

priority: Specifies an 802.1p priority for IGMP messages, in the range of 0 to 7. The greater the value, the higher the priority.

Usage guidelines

You can set the 802.1p priority globally for all VLANs and VSIs in IGMP-snooping view or for a VLAN in VLAN view. For a VLAN, the VLAN-specific configuration takes priority over the global configuration.

Examples

Set the 802.1p priority for IGMP messages to 3 globally.

```
<Switch> system-view
[Switch] igmp-snooping
[Switch-igmp-snooping] dot1p-priority 3
```

Related commands

igmp-snooping dot1p-priority

1.1.13. dscp

Use **dscp** to set the DSCP value for outgoing IGMP snooping protocol packets.

Use **undo dscp** to restore the default.

Syntax

dscp *dscp-value*

undo dscp

Default

The DSCP value is 48 for outgoing IGMP snooping protocol packets.

Views

IGMP-snooping view

Predefined user roles

network-admin

Parameters

dscp-value: Specifies a DSCP value in the range of 0 to 63.

Usage guidelines

The DSCP value is carried in the ToS field of an IP packet to determine the transmission priority of the packet. A greater DSCP value represents a higher priority.

Examples

Set the DSCP value to 63 for outgoing IGMP snooping protocol packets.

```
<Switch> system-view
[Switch] igmp-snooping
[Switch-igmp-snooping] dscp 63
```

1.1.14. entry-limit (IGMP-snooping view)

Use **entry-limit** to globally set the maximum number of IGMP snooping forwarding entries, including dynamic entries and static entries.

Use **undo entry-limit** to restore the default.

Syntax

entry-limit *limit*

undo entry-limit

Default

The maximum number of IGMP snooping forwarding entries is 4294967295.

Views

IGMP-snooping view

Predefined user roles

network-admin

Parameters

limit: Specifies the maximum number of IGMP snooping forwarding entries, in the range of 0 to 4294967295.

Examples

Set the global maximum number of IGMP snooping forwarding entries to 512.

```
<Switch> system-view
[Switch] igmp-snooping
[Switch-igmp-snooping] entry-limit 512
```

1.1.15. fast-leave (IGMP-snooping view)

Use **fast-leave** to enable fast-leave processing globally.

Use **undo fast-leave** to disable fast-leave processing globally.

Syntax

fast-leave [**vlan** *vlan-list*]

undo fast-leave [**vlan** *vlan-list*]

Default

Fast-leave processing is disabled.

Views

IGMP-snooping view

Predefined user roles

network-admin

Parameters

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The VLAN ID is in the range of 1 to 4094. If you do not specify a VLAN, this command takes effect on all VLANs and VSIs.

Usage guidelines

The fast-leave processing feature enables the device to immediately remove a port from the forwarding entry for a multicast group when the port receives a leave message.

You can enable fast-leave processing globally for all ports in IGMP-snooping view or for a port in interface view. For a port, the port-specific configuration takes priority over the global configuration.

Examples

Globally enable fast-leave processing for VLAN 2.

```
<Switch> system-view
[Switch] igmp-snooping
[Switch-igmp-snooping] fast-leave vlan 2
```

Related commands

igmp-snooping fast-leave

1.1.16. group-policy (IGMP-snooping view)

Use **group-policy** to globally configure a multicast group policy to control the multicast groups that hosts can join.

Use **undo group-policy** to globally delete multicast group policies.

Syntax

group-policy *ipv4-acl-number* [**vlan** *vlan-list*]

undo group-policy [**vlan** *vlan-list*]

Default

No multicast group policies exist. Hosts can join any multicast groups.

Views

IGMP-snooping view

Predefined user roles

network-admin

Parameters

ipv4-acl-number: Specifies an IPv4 basic or advanced ACL by its number in the range of 2000 to 3999. Hosts can join only the multicast groups that the ACL permits. If the ACL does not exist or does not have valid rules, hosts cannot join multicast groups.

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The VLAN ID is in the range of 1 to 4094. If you do not specify a VLAN, this command takes effect on all VLANs and VSIs.

Usage guidelines

A multicast group policy filters IGMP reports to control the multicast groups that hosts can join.

This command does not take effect on static member ports, because static member ports do not send IGMP reports.

You can configure a multicast group policy globally for all ports in IGMP-snooping view or for a port in interface view. For a port, the port-specific configuration takes priority over the global configuration.

When you configure a rule in the IPv4 ACL, follow these restrictions and guidelines:

- For the rule to take effect, do not specify the **vpn-instance** *vpn-instance* option.
- In a basic ACL, the **source** *source-address source-wildcard* option specifies a multicast group address.
- In an advanced ACL, the **source** *source-address source-wildcard* option specifies a multicast source address. The **destination** *dest-address dest-wildcard* option specifies a multicast group address.

  To match the following IGMP reports, set the **source** *source-address source-wildcard* option to 0.0.0.0:

  - IGMPv1 and IGMPv2 reports.
  - IGMPv3 IS_EX and IGMPv3 TO_EX reports that do not carry multicast source addresses.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

You can configure different ACLs for all ports in different VLANs. If you configure multiple ACLs for all ports in the same VLAN, the most recent configuration takes effect.

Examples

Configure a multicast group policy for VLAN 2 so that hosts in VLAN 2 can join only multicast group 225.1.1.1.

```
<Switch> system-view
[Switch] acl basic 2000
[Switch-acl-ipv4-basic-2000] rule permit source 225.1.1.1 0
[Switch-acl-ipv4-basic-2000] quit
[Switch] igmp-snooping
```

```
[Switch-igmp-snooping] group-policy 2000 vlan 2
```

Related commands

igmp-snooping group-policy

1.1.17. host-aging-time (IGMP-snooping view)

Use **host-aging-time** to set the aging timer for dynamic member ports globally.

Use **undo host-aging-time** to restore the default.

Syntax

host-aging-time *seconds*

undo host-aging-time

Default

The aging timer for dynamic member ports is 260 seconds.

Views

IGMP-snooping view

Predefined user roles

network-admin

Parameters

seconds: Specifies an aging timer for dynamic member ports, in the range of 1 to 8097894 seconds.

Usage guidelines

You can set the timer globally for all VLANs and VSIs in IGMP-snooping view, for a VSI in VSI view, or for a VLAN in VLAN view. For a VSI, the VSI-specific configuration takes priority over the global configuration. For a VLAN, the VLAN-specific configuration takes priority over the global configuration.

To avoid mistakenly deleting multicast group members, set the aging timer for dynamic member ports to be greater than the value calculated by using the following formula:

[IGMP general query interval] + [maximum response time for IGMP general queries]

As a best practice, set the aging timer of dynamic member ports to the value calculated by using the following formula:

[IGMP general query interval] × 2 + [maximum response time for IGMP general queries]

Examples

Set the global aging timer for dynamic member ports to 300 seconds.

```
<Switch> system-view
[Switch] igmp-snooping
[Switch-igmp-snooping] host-aging-time 300
```

Related commands

igmp-snooping host-aging-time

1.1.18. igmp-snooping

Use **igmp-snooping** to enable the IGMP snooping feature and enter IGMP-snooping view.

Use **undo igmp-snooping** to disable the IGMP snooping feature.

Syntax

igmp-snooping

undo igmp-snooping

After enabling IGMP snooping globally, enable IGMP snooping on the VLANs you use. For IGMP snooping settings, see Section 6 *IP Multicast "IGMP Snooping"* in the Configuration Guides.

Default

The IGMP snooping feature is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

If you disable the IGMP snooping feature, IGMP snooping is disabled in all VLANs and VSIs.

Examples

Enable the IGMP snooping feature and enter IGMP-snooping view.

```
<Switch> system-view
[Switch] igmp-snooping
[Switch-igmp-snooping]
```

Related commands

igmp-snooping enable

1.1.19. igmp-snooping dot1p-priority

Use **igmp-snooping dot1p-priority** to set the 802.1p priority for IGMP messages in a VLAN.

Use **undo igmp-snooping dot1p-priority** to restore the default.

Syntax

igmp-snooping dot1p-priority *priority*

undo igmp-snooping dot1p-priority

Default

The 802.1p priority for IGMP messages is not configured. For IGMP messages created by the device, the 802.1p priority is 0. For IGMP messages to be forwarded, the device does not change the 802.1p priority.

Views

VLAN view

Predefined user roles

network-admin

Parameters

priority: Specifies an 802.1p priority for IGMP messages, in the range of 0 to 7. The greater the value, the higher the priority.

Usage guidelines

You must enable IGMP snooping for a VLAN before you execute this command.

You can set the 802.1p priority for a VLAN in VLAN view or globally for all VLANs in IGMP-snooping view. The VLAN-specific configuration takes priority over the global configuration.

Examples

In VLAN 2, enable IGMP snooping, and set the 802.1p priority for IGMP messages to 3.

```
<Switch> system-view
[Switch] igmp-snooping
[Switch-igmp-snooping] quit
[Switch] vlan 2
[Switch-vlan2] igmp-snooping enable
[Switch-vlan2] igmp-snooping dot1p-priority 3
```

Related commands

dot1p-priority (IGMP-snooping view)

igmp-snooping enable

1.1.20. igmp-snooping drop-unknown

Use **igmp-snooping drop-unknown** to enable dropping unknown multicast data packets for a VLAN or VSI.

Use **undo igmp-snooping drop-unknown** to disable dropping unknown multicast data packets for a VLAN or VSI.

Syntax

igmp-snooping drop-unknown

undo igmp-snooping drop-unknown

Default

Dropping unknown multicast data packets is disabled. Unknown multicast data packets are flooded.

Views

VLAN view

VSI view

Predefined user roles

network-admin

Usage guidelines

You must enable IGMP snooping for a VLAN or VSI before you execute this command.

Examples

In VLAN 2, enable IGMP snooping, and enable dropping unknown multicast data packets.

```
<Switch> system-view
[Switch] igmp-snooping
[Switch-igmp-snooping] quit
```

```
[Switch] vlan 2
[Switch-vlan2] igmp-snooping enable
[Switch-vlan2] igmp-snooping drop-unknown
```

In VSI **aaa**, enable IGMP snooping, and enable dropping unknown multicast data packets.

```
<Switch> system-view
[Switch] igmp-snooping
[Switch-igmp-snooping] quit
[Switch] vsi aaa
[Switch-vsi-aaa] igmp-snooping enable
[Switch-vsi-aaa] igmp-snooping drop-unknown
```

Related commands

igmp-snooping enable

1.1.21. igmp-snooping enable

Use **igmp-snooping enable** to enable IGMP snooping for a VLAN or VSI.

Use **undo igmp-snooping** to disable IGMP snooping for a VLAN or VSI.

Syntax

igmp-snooping enable

undo igmp-snooping

After enabling IGMP snooping globally, enable IGMP snooping on the VLANs you use. For IGMP snooping settings, see Section 6 *IP Multicast "IGMP Snooping"* in the Configuration Guides.

Default

IGMP snooping is disabled for a VLAN or VSI.

Views

VLAN view

VSI view

Predefined user roles

network-admin

Usage guidelines

You must enable the IGMP snooping feature by using the **igmp-snooping** command before you enable IGMP snooping for a VLAN or VSI.

You can enable IGMP snooping for a VLAN by using this command in VLAN view. The configuration in VLAN view has the same priority as the configuration in IGMP-snooping view, and the most recent configuration takes effect.

Examples

Enable the IGMP snooping feature, and then enable IGMP snooping for VLAN 2.

```
<Switch> system-view
[Switch] igmp-snooping
[Switch-igmp-snooping] quit
[Switch] vlan 2
[Switch-vlan2] igmp-snooping enable
```

Enable the IGMP snooping feature, and then enable IGMP snooping for VSI **aaa**.

```
<Switch> system-view
[Switch] igmp-snooping
[Switch-igmp-snooping] quit
[Switch] vsi aaa
[Switch-vsi-aaa] igmp-snooping enable
```

Related commands

igmp-snooping

1.1.22. igmp-snooping fast-leave

Use **igmp-snooping fast-leave** to enable fast-leave processing on a port.

Use **undo igmp-snooping fast-leave** to disable fast-leave processing on a port.

Syntax

igmp-snooping fast-leave [**vlan** *vlan-list*]

undo igmp-snooping fast-leave [**vlan** *vlan-list*]

Default

Fast-leave processing is disabled on a port.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The VLAN ID is in the range of 1 to 4094. If you do not specify a VLAN, this command takes effect on all VLANs.

Usage guidelines

The fast-leave processing feature enables the device to immediately remove a port from the forwarding entry for a multicast group when the port receives a leave message.

You can enable fast-leave processing for a port in interface view or globally for all ports in IGMP-snooping view. For a port, the port-specific configuration takes priority over the global configuration.

Examples

Enable fast-leave processing for VLAN 2 on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] igmp-snooping fast-leave vlan 2
```

Related commands

fast-leave (IGMP-snooping view)

1.1.23. igmp-snooping general-query source-ip

Use **igmp-snooping general-query source-ip** to configure the source IP address for IGMP general queries.

Use **undo igmp-snooping general-query source-ip** to restore the default.

Syntax

igmp-snooping general-query source-ip *ip-address*

undo igmp-snooping general-query source-ip

Default

In a VLAN, the source IP address of IGMP general queries is the IP address of the current VLAN interface. If the current VLAN interface does not have an IP address, the source IP address is 0.0.0.0.

In a VSI, the source IP address of IGMP general queries is the IP address of the gateway interface for the VSI. If the gateway interface does not have an interface, the source IP address is 0.0.0.0.

Views

VLAN view

VSI view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the source IP address for IGMP general queries.

Usage guidelines

You must enable IGMP snooping for a VLAN or VSI before you execute this command.

Examples

In VLAN 2, enable IGMP snooping, and specify 10.1.1.1 as the source IP address of IGMP general queries.

```
<Switch> system-view
[Switch] igmp-snooping
[Switch-igmp-snooping] quit
[Switch] vlan 2
[Switch-vlan2] igmp-snooping enable
[Switch-vlan2] igmp-snooping general-query source-ip 10.1.1.1
```

In VSI **aaa**, enable IGMP snooping, and specify 10.1.1.1 as the source IP address of IGMP general queries.

```
<Switch> system-view
[Switch] igmp-snooping
[Switch-igmp-snooping] quit
[Switch] vsi aaa
[Switch-vsi-aaa] igmp-snooping enable
[Switch-vsi-aaa] igmp-snooping general-query source-ip 10.1.1.1
```

Related commands

igmp-snooping enable

1.1.24. igmp-snooping group-limit

Use **igmp-snooping group-limit** to set the maximum number of multicast groups that a port can join.

Use **undo igmp-snooping group-limit** to remove the limit on the maximum number of multicast groups that a port can join.

Syntax

igmp-snooping group-limit *limit* [**vlan** *vlan-list*]

undo igmp-snooping group-limit [**vlan** *vlan-list*]

Default

No limit is placed on the maximum number of multicast groups that a port can join.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

limit: Specifies the maximum number of multicast groups that a port can join, in the range of 0 to 4294967295.

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The VLAN ID is in the range of 1 to 4094. If you do not specify a VLAN, this command takes effect on all VLANs.

Usage guidelines

This command takes effect only on the multicast groups that a port joins dynamically.

Examples

On GigabitEthernet 1/0/1, set the maximum number of multicast groups the port can join in VLAN 2 to 10.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] igmp-snooping group-limit 10 vlan 2
```

1.1.25. igmp-snooping group-policy

Use **igmp-snooping group-policy** to configure a multicast group policy on a port to control the multicast groups that hosts attached to the port can join.

Use **undo igmp-snooping group-policy** to delete multicast group policies on a port.

Syntax

igmp-snooping group-policy *ipv4-acl-number* [**vlan** *vlan-list*]

undo igmp-snooping group-policy [**vlan** *vlan-list*]

Default

No multicast group polices exist on a port. Hosts attached to the port can join any multicast groups.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

ipv4-acl-number: Specifies an IPv4 basic or advanced ACL by its number in the range of 2000 to 3999. Hosts can join only the multicast groups that the ACL permits. If the ACL does not exist or does not have valid rules, hosts cannot join multicast groups.

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The VLAN ID is in the range of 1 to 4094. If you do not specify a VLAN, this command takes effect on all VLANs.

Usage guidelines

A multicast group policy filters IGMP reports to control the multicast groups that hosts can join.

This command does not take effect on static member ports, because static member ports do not send IGMP reports.

You can configure a multicast group policy for a port in interface view or globally for all ports in IGMP-snooping view. For a port, the port-specific configuration takes priority over the global configuration.

When you configure a rule in the IPv4 ACL, follow these restrictions and guidelines:

- For the rule to take effect, do not specify the **vpn-instance** *vpn-instance* option.
- In a basic ACL, the **source** *source-address source-wildcard* option specifies a multicast group address.
- In an advanced ACL, the **source** *source-address source-wildcard* option specifies a multicast source address. The **destination** *dest-address dest-wildcard* option specifies a multicast group address.

  To match the following IGMP reports, set the **source** *source-address source-wildcard* option to 0.0.0.0:

  - IGMPv1 and IGMPv2 reports.
  - IGMPv3 IS_EX and IGMPv3 TO_EX reports that do not carry multicast source addresses.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

You can configure different ACLs on a port for different VLANs. If you configure multiple ACLs on a port for the same VLAN, the most recent configuration takes effect.

Examples

On GigabitEthernet 1/0/1, configure a multicast group policy for VLAN 2 so that hosts in VLAN 2 can join only multicast group 225.1.1.1.

```
<Switch> system-view
[Switch] acl basic 2000
[Switch-acl-ipv4-basic-2000] rule permit source 225.1.1.1 0
[Switch-acl-ipv4-basic-2000] quit
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] igmp-snooping group-policy 2000 vlan 2
```

Related commands

group-policy (IGMP-snooping view)

1.1.26. igmp-snooping host-aging-time

Use **igmp-snooping host-aging-time** to set the aging timer for dynamic member ports in a VLAN or VSI.

Use **undo igmp-snooping host-aging-time** to restore the default.

Syntax

igmp-snooping host-aging-time *seconds*

undo igmp-snooping host-aging-time

Default

The aging timer for dynamic member ports is 260 seconds.

Views

VLAN view

VSI view

Predefined user roles

network-admin

Parameters

seconds: Specifies an aging timer for dynamic member ports, in the range of 1 to 8097894 seconds.

Usage guidelines

You must enable IGMP snooping for a VLAN or VSI before you execute this command.

You can set the timer for a VLAN in VLAN view, for a VSI in VSI view, or globally for all VLANs and VSIs in IGMP-snooping view. For a VLAN, the VLAN-specific configuration takes priority over the global configuration. For a VSI, the VSI-specific configuration takes priority over the global configuration.

To avoid mistakenly deleting multicast group members, set the aging timer for dynamic member ports to be greater than the value calculated by using the following formula:

[IGMP general query interval] + [maximum response time for IGMP general queries]

As a best practice, set the aging timer of dynamic member ports to the value calculated by using the following formula:

[IGMP general query interval] × 2 + [maximum response time for IGMP general queries]

Examples

In VLAN 2, enable IGMP snooping, and set the aging timer for dynamic member ports to 300 seconds.

```
<Switch> system-view
[Switch] igmp-snooping
[Switch-igmp-snooping] quit
[Switch] vlan 2
[Switch-vlan2] igmp-snooping enable
[Switch-vlan2] igmp-snooping host-aging-time 300
```

In VSI **aaa**, enable IGMP snooping, and set the aging timer for dynamic member ports to 300 seconds.

```
<Switch> system-view
[Switch] igmp-snooping
[Switch-igmp-snooping] quit
[Switch] vsi aaa
[Switch-vsi-aaa] igmp-snooping enable
[Switch-vsi-aaa] igmp-snooping host-aging-time 300
```

Related commands

host-aging-time (IGMP-snooping view)

igmp-snooping enable

1.1.27. igmp-snooping host-join

Use **igmp-snooping host-join** to configure a port as a simulated member host for a multicast group.

Use **undo igmp-snooping host-join** to remove the configuration of a simulated member host for a multicast group.

Syntax

igmp-snooping host-join *group-address* [**source-ip** *source-address*] **vlan** *vlan-id*

undo igmp-snooping host-join { *group-address* [**source-ip** *source-address*] **vlan** *vlan-id* | **all** }

Default

A port is not configured as a simulated member host for multicast groups.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

group-address: Specifies a multicast group in the range of 224.0.1.0 to 239.255.255.255.

source-ip *source-address*: Specifies a multicast source by its IP address. If you specify a multicast source, this command configures the port as a simulated member host for a multicast source and group. If you do not specify a multicast source, this command configures the port as a simulated member host for a multicast group. This option takes effect on IGMPv3 snooping devices.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094.

all: Specifies all multicast groups.

Usage guidelines

The version of IGMP running on a simulated member host is the same as the version of IGMP snooping running on the port. The port ages out in the same way as a dynamic member port.

Examples

Configure GigabitEthernet 1/0/1 as a simulated member host of the multicast source and group (1.1.1.1, 232.1.1.1) in VLAN 2.

```
<Switch> system-view
[Switch] igmp-snooping
[Switch-igmp-snooping] quit
[Switch] vlan 2
[Switch-vlan2] igmp-snooping enable
[Switch-vlan2] igmp-snooping version 3
[Switch-vlan2] quit
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] igmp-snooping host-join 232.1.1.1 source-ip 1.1.1.1 vlan
2
```

1.1.28. igmp-snooping last-member-query-interval

Use **igmp-snooping last-member-query-interval** to set the IGMP last member query interval for a VLAN or VSI.

Use **undo igmp-snooping last-member-query-interval** to restore the default.

Syntax

igmp-snooping last-member-query-interval *interval*

undo igmp-snooping last-member-query-interval

Default

The IGMP last member query interval is 1 second.

Views

VLAN view

VSI view

Predefined user roles

network-admin

Parameters

interval: Specifies an IGMP last member query interval in the range of 1 to 25 seconds.

Usage guidelines

You must enable IGMP snooping for a VLAN or VSI before you execute this command.

You can set the interval for a VLAN in VLAN view, for a VSI in VSI view, or globally for all VLANs and VSIs in IGMP-snooping view. For a VLAN, the VLAN-specific configuration takes priority over the global configuration. For a VSI, the VSI-specific configuration takes priority over the global configuration.

Examples

In VLAN 2, enable IGMP snooping, and set the IGMP last member query interval to 3 seconds.

```
<Switch> system-view
[Switch] igmp-snooping
[Switch-igmp-snooping] quit
[Switch] vlan 2
```

```
[Switch-vlan2] igmp-snooping enable
[Switch-vlan2] igmp-snooping last-member-query-interval 3
```

In VSI **aaa**, enable IGMP snooping, and set the IGMP last member query interval to 3 seconds.

```
<Switch> system-view
[Switch] igmp-snooping
[Switch-igmp-snooping] quit
[Switch] vsi aaa
[Switch-vsi-aaa] igmp-snooping enable
[Switch-vsi-aaa] igmp-snooping last-member-query-interval 3
```

Related commands

igmp-snooping enable

last-member-query-interval (IGMP-snooping view)

1.1.29. igmp-snooping leave source-ip

Use **igmp-snooping leave source-ip** to configure the source IP address for IGMP leave messages.

Use **undo igmp-snooping leave source-ip** to restore the default.

Syntax

igmp-snooping leave source-ip *ip-address*

undo igmp-snooping leave source-ip

Default

In a VLAN, the source IP address of IGMP leave messages is the IP address of the current VLAN interface. If the current VLAN interface does not have an IP address, the source IP address is 0.0.0.0.

In a VSI, the source IP address of IGMP leave messages is the IP address of the gateway interface for the VSI. If the gateway interface does not have an IP address, the source IP address is 0.0.0.0.

Views

VLAN view

VSI view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the source IP address for IGMP leave messages.

Usage guidelines

You must enable IGMP snooping for a VLAN before you execute this command.

Examples

In VLAN 2, enable IGMP snooping, and specify 10.1.1.1 as the source IP address of IGMP leave messages.

```
<Switch> system-view
[Switch] igmp-snooping
[Switch-igmp-snooping] quit
```

```
[Switch] vlan 2
[Switch-vlan2] igmp-snooping enable
[Switch-vlan2] igmp-snooping leave source-ip 10.1.1.1
```

In VSI **aaa**, enable IGMP snooping, and specify 10.1.1.1 as the source IP address of IGMP leave messages.

```
<Switch> system-view
[Switch] igmp-snooping
[Switch-igmp-snooping] quit
[Switch] vsi aaa
[Switch-vsi-aaa] igmp-snooping enable
[Switch-vsi-aaa] igmp-snooping leave source-ip 10.1.1.1
```

Related commands

igmp-snooping enable

1.1.30. igmp-snooping max-response-time

Use **igmp-snooping max-response-time** to set the maximum response time for IGMP general queries in a VLAN or VSI.

Use **undo igmp-snooping max-response-time** to restore the default.

Syntax

igmp-snooping max-response-time *seconds*

undo igmp-snooping max-response-time

Default

The maximum response time for IGMP general queries is 10 seconds.

Views

VLAN view

VSI view

Predefined user roles

network-admin

Parameters

seconds: Specifies the maximum response time for IGMP general queries, in the range of 1 to 3174 seconds.

Usage guidelines

You must enable IGMP snooping for a VLAN or VSI before you execute this command.

You can set the time for a VLAN in VLAN view, for a VSI in VSI view, or globally for all VLANs and VSIs in IGMP-snooping view. For a VLAN, the VLAN-specific configuration takes priority over the global configuration. For a VSI, the VSI-specific configuration takes priority over the global configuration.

To avoid mistakenly deleting multicast group members, set the maximum response time for IGMP general queries to be less than the IGMP general query interval.

Examples

In VLAN 2, enable IGMP snooping, and set the maximum response time for IGMP general queries to 5 seconds.

```
<Switch> system-view
[Switch] igmp-snooping
[Switch-igmp-snooping] quit
[Switch] vlan 2
[Switch-vlan2] igmp-snooping enable
[Switch-vlan2] igmp-snooping max-response-time 5
```

In VSI **aaa**, enable IGMP snooping, and set the maximum response time for IGMP general queries to 5 seconds.

```
<Switch> system-view
[Switch] igmp-snooping
[Switch-igmp-snooping] quit
[Switch] vsi aaa
[Switch-vsi-aaa] igmp-snooping enable
[Switch-vsi-aaa] igmp-snooping max-response-time 5
```

Related commands

igmp-snooping enable

igmp-snooping query-interval

max-response-time (IGMP-snooping view)

1.1.31. igmp-snooping overflow-replace

Use **igmp-snooping overflow-replace** to enable multicast group replacement on a port.

Use **undo igmp-snooping overflow-replace** to disable multicast group replacement on a port.

Syntax

igmp-snooping overflow-replace [**vlan** *vlan-list*]

undo igmp-snooping overflow-replace [**vlan** *vlan-list*]

Default

Multicast group replacement is disabled.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The VLAN ID is in the range of 1 to 4094. If you do not specify a VLAN, this command takes effect on all VLANs.

Usage guidelines

This command takes effect only on the multicast groups that a port joins dynamically.

You can enable multicast group replacement for a port in interface view or globally for all ports in IGMP-snooping view. For a port, the port-specific configuration takes priority over the global configuration.

Examples

On GigabitEthernet 1/0/1, enable multicast group replacement for VLAN 2.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] igmp-snooping overflow-replace vlan 2
```

Related commands

overflow-replace (IGMP-snooping view)

1.1.32. igmp-snooping proxy enable

Use **igmp-snooping proxy enable** to enable IGMP snooping proxying for a VLAN or VSI.

Use **undo igmp-snooping proxy enable** to disable IGMP snooping proxying for a VLAN or VSI.

Syntax

igmp-snooping proxy enable

undo igmp-snooping proxy enable

Default

IGMP snooping proxying is disabled.

Views

VLAN view

VSI view

Predefined user roles

network-admin

Usage guidelines

You must enable IGMP snooping for a VLAN or VSI before you execute this command.

This command does not take effect on a VLAN that is a sub-VLAN of a multicast VLAN.

Examples

In VLAN 2, enable IGMP snooping, and enable IGMP snooping proxying.

```
<Switch> system-view
[Switch] igmp-snooping
[Switch-igmp-snooping] quit
[Switch] vlan 2
[Switch-vlan2] igmp-snooping enable
[Switch-vlan2] igmp-snooping proxy enable
```

In VSI **aaa**, enable IGMP snooping, and enable IGMP snooping proxying.

```
<Switch> system-view
[Switch] igmp-snooping
[Switch-igmp-snooping] quit
[Switch] vsi aaa
[Switch-vsi-aaa] igmp-snooping enable
[Switch-vsi-aaa] igmp-snooping proxy enable
```

Related commands

igmp-snooping enable

subvlan (multicast-VLAN view)

1.1.33. igmp-snooping querier

Use **igmp-snooping querier** to enable the IGMP snooping querier.

Use **undo igmp-snooping querier** to disable the IGMP snooping querier.

Syntax

igmp-snooping querier

undo igmp-snooping querier

Default

The IGMP snooping querier is disabled.

Views

VLAN view

VSI view

Predefined user roles

network-admin

Usage guidelines

You must enable IGMP snooping for a VLAN or VSI before you execute this command.

For a sub-VLAN of a multicast VLAN, this command takes effect only after you remove the sub-VLAN from the multicast VLAN.

Examples

In VLAN 2, enable IGMP snooping, and enable the IGMP snooping querier.

```
<Switch> system-view
[Switch] igmp-snooping
[Switch-igmp-snooping] quit
[Switch] vlan 2
[Switch-vlan2] igmp-snooping enable
[Switch-vlan2] igmp-snooping querier
```

In VSI **aaa**, enable IGMP snooping, and enable the IGMP snooping querier.

```
<Switch> system-view
[Switch] igmp-snooping
[Switch-igmp-snooping] quit
[Switch] vsi aaa
[Switch-vsi-aaa] igmp-snooping enable
[Switch-vsi-aaa] igmp-snooping querier
```

Related commands

igmp-snooping enable

subvlan (multicast VLAN view)

Related commands

igmp-snooping querier

1.1.34. igmp-snooping query-interval

Use **igmp-snooping query-interval** to set the IGMP general query interval for a VLAN or VSI.

Use **undo igmp-snooping query-interval** to restore the default.

Syntax

igmp-snooping query-interval *interval*

undo igmp-snooping query-interval

Default

The IGMP general query interval is 125 seconds.

Views

VLAN view

VSI view

Predefined user roles

network-admin

Parameters

interval: Specifies an IGMP general query interval in the range of 2 to 31744 seconds.

Usage guidelines

You must enable IGMP snooping for a VLAN or VSI before you execute this command.

To avoid mistakenly deleting multicast group members, set the IGMP general query interval to be greater than the maximum response time for IGMP general queries.

Examples

In VLAN 2, enable IGMP snooping, and set the IGMP general query interval to 20 seconds.

```
<Switch> system-view
[Switch] igmp-snooping
[Switch-igmp-snooping] quit
[Switch] vlan 2
[Switch-vlan2] igmp-snooping enable
[Switch-vlan2] igmp-snooping query-interval 20
```

In VSI **aaa**, enable IGMP snooping, and set the IGMP general query interval to 20 seconds.

```
<Switch> system-view
[Switch] igmp-snooping
[Switch-igmp-snooping] quit
[Switch] vsi aaa
[Switch-vsi-aaa] igmp-snooping enable
[Switch-vsi-aaa] igmp-snooping query-interval 20
```

Related commands

igmp-snooping enable

igmp-snooping max-response-time

igmp-snooping querier

max-response-time

1.1.35. igmp-snooping report source-ip

Use **igmp-snooping report source-ip** to configure the source IP address for IGMP reports.

Use **undo igmp-snooping report source-ip** to restore the default.

Syntax

igmp-snooping report source-ip *ip-address*

undo igmp-snooping report source-ip

Default

In a VLAN, the source IP address of IGMP reports is the IP address of the current VLAN interface. If the current VLAN interface does not have an IP address, the source IP address is 0.0.0.0.

In a VSI, the source IP address of IGMP reports is the IP address of the gateway interface for the VSI. If the gateway interface does not have an IP address, the source IP address is 0.0.0.0.

Views

VLAN view

VSI view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the source IP address for IGMP reports.

Usage guidelines

You must enable IGMP snooping for a VLAN before you execute this command.

Examples

In VLAN 2, enable IGMP snooping, and specify 10.1.1.1 as the source IP address of IGMP reports.

```
<Switch> system-view
[Switch] igmp-snooping
[Switch-igmp-snooping] quit
[Switch] vlan 2
[Switch-vlan2] igmp-snooping enable
[Switch-vlan2] igmp-snooping report source-ip 10.1.1.1
```

In VSI **aaa**, enable IGMP snooping, and specify 10.1.1.1 as the source IP address of IGMP reports.

```
<Switch> system-view
[Switch] igmp-snooping
[Switch-igmp-snooping] quit
[Switch] vsi aaa
[Switch-vsi-aaa] igmp-snooping enable
[Switch-vsi-aaa] igmp-snooping report source-ip 10.1.1.1
```

Related commands

igmp-snooping enable

1.1.36. igmp-snooping router-aging-time

Use **igmp-snooping router-aging-time** to set the aging timer for dynamic router ports in a VLAN or VSI.

Use **undo igmp-snooping router-aging-time** to restore the default.

Syntax

igmp-snooping router-aging-time *seconds*

undo igmp-snooping router-aging-time

Default

The aging timer for dynamic router ports is 260 seconds.

Views

VLAN view

VSI view

Predefined user roles

network-admin

Parameters

seconds: Specifies an aging timer for dynamic router ports, in the range of 1 to 8097894 seconds.

Usage guidelines

You must enable IGMP snooping for a VLAN or VSI before you execute this command.

You can set the timer for a VLAN in VLAN view, for a VSI in VSI view, or globally for all VLANs and VSIs in IGMP-snooping view. For a VLAN, the VLAN-specific configuration takes priority over the global configuration. For a VSI, the VSI-specific configuration takes priority over the global configuration.

Examples

In VLAN 2, enable IGMP snooping, and set the aging timer for dynamic router ports to 100 seconds.

```
<Switch> system-view
[Switch] igmp-snooping
[Switch-igmp-snooping] quit
[Switch] vlan 2
[Switch-vlan2] igmp-snooping enable
[Switch-vlan2] igmp-snooping router-aging-time 100
```

In VSI **aaa**, enable IGMP snooping, and set the aging timer for dynamic router ports to 100 seconds.

```
<Switch> system-view
[Switch] igmp-snooping
[Switch-igmp-snooping] quit
[Switch] vsi aaa
[Switch-vsi-aaa] igmp-snooping enable
[Switch-vsi-aaa] igmp-snooping router-aging-time 100
```

Related commands

igmp-snooping enable

router-aging-time (IGMP-snooping view)

1.1.37. igmp-snooping source-deny

Use **igmp-snooping source-deny** to enable multicast source port filtering on a port to discard all multicast data packets.

Use **undo igmp-snooping source-deny** to disable multicast source port filtering on a port.

Syntax

igmp-snooping source-deny

undo igmp-snooping source-deny

Default

Multicast source port filtering is disabled.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

You can enable this feature for a port in interface view or for the specified ports in IGMP-snooping view. For a port, the configuration in interface view has the same priority as the configuration in IGMP-snooping view, and the most recent configuration takes effect.

Examples

Enable source port filtering for multicast data on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] igmp-snooping source-deny
```

Related commands

source-deny (IGMP-snooping view)

1.1.38. igmp-snooping special-query source-ip

Use **igmp-snooping special-query source-ip** to configure the source IP address for IGMP group-specific queries.

Use **undo igmp-snooping special-query source-ip** to restore the default.

Syntax

igmp-snooping special-query source-ip *ip-address*

undo igmp-snooping special-query source-ip

Default

In a VLAN, the source IP address of IGMP group-specific queries is one of the following:

- The source address of IGMP group-specific queries if the IGMP snooping querier of the VLAN has received IGMP general queries.
- The IP address of the current VLAN interface if the IGMP snooping querier does not receive an IGMP general query.
- 0.0.0.0 if the IGMP snooping querier does not receive an IGMP general query and the current VLAN interface does not have an IP address.

In a VSI, the source IP address of IGMP group-specific queries is one of the following:

- The source IP address of IGMP general queries if the IGMP snooping querier of the VSI has received IGMP general queries.
- The IP address of the gateway interface for the VSI if the IGMP snooping querier does not receive an IGMP general query.
- 0.0.0.0 if the gateway interface for the VSI does not have an IP address.

Views

VLAN view

VSI view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the source IP address for IGMP group-specific queries.

Usage guidelines

You must enable IGMP snooping for a VLAN or VSI before you execute this command.

Examples

In VLAN 2, enable IGMP snooping, and specify 10.1.1.1 as the source IP address of IGMP group-specific queries.

```
<Switch> system-view
[Switch] igmp-snooping
[Switch-igmp-snooping] quit
[Switch] vlan 2
[Switch-vlan2] igmp-snooping enable
[Switch-vlan2] igmp-snooping special-query source-ip 10.1.1.1
```

In VSI **aaa**, enable IGMP snooping, and specify 10.1.1.1 as the source IP address of IGMP group-specific queries.

```
<Switch> system-view
[Switch] igmp-snooping
[Switch-igmp-snooping] quit
[Switch] vsi aaa
[Switch-vsi-aaa] igmp-snooping enable
[Switch-vsi-aaa] igmp-snooping special-query source-ip 10.1.1.1
```

Related commands

igmp-snooping enable

1.1.39. igmp-snooping static-group

Use **igmp-snooping static-group** to configure a port as a static member port of a multicast group.

Use **undo igmp-snooping static-group** to remove the configuration of static member ports.

Syntax

igmp-snooping static-group *group-address* [**source-ip** *source-address*] **vlan** *vlan-id*

undo igmp-snooping static-group { *group-address* [**source-ip** *source-address*] **vlan** *vlan-id* | **all** }

Default

A port is not a static member port of a multicast group.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

group-address: Specifies a multicast group address in the range of 224.0.1.0 to 239.255.255.255.

source-ip *source-address*: Specifies a multicast source by its IP address. If you specify a multicast source, this command configures the port as a static member port for a multicast source and group. If you do not specify a multicast source, this command configures the port as a static member port for a multicast group. This option takes effect on IGMPv3 snooping devices.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094.

all: Specifies all multicast groups.

Examples

Configure GigabitEthernet 1/0/1 as a static member port of the multicast source and group (1.1.1.1, 225.0.0.1) in VLAN 2.

```
<Switch> system-view
[Switch] igmp-snooping
[Switch-igmp-snooping] quit
[Switch] vlan 2
[Switch-vlan2] igmp-snooping enable
[Switch-vlan2] igmp-snooping version 3
[Switch-vlan2] quit
[Switch] interface GigabitEthernet 1/0/1
[Switch-GigabitEthernet1/0/1] igmp-snooping static-group 225.0.0.1 source-ip 1.1.1.1
vlan 2
```

1.1.40. igmp-snooping static-router-port

Use **igmp-snooping static-router-port** to configure a port as a static router port.

Use **undo igmp-snooping static-router-port** to remove the configuration of static router ports.

Syntax

igmp-snooping static-router-port vlan *vlan-id*

undo igmp-snooping static-router-port { **all** | **vlan** *vlan-id* }

Default

A port is not a static router port.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

all: Specifies all VLANs.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094.

Examples

Configure GigabitEthernet 1/0/1 as a static router port in VLAN 2.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] igmp-snooping static-router-port vlan 2
```

1.1.41. igmp-snooping version

Use **igmp-snooping version** to specify an IGMP snooping version for a VLAN or VSI.

Use **undo igmp-snooping version** to restore the default.

Syntax

igmp-snooping version *version-number*

undo igmp-snooping version

Default

The IGMP snooping version in a VLAN or VSI is 2.

Views

VLAN view

VSI view

Predefined user roles

network-admin

Parameters

version-number: Specifies an IGMP snooping version, 2 or 3.

Usage guidelines

You must enable IGMP snooping for a VLAN or VSI before you execute this command.

You can specify the version for a VLAN in VLAN view or for the specified VLANs in IGMP-snooping view. The VLAN-specific configuration has the same priority as the configuration in IGMP-snooping view, and the most recent configuration takes effect.

Examples

In VLAN 2, enable IGMP snooping, and specify IGMP snooping version 3.

```
<Switch> system-view
[Switch] igmp-snooping
[Switch-igmp-snooping] quit
[Switch] vlan 2
[Switch-vlan2] igmp-snooping enable
[Switch-vlan2] igmp-snooping version 3
```

In VSI **aaa**, enable IGMP snooping, and specify IGMP snooping version 3.

```
<Switch> system-view
[Switch] igmp-snooping
[Switch-igmp-snooping] quit
[Switch] vsi aaa
[Switch-vsi-aaa] igmp-snooping enable
[Switch-vsi-aaa] igmp-snooping version 3
```

Related commands

igmp-snooping enable

1.1.42. last-member-query-interval (IGMP-snooping view)

Use **last-member-query-interval** to set the IGMP last member query interval globally.

Use **undo last-member-query-interval** to restore the default.

Syntax

last-member-query-interval *interval*

undo last-member-query-interval

Default

The IGMP last member query interval is 1 second.

Views

IGMP-snooping view

Predefined user roles

network-admin

Parameters

interval: Specifies an IGMP last member query interval in the range of 1 to 25 seconds.

Usage guidelines

You can set the interval for a VLAN in VLAN view, for a VSI in VSI view, or globally for all VLANs and VSIs in IGMP-snooping view. For a VLAN, the VLAN-specific configuration takes priority over the global configuration. For a VSI, the VSI-specific configuration takes priority over the global configuration.

Examples

Set the global IGMP last member query interval to 3 seconds.

```
<Switch> system-view
[Switch] igmp-snooping
[Switch-igmp-snooping] last-member-query-interval 3
```

Related commands

igmp-snooping last-member-query-interval

1.1.43. mac-address multicast

Use **mac-address multicast** to configure a static multicast MAC address entry.

Use **undo mac-address multicast** to delete a static multicast MAC address entry.

Syntax

In system view:

mac-address multicast *mac-address* **interface** *interface-list* **vlan** *vlan-id*

undo mac-address [**multicast**] [[*mac-address* [**interface** *interface-list*]] **vlan** *vlan-id*]

In Layer 2 aggregate interface view or Layer 2 Ethernet interface view:

mac-address multicast *mac-address* **vlan** *vlan-id*

undo mac-address [**multicast**] *mac-address* **vlan** *vlan-id*

Default

No static multicast MAC address entries exist.

Views

System view

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

mac-address: Specifies a static multicast MAC address, in the format of H-H-H. You must specify an unused multicast MAC address. A multicast MAC address is a MAC address in which the least significant bit of the most significant octet is 1.

interface *interface-list*: Specifies a space-separated list of up to four interface items. Each item specifies an interface or an interface list in the format of *start-interface-type interface-number* **to** *end-interface-type interface-number*. The *interface-type interface-number* argument specifies an interface by its type and number. The available interface types include Layer 2 Ethernet interfaces and Layer 2 aggregate interfaces.

vlan *vlan-id*: Specifies an existing VLAN by its VLAN ID in the range of 1 to 4094. The system gives a prompt if the specified interface does not belong to the VLAN.

Usage guidelines

You do not need to enable IP multicast routing before you execute this command.

You can configure static multicast MAC address entries for the specified interfaces in system view or for the current interface in interface view.

If you do not specify the **multicast** keyword in the **undo mac-address** command, all static unicast MAC address entries and static multicast MAC entries are deleted.

Examples

Configure a static multicast MAC address entry. In the entry, the multicast MAC address is 0100-0001-0001 and the outgoing ports are GigabitEthernet 1/0/1 through GigabitEthernet 1/0/5 in VLAN 2.

```
<Switch> system-view
[Switch] mac-address multicast 0100-0001-0001 interface gigabitethernet 1/0/1 to
gigabitethernet 1/0/5 vlan 2
```

Configure a static multicast MAC address entry on GigabitEthernet 1/0/1. In the entry, the multicast MAC address is 0100-0001-0001 and the outgoing port is GigabitEthernet 1/0/1, which belongs to VLAN 2.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] mac-address multicast 0100-0001-0001 vlan 2
```

Related commands

display mac-address multicast

1.1.44. max-response-time (IGMP-snooping view)

Use **max-response-time** to set the maximum response time for IGMP general queries globally.

Use **undo max-response-time** to restore the default.

Syntax

max-response-time *seconds*

undo max-response-time

Default

The maximum response time for IGMP general queries is 10 seconds.

Views

IGMP-snooping view

Predefined user roles

network-admin

Parameters

seconds: Specifies the maximum response time for IGMP general queries, in the range of 1 to 3174 seconds.

Usage guidelines

You can set the time for a VLAN in VLAN view, for a VSI in VSI view, or globally for all VLANs and VSIs in IGMP-snooping view. For a VLAN, the VLAN-specific configuration takes priority over the global configuration. For a VSI, the VSI-specific configuration takes priority over the global configuration.

To avoid mistakenly deleting multicast group members, set the maximum response time for IGMP general queries to be less than the IGMP general query interval.

Examples

Set the global maximum response time for IGMP general queries to 5 seconds.

```
<Switch> system-view
[Switch] igmp-snooping
[Switch-igmp-snooping] max-response-time 5
```

Related commands

igmp-snooping max-response-time

igmp-snooping query-interval

1.1.45. overflow-replace (IGMP-snooping view)

Use **overflow-replace** to enable the multicast group replacement feature globally.

Use **undo overflow-replace** to disable the multicast group replacement feature globally.

Syntax

overflow-replace [**vlan** *vlan-list*]

undo overflow-replace [**vlan** *vlan-list*]

Default

The multicast group replacement feature is disabled.

Views

IGMP-snooping view

Predefined user roles

network-admin

Parameters

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The VLAN ID is in the range of 1 to 4094. If you do not specify a VLAN, this command takes effect on all VLANs.

Usage guidelines

This command takes effect only on the multicast groups that a port joins dynamically.

You can enable the multicast group replacement feature globally for all ports in IGMP-snooping view or for a port in interface view. For a port, the port-specific configuration takes priority over the global configuration.

Examples

Globally enable the multicast group replacement feature for VLAN 2.

```
<Switch> system-view
[Switch] igmp-snooping
[Switch-igmp-snooping] overflow-replace vlan 2
```

Related commands

igmp-snooping overflow-replace

1.1.46. report-aggregation (IGMP-snooping view)

Use **report-aggregation** to enable IGMP report suppression.

Use **undo report-aggregation** to disable IGMP report suppression.

Syntax

report-aggregation

undo report-aggregation

Default

IGMP report suppression is enabled.

Views

IGMP-snooping view

Predefined user roles

network-admin

Examples

Disable IGMP report suppression.

```
<Switch> system-view
[Switch] igmp-snooping
[Switch-igmp-snooping] undo report-aggregation
```

1.1.47. reset igmp-snooping group

Use **reset igmp-snooping group** to clear information about dynamic IGMP snooping group entries.

Syntax

reset igmp-snooping group { *group-address* [*source-address*] | **all** } [**vlan** *vlan-id* | **vsi** *vsi-name*]

Views

User view

Predefined user roles

network-admin

Parameters

group-address: Specifies a multicast group address in the range of 224.0.1.0 to 239.255.255.255.

source-address: Specifies a multicast source address. If you do not specify a multicast source, this command clears information about dynamic IGMP snooping group entries for all multicast sources.

all: Specifies all multicast groups.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command clears information about dynamic IGMP snooping group entries for all VLANs.

vsi *vsi-name*: Specifies a VSI by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VSI, this command clears information about dynamic IGMP snooping group entries for all VSIs.

Examples

Clear information about all dynamic IGMP snooping group entries.

```
<Switch> reset igmp-snooping group all
```

Related commands

display igmp-snooping group

1.1.48. reset igmp-snooping router-port

Use **reset igmp-snooping router-port** to clear dynamic router port information.

Syntax

reset igmp-snooping router-port { **all** | **vlan** *vlan-id* | **vsi** *vsi-name* }

Views

User view

Predefined user roles

network-admin

Parameters

all: Specifies all dynamic router ports.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command clears dynamic router port information for all VLANs.

vsi *vsi-name*: Specifies a VSI by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VSI, this command clears dynamic router port information for all VSIs.

Examples

Clear dynamic router port information.

```
<Switch> reset igmp-snooping router-port all
```

Related commands

display igmp-snooping router-port

1.1.49. reset igmp-snooping statistics

Use **reset igmp-snooping statistics** to clear statistics for IGMP messages and PIMv2 hello messages learned through IGMP snooping.

Syntax

reset igmp-snooping statistics

Views

User view

Predefined user roles

network-admin

Examples

Clear the statistics for all IGMP messages and PIMv2 hello messages learned through IGMP snooping.

```
<Switch> reset igmp-snooping statistics
```

Related commands

display igmp-snooping statistics

1.1.50. router-aging-time (IGMP-snooping view)

Use **router-aging-time** to set the aging timer for dynamic router ports globally.

Use **undo router-aging-time** to restore the default.

Syntax

router-aging-time *seconds*

undo router-aging-time

Default

The aging timer for dynamic router ports is 260 seconds.

Views

IGMP-snooping view

Predefined user roles

network-admin

Parameters

seconds: Specifies an aging timer for dynamic router ports, in the range of 1 to 8097894 seconds.

Usage guidelines

You can set the timer globally for all VLANs and VSIs in IGMP-snooping view, for a VSI in VSI view, or for a VLAN in VLAN view. For a VSI, the VSI-specific configuration takes priority over the global configuration. For a VLAN, the VLAN-specific configuration takes priority over the global configuration.

Examples

Set the global aging timer for dynamic router ports to 100 seconds.

```
<Switch> system-view
[Switch] igmp-snooping
[Switch-igmp-snooping] router-aging-time 100
```

Related commands

igmp-snooping router-aging-time

1.1.51. source-deny (IGMP-snooping view)

Use **source-deny** to enable multicast source port filtering on ports to discard all multicast data packets.

Use **undo source-deny** to disable multicast source port filtering on ports.

Syntax

source-deny port *interface-list*

undo source-deny port *interface-list*

Default

Multicast source port filtering is disabled.

Views

IGMP-snooping view

Predefined user roles

network-admin

Parameters

port *interface-list*: Specifies a space-separated list of port items. Each item specifies a port by its port type and number or a range of ports in the form of *start-interface-type interface-number* **to** *end-interface-type interface-number*.

Usage guidelines

You can enable this feature for the specified ports in IGMP-snooping view or for a port in interface view. For a port, the configuration in IGMP-snooping view has the same priority as the configuration in interface view, and the most recent configuration takes effect.

Examples

Enable multicast source port filtering on ports GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4.

```
<Switch> system-view
[Switch] igmp-snooping
[Switch-igmp-snooping] source-deny port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
```

Related commands

igmp-snooping source-deny

Contents

A page of this section is **6-x-x**

2. Multicast VLAN commands 2-1
2.1. Multicast VLAN commands 2-1
2.1.1. display multicast-vlan 2-1
2.1.2. display multicast-vlan forwarding-table 2-2
2.1.3. display multicast-vlan group 2-3
2.1.4. multicast-vlan 2-5
2.1.5. multicast-vlan entry-limit 2-6
2.1.6. port (multicast-VLAN view) 2-7
2.1.7. port multicast-vlan 2-7
2.1.8. reset multicast-vlan group 2-8
2.1.9. subvlan (multicast-VLAN view) 2-9

2. Multicast VLAN commands

2.1. Multicast VLAN commands

2.1.1. display multicast-vlan

Use **display multicast-vlan** to display information about multicast VLANs.

Syntax

display multicast-vlan [*vlan-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vlan-id: Specifies a multicast VLAN ID in the range of 1 to 4094. If you do not specify a multicast VLAN ID, this command displays information about all multicast VLANs.

Examples

Display information about all multicast VLANs.

```
<Switch> display multicast-vlan
Total 2 multicast VLANs.

Multicast VLAN 100:
  Sub-VLAN list(3 in total):
    2-3, 6
  Port list(3 in total):
    GE1/0/1
    GE1/0/2
    GE1/0/3

Multicast VLAN 200:
  Sub-VLAN list(0 in total):
  Port list(0 in total):
```

Table 2-1 Command output

Field	Description
Total 2 multicast VLANs	Total number of multicast VLANs.
Sub-VLAN list(3 in total)	Sub-VLAN list of the multicast VLAN, and the total number of the sub-VLANs.
Port list(3 in total)	Port list of the multicast VLAN, and the total number of the ports.

2.1.2. display multicast-vlan forwarding-table

Use **display multicast-vlan forwarding-table** to display multicast VLAN forwarding entries.

Syntax

display multicast-vlan forwarding-table [*group-address* [**mask** { *mask-length* | *mask* }] | *source-address* [**mask** { *mask-length* | *mask* }] | **slot** *slot-number* | **subvlan** *vlan-id* | **vlan** *vlan-id*] *

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

group-address: Specifies a multicast group by its IP address in the range of 224.0.0.0 to 239.255.255.255. If you do not specify a multicast group, this command displays multicast VLAN forwarding entries for all multicast groups.

mask { *mask-length* | *mask* }: Specifies a mask length or subnet mask for the multicast group address. The value range for the *mask-length* argument is 4 to 32 (default), and the default value for the *mask* argument is 255.255.255.255.

source-address: Specifies a multicast source by its IP address. If you do not specify a multicast source, this command displays multicast VLAN forwarding entries for all multicast sources.

mask { *mask-length* | *mask* }: Specifies a mask length or subnet mask for the multicast source address. The value range for the *mask-length* argument is 0 to 32 (default), and the default value for the *mask* argument is 255.255.255.255.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays multicast VLAN forwarding entries for the master device.

subvlan *vlan-id*: Specifies a sub-VLAN by its VLAN ID. If you do not specify a sub-VLAN, this command displays multicast VLAN forwarding entries for all sub-VLANs.

vlan *vlan-id*: Specifies a multicast VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a multicast VLAN, this command displays multicast VLAN forwarding entries for all multicast VLANs.

Examples

Display all multicast VLAN forwarding entries.

```
<Switch> display multicast-vlan forwarding-table
Multicast VLAN 100 Forwarding Table
Total 1 entries, 1 matched

00001. (1.1.1.1, 225.0.0.1)
     Flags: 0x10000
     Multicast VLAN: 100
     List of sub-VLANs (3 in total):
       1: VLAN 10
       2: VLAN 20
```

```
3: VLAN 30
```

Table 2-2 Command output

Field	Description
Multicast VLAN 100 Forwarding Table	Forwarding entries for multicast VLAN 100.
Total 1 entries, 1 matched	Total number of (S, G) entries, and the number of matching entries.
00001	Sequence number of the (S, G) entry.
(1.1.1.1, 255.0.0.1)	(S, G) entry, where **0.0.0.0** in the S position means all multicast sources.
Flags	Entry flag. This field displays one flag or the sum of multiple flags. In this example, the value 0x10000 means that the entry has only one flag 0x10000. The following flags are available for an entry: • **0x1**—The entry is in inactive state. • **0x4**—The entry fails to update. • **0x8**—The sub-VLAN information fails to update for the entry. • **0x200**—The entry is in GR state. • **0x10000**—The entry is a multicast VLAN forwarding entry.
List of sub-VLANs (3 in total)	Sub-VLAN list of the multicast VLAN, and the total number of the sub-VLANs.

2.1.3. display multicast-vlan group

Use **display multicast-vlan group** to display information about multicast groups in multicast VLANs.

Syntax

display multicast-vlan group [*source-address* | *group-address* | **slot** *slot-number* | **verbose** | **vlan** *vlan-id*] *

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

source-address: Specifies a multicast source by its IP address. If you do not specify a multicast source, this command displays information about multicast groups for all multicast sources in multicast VLANs.

group-address: Specifies a multicast group by its IP address in the range of 224.0.1.0 to 239.255.255.255. If you do not specify a multicast group, this command displays information for all multicast groups in multicast VLANs.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information about multicast groups in multicast VLANs for the master device.

verbose: Displays detailed information.

vlan *vlan-id*: Specifies a multicast VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a multicast VLAN, this command displays information about multicast groups for all multicast VLANs.

Examples

Display detailed information about all multicast groups in multicast VLANs.

```
<Switch> display multicast-vlan group verbose
Total 6 entries.

Multicast VLAN 10: Total 3 entries.
  (2.2.2.2, 225.1.1.2)
    Flags: 0x70000020
    Sub-VLANs (1 in total):
      VLAN 40
  (111.112.113.115, 225.1.1.4)
    Flags: 0x70000030
    Sub-VLANs (1 in total):
      VLAN 40
  (0.0.0.0, 226.1.1.6)
    Flags: 0x60000020
    Sub-VLANs (1 in total):
      VLAN 40

Multicast VLAN 20: Total 3 entries.
  (2.2.2.2, 225.1.1.2)
    Flags: 0x70000010
    Sub-VLANs (0 in total):
  (111.112.113.115, 225.1.1.4)
    Flags: 0x70000010
    Sub-VLANs (0 in total):
  (0.0.0.0, 226.1.1.6)
    Flags: 0x50000010
    Sub-VLANs (0 in total):
```

Table 2-3 Command output

Field	Description
Total 6 entries	Total number of (S, G) entries.
Multicast VLAN 10: Total 3 entries	Total number of (S, G) entries in multicast VLAN 10.
(0.0.0.0, 226.1.1.6)	(S, G) entry, where **0.0.0.0** in the S position means all multicast sources.
Flags	Entry flag. This field displays one flag or the sum of multiple flags. For example, the value 0x70000020 means that the entry has flags 0x20, 0x10000000, 0x20000000, and

Field	Description

	0x40000000.
	The following flags are available for an entry:
	• **0x10**—The entry is created by the multicast VLAN.
	• **0x20**—The entry is created by the sub-VLAN of the multicast VLAN.
	• **0x40**—The entry is to be deleted.
	• **0x10000000**—This value represents one of the following situations:
	  ○ The entry is newly created.
	  ○ The device receives an IGMP query that matches the (S, G) entry but does not receive any matching IGMPv1 reports within an IGMP general query interval.
	• **0x20000000**—The device does not receive IGMPv2 or IGMPv3 reports that match the (S, G) entry within an IGMP general query interval.
	• **0x40000000**—The device does not receive IGMPv3 IS_EX (NULL) reports that match the (S, G) entry within an IGMP general query interval.

Sub-VLANs (1 in total)	Sub-VLAN list of the multicast VLAN, and the total number of the sub-VLANs.

Related commands

reset multicast-vlan group

2.1.4. multicast-vlan

Use **multicast-vlan** to configure a multicast VLAN and enter its view, or enter the view of an existing multicast VLAN.

Use **undo multicast-vlan** to remove the configuration of multicast VLANs.

Syntax

multicast-vlan *vlan-id*

undo multicast-vlan { **all** | *vlan-id* }

Default

No multicast VLANs exist.

Views

System view

Predefined user roles

network-admin

Parameters

vlan-id: Specifies an existing VLAN by its ID in the range of 1 to 4094.

all: Specifies all multicast VLANs.

Usage guidelines

The total number of multicast VLANs on a device cannot exceed the system upper limit.

You must enable IGMP snooping for the VLAN to be configured as a multicast VLAN.

As a best practice, do not configure a multicast VLAN on a device that is enabled with IP multicast routing.

Examples

Enable IGMP snooping for VLAN 100. Configure VLAN 100 as a multicast VLAN and enter its view.

```
<Switch> system-view
[Switch] igmp-snooping
[Switch-igmp-snooping] quit
[Switch] vlan 100
[Switch-vlan100] igmp-snooping enable
[Switch-vlan100] quit
[Switch] multicast-vlan 100
[Switch-mvlan-100]
```

Related commands

igmp-snooping enable

multicast routing

2.1.5. multicast-vlan entry-limit

Use **multicast-vlan entry-limit** to set the maximum number of multicast VLAN forwarding entries.

Use **undo multicast-vlan entry-limit** to restore the default.

Syntax

multicast-vlan entry-limit *limit*

undo multicast-vlan entry-limit

Default

The maximum number of multicast VLAN forwarding entries is 4000.

Views

System view

Predefined user roles

network-admin

Parameters

limit: Specifies the maximum number of multicast VLAN forwarding entries, in the range of 0 to 4000.

Examples

Set the maximum number of multicast VLAN forwarding entries to 128.

```
<Switch> system-view
[Switch] multicast-vlan entry-limit 128
```

Related commands

entry-limit (IGMP-snooping view)

2.1.6. port (multicast-VLAN view)

Use **port** to assign user ports to a multicast VLAN.

Use **undo port** to delete user ports from a multicast VLAN.

Syntax

port *interface-list*

undo port { **all** | *interface-list* }

Default

A multicast VLAN does not have user ports.

Views

Multicast VLAN view

Predefined user roles

network-admin

Parameters

interface-list: Specifies a port in the form of *interface-type interface-number*, or a port range in the form of *interface-type interface-number* to *interface-type interface-number*.

all: Specifies all user ports in the current multicast VLAN.

Usage guidelines

You can assign only Layer 2 Ethernet ports or Layer 2 aggregate interfaces to multicast VLANs. Additionally, you can assign a port to only one multicast VLAN.

For ports to be assigned to a multicast VLAN, you must enable IGMP snooping for the VLANs to which the ports belong.

Examples

Assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 as user ports to multicast VLAN 100.

```
<Switch> system-view
[Switch] multicast-vlan 100
[Switch-mvlan-100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/3
```

2.1.7. port multicast-vlan

Use **port multicast-vlan** to assign a user port to a multicast VLAN.

Use **undo port multicast-vlan** to restore the default.

Syntax

port multicast-vlan *vlan-id*

undo port multicast-vlan

Default

A port does not belong to a multicast VLAN.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

vlan-id: Specifies a multicast VLAN by its VLAN ID in the range of 1 to 4094.

Usage guidelines

You can assign a port to only one multicast VLAN.

For a port to be assigned to a multicast VLAN, you must enable IGMP snooping for the VLAN to which the port belongs.

Examples

Assign GigabitEthernet 1/0/1 as a user port to multicast VLAN 100.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port multicast-vlan 100
```

2.1.8. reset multicast-vlan group

Use **reset multicast-vlan group** to clear multicast groups in multicast VLANs.

Syntax

reset multicast-vlan group [*source-address* [**mask** { *mask-length* | *mask* }] | *group-address* [**mask** { *mask-length* | *mask* }] | **vlan** *vlan-id*] *

Views

User view

Predefined user roles

network-admin

Parameters

source-address: Specifies a multicast source by its IP address. If you do not specify a multicast source, this command clears multicast groups for all multicast sources in multicast VLANs.

mask { *mask-length* | *mask* }: Specifies a mask length or subnet mask for the multicast source address. The value range for the *mask-length* argument is 0 to 32 (default), and the default value for the *mask* argument is 255.255.255.255.

group-address: Specifies a multicast group by its IP address in the range of 224.0.1.0 to 239.255.255.255. If you do not specify a multicast group, this command clears all multicast groups in multicast VLANs.

mask { *mask-length* | *mask* }: Specifies a mask length or subnet mask for the multicast group address. The value range for the *mask-length* argument is 4 to 32 (default), and the default value for the *mask* argument is 255.255.255.255.

vlan *vlan-id*: Specifies a multicast VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a multicast VLAN, this command clears multicast groups for all multicast VLANs.

Examples

Clear multicast groups for all multicast VLANs.

```
<Switch> reset multicast-vlan group
```

Related commands

display multicast-vlan group

2.1.9. subvlan (multicast-VLAN view)

Use **subvlan** to assign VLANs as sub-VLANs to a multicast VLAN.

Use **undo subvlan** to delete sub-VLANs from a multicast VLAN.

Syntax

subvlan *vlan-list*

undo subvlan { **all** | *vlan-list* }

Default

A multicast VLAN does not have sub-VLANs.

Views

Multicast VLAN view

Predefined user roles

network-admin

Parameters

vlan-list: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The value range for the VLAN ID is 1 to 4094. The specified VLANs must exist and cannot be multicast VLANs or sub-VLANs of other multicast VLANs.

all: Specifies all sub-VLANs of the current multicast VLAN.

Usage guidelines

You must enable IGMP snooping for VLANs to be configured as sub-VLANs.

Examples

Assign VLAN 10 through VLAN 15 as sub-VLANs to multicast VLAN 100.

```
<Switch> system-view
[Switch] multicast-vlan 100
[Switch-mvlan-100] subvlan 10 to 15
```

Contents

A page of this section is **6-x-x**

3. Multicast routing and forwarding commands 3-1
3.1. Multicast routing and forwarding commands 3-1
3.1.1. delete ip rpf-route-static 3-1
3.1.2. display multicast boundary 3-1
3.1.3. display multicast forwarding-table 3-2
3.1.4. display multicast routing-table 3-5
3.1.5. display multicast routing-table static 3-6
3.1.6. display multicast rpf-info 3-7
3.1.7. ip rpf-route-static 3-8
3.1.8. load-splitting (MRIB view) 3-10
3.1.9. longest-match (MRIB view) 3-10
3.1.10. multicast boundary 3-11
3.1.11. multicast routing 3-12
3.1.12. reset multicast forwarding-table 3-12
3.1.13. reset multicast routing-table 3-13

3. Multicast routing and forwarding commands

MEMO:

The **vpn-instance** *vpn-instance-name* option for each command is supported by V7.2.18 and later software.

3.1. Multicast routing and forwarding commands

3.1.1. delete ip rpf-route-static

Use **delete ip rpf-route-static** to delete all static multicast routes.

Syntax

delete ip rpf-route-static [**vpn-instance** *vpn-instance-name*]

Views

System view

Predefined user roles

network-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command deletes all static multicast routes on the public network.

Usage guidelines

This command deletes all static multicast routes. To delete a specified static multicast route, use the **undo ip rpf-route-static** command.

Examples

Delete all static multicast routes.

```
<Switch> system-view
[Switch] delete ip rpf-route-static
This will erase all multicast static routes and their configurations, you must reconfigure all static routes.
Are you sure?[Y/N]:y
```

Related commands

ip rpf-route-static

3.1.2. display multicast boundary

Use **display multicast boundary** to display multicast boundary information.

Syntax

display multicast [**vpn-instance** *vpn-instance-name*] **boundary** [*group-address* [*mask-length* | *mask*]] [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command deletes all static multicast routes on the public network.

group-address: Specifies a multicast group by its IP address in the range of 224.0.0.0 to 239.255.255.255. If you do not specify a multicast group, this command displays multicast boundary information for all multicast groups.

mask-length: Specifies an address mask length in the range of 4 to 32. The default is 32.

mask: Specifies an address mask. The default is 255.255.255.255.

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays multicast boundary information for all interfaces.

Examples

Display information about all multicast boundaries.

```
<Switch> display multicast boundary
 Boundary            Interface
 224.1.1.0/24        Vlan1
 239.2.2.0/24        Vlan2
```

Table 3-1 Command output

Field	Description
Boundary	Multicast group associated with the multicast boundary.
Interface	Boundary interface associated with the multicast boundary.

Related commands

multicast boundary

3.1.3. display multicast forwarding-table

Use **display multicast** [**vpn-instance** *vpn-instance-name*] **forwarding-table** to display multicast forwarding entries.

Syntax

display multicast forwarding-table [*source-address* [**mask** { *mask-length* | *mask* }] | *group-address* [**mask** { *mask-length* | *mask* }] | **incoming-interface** *interface-type interface-number* | **outgoing-interface** { **exclude** | **include**

| **match** } *interface-type interface-number* | **slot** *slot-number* | **statistics**] *

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command deletes all static multicast routes on the public network.

source-address: Specifies a multicast source address.

group-address: Specifies a multicast group address in the range of 224.0.0.0 to 239.255.255.255.

mask-length: Specifies an address mask length. The default value is 32. For a multicast group address, the value range for this argument is 4 to 32. For a multicast source address, the value range for this argument is 0 to 32.

mask: Specifies an address mask. The default value is 255.255.255.255.

incoming-interface: Specifies the multicast forwarding entries that contain the specified incoming interface.

interface-type interface-number: Specifies an incoming interface by its type and number.

outgoing-interface: Specifies the multicast forwarding entries that contain the specified outgoing interface.

exclude: Specifies the multicast forwarding entries that do not contain the specified interface in the outgoing interface list.

include: Specifies the multicast forwarding entries that contain the specified interface in the outgoing interface list.

match: Specifies the forwarding entries that contain only the specified interface in the outgoing interface list.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays multicast forwarding entries for the master device.

statistics: Displays statistics for the multicast forwarding table.

Examples

Display multicast forwarding entries.

```
<Switch> display multicast forwarding-table
Total 1 entries, 1 matched

00001. (172.168.0.2, 227.0.0.1)
     Flags: 0x0
     Uptime: 00:08:32, Timeout in: 00:03:26
     Incoming interface: Vlan-interface10
          Incoming sub-VLAN: VLAN 11
          Outgoing sub-VLAN: VLAN 12
```

```
                          VLAN 13
List of 1 outgoing interfaces:
  1: Vlan-interface20
     Sub-VLAN: VLAN 21
               VLAN 22
Matched 19648 packets(20512512 bytes), Wrong If 0 packet
Forwarded 19648 packets(20512512 bytes)
```

Table 3-2 Command output

Field	Description
Total 1 entries, 1 matched	Total number of (S, G) entries, and the total number of matching (S, G) entries.
00001	Sequence number of the (S, G) entry.
(172.168.0.2,227.0.0.1)	(S, G) entry.
Flags	Entry flag. This field displays one flag or the sum of multiple flags. In this example, the value 0x0 means that the entry has only one flag 0x0. The following entries are available for an entry: • **0x0**—The entry is in correct state. • **0x1**—The entry is in inactive state. • **0x2**—The entry is null. • **0x4**—The entry fails to update. • **0x8**—Outgoing interface information fails to update for the entry. • **0x10**—Data-group information fails to update for the entry. • **0x20**—A register outgoing interface is available. • **0x40**—The entry is to be deleted. • **0x80**—The entry is in registration suppression state. • **0x100**—The entry is being deleted. • **0x200**—The entry is in GR state. • **0x400**—The entry has the VLAN interface of the super VLAN. • **0x800**—The entry has the associated ARP entry for the multicast source address. • **0x400000**—The entry is created by the IGMP proxy.
Uptime	Length of time for which the (S, G) entry has been up.
Timeout in	Length of time in which the (S, G) entry will expire.
Incoming interface	Incoming interface of the (S, G) entry.
Incoming sub-VLAN	Incoming sub-VLAN of the super VLAN when the incoming interface of the (S, G) entry is the VLAN interface of this super VLAN.
Outgoing sub-VLAN	Outgoing sub-VLAN of the super VLAN when the incoming interface of the (S, G) entry is the VLAN interface of this super VLAN.
List of 1 outgoing interfaces	Outgoing interface list of the (S, G) entry.
Sub-VLAN	Outgoing sub-VLAN of the super VLAN when the outgoing interface of the (S, G) entry is the VLAN interface of this

Field	Description
	super VLAN.
Matched 19648 packets(20512512 bytes), Wrong If 0 packet	Number of packets (bytes) that match the (S, G) entry, and number of packets with incoming interface errors. The numbers are displayed as 0 if an outgoing interface of the (S, G) entry is on the specified slot.
Forwarded 19648 packets(20512512 bytes)	Number of packets (bytes) that have been forwarded. The numbers are displayed as 0 if an outgoing interface of the (S, G) entry is on the specified slot.

Related commands

reset multicast forwarding-table

3.1.4. display multicast routing-table

Use **display multicast routing-table** to display multicast routing entries.

Syntax

display multicast [**vpn-instance** *vpn-instance-name*] **routing-table** [*source-address* [**mask** { *mask-length* | *mask* }] | *group-address* [**mask** { *mask-length* | *mask* }] | **incoming-interface** *interface-type interface-number* | **outgoing-interface** { **exclude** | **include** | **match** } *interface-type interface-number*] *

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command deletes all static multicast routes on the public network.

source-address: Specifies a multicast source address.

group-address: Specifies a multicast group address in the range of 224.0.0.0 to 239.255.255.255.

mask-length: Specifies an address mask length. The default value is 32. For a multicast group address, the value range for this argument is 4 to 32. For a multicast source address, the value range for this argument is 0 to 32.

mask: Specifies an address mask. The default is 255.255.255.255.

incoming-interface: Specifies the multicast routing entries that contain the specified incoming interface.

interface-type interface-number: Specifies an interface by its type and number.

outgoing-interface: Specifies the multicast routing entries that contain the specified outgoing interface.

exclude: Specifies the multicast routing entries that do not contain the specified interface in the outgoing interface list.

include: Specifies the multicast routing entries that contain the specified interface in the outgoing interface list.

match: Specifies the multicast routing entries that contain only the specified interface in the outgoing interface list.

Usage guidelines

Multicast routing entries are the basis of multicast forwarding. You can use this command to view the establishment state of (S, G) entries.

Examples

Display multicast routing entries.

```
<Switch> display multicast routing-table
 Total 1 entries

 00001. (172.168.0.2, 227.0.0.1)
       Uptime: 00:00:28
       Upstream Interface: Vlan-interface1
       List of 2 downstream interfaces
           1:  Vlan-interface2
           2:  Vlan-interface3
```

Table 3-3 Command output

Field	Description
Total 1 entries	Total number of (S, G) entries.
00001	Sequence number of the (S, G) entry.
(172.168.0.2, 227.0.0.1)	(S, G) entry.
Uptime	Length of time for which the (S, G) entry has been up.
Upstream Interface	Upstream interface at which (S, G) packets should arrive.
List of 2 downstream interfaces	List of downstream interfaces that need to forward (S, G) packets.

Related commands

reset multicast routing-table

3.1.5. display multicast routing-table static

Use **display multicast routing-table static** to display static multicast routing entries.

Syntax

display multicast [**vpn-instance** *vpn-instance-name*] **routing-table static** [*source-address* { *mask-length* | *mask* }]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command deletes all static multicast routes on the public network.

source-address: Specifies a multicast source address.

mask-length: Specifies an address mask length in the range of 0 to 32.

mask: Specifies an address mask.

Usage guidelines

This command displays only valid static multicast routing entries.

Examples

Display static multicast routing entries.

```
<Switch> display multicast routing-table static
Destinations: 3        Routes: 4

Destination/Mask    Pre  RPF neighbor    Interface
1.1.0.0/16          10   7.12.0.1        Vlan12
                         7.11.0.1        Vlan11
2.2.2.0/24          20   7.11.0.1        Vlan11
3.3.3.3/32          50   7.12.0.1        Vlan12
```

Table 3-4 Command output

Field	Description
Destinations	Number of the multicast destination addresses.
Routes	Number of routes.
Destination/Mask	Destination address and its mask length.
Pre	Route preference.
RPF neighbor	IP address of the RPF neighbor to the reachable destination.
Interface	Outgoing interface to the reachable destination.

3.1.6. display multicast rpf-info

Use **display multicast rpf-info** to display RPF information for a multicast source.

Syntax

display multicast [**vpn-instance** *vpn-instance-name*] **rpf-info** *source-address* [*group-address*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command deletes all static multicast routes on the public network.

source-address: Specifies a multicast source address.

group-address: Specifies a multicast group address in the range of 224.0.1.0 to 239.255.255.255.

Examples

Display RPF information for multicast source 192.168.1.55.

```
<Switch> display multicast rpf-info 192.168.1.55
 RPF information about source 192.168.1.55:
     RPF interface:Vlan-interface1, RPF neighbor: 10.1.1.1
     Referenced route/mask: 192.168.1.0/24
     Referenced route type: igp
     Route selection rule: preference-preferred
     Load splitting rule: disable
```

Table 3-5 Command output

Field	Description
RPF neighbor	IP address of the RPF neighbor.
Referenced route/mask	Referenced route and its mask length.
Referenced route type	Type of the referenced route: • **igp**—IGP unicast route. • **egp**—EGP unicast route. • **unicast (direct)**—Directly connected unicast route. • **unicast**—Other unicast routes, such as static unicast route. • **multicast static**—Static multicast route. • **mbgp**—MBGP route.
Route selection rule	Rule for RPF route selection: • Route preference. • Longest prefix match.
Load splitting rule	Status of the load splitting rule: enable or disable.

Related commands

display multicast forwarding-table

display multicast routing-table

3.1.7. ip rpf-route-static

Use **ip rpf-route-static** to configure a static multicast route.

Use **undo ip rpf-route-static** to delete a static multicast route.

Syntax

ip rpf-route-static [**vpn-instance** *vpn-instance-name*] *source-address* { *mask-length* | *mask* } { *rpf-nbr-address* | *interface-type interface-number* } [**preference** *preference*]

undo ip rpf-route-static [**vpn-instance** *vpn-instance-name*] *source-address* { *mask-length* | *mask* } { *rpf-nbr-address* | *interface-type interface-number* }

Default

No static multicast routes exist.

Views

System view

Predefined user roles

network-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command deletes all static multicast routes on the public network.

source-address: Specifies a multicast source address.

mask-length: Specifies an address mask length in the range of 0 to 32.

mask: Specifies an address mask.

rpf-nbr-address: Specifies an RPF neighbor by its IP address.

interface-type interface-number: Specifies an interface by its type and number. The interface connects the RPF neighbor.

preference: Sets a route preference in the range of 1 to 255. The default value is 1.

Usage guidelines

If the interface connected to an RPF neighbor is a point-to-point interface, you must specify the interface by its type and number.

If the interface connected to an RPF neighbor is not a point-to-point interface, you must specify the interface by its IP address. This type of interfaces includes Layer 3 Ethernet, Loopback, and VLAN interfaces.

The configured static multicast route might not take effect when one of the following conditions exists:

- The outgoing interface iteration fails.
- The specified interface is not a point-to-point interface.
- The specified interface is down.

If multiple static multicast routes within the same multicast source address range are available, only the one with the highest route preference can become active. You can use the **display multicast routing-table static** command to verify that the configured static multicast route has taken effect.

The **undo ip rpf-route-static** command deletes the specified static multicast route, but the **delete ip rpf-route-static** command deletes all static multicast routes.

Examples

Configure a static multicast route to multicast source 10.1.1.0/24 and specify the interface with IP address 192.168.1.23 as the RPF neighbor.

```
<Switch> system-view
[Switch] ip rpf-route-static 10.1.1.0 24 192.168.1.23
```

Related commands

delete ip rpf-route-static

display multicast routing-table static

3.1.8. load-splitting (MRIB view)

Use **load-splitting** to enable multicast load splitting.

Use **undo load-splitting** to restore the default.

Syntax

load-splitting { **source** | **source-group** }

undo load-splitting

Default

Multicast load splitting is disabled.

Views

MRIB view

Predefined user roles

network-admin

Parameters

source: Enables multicast load splitting based on multicast source.

source-group: Enables multicast load splitting based on multicast source and group.

Examples

Enable multicast load splitting based on multicast source.

```
<Switch> system-view
[Switch] multicast routing
[Switch-mrib] load-splitting source
```

3.1.9. longest-match (MRIB view)

Use **longest-match** to specify the longest prefix match principle for RPF route.

Use **undo longest-match** to restore the default.

Syntax

longest-match

undo longest-match

Default

Route preference is used for RPF route selection. The route with the highest preference is used as the RPF route.

Views

MRIB view

Predefined user roles

network-admin

Usage guidelines

This command enables the device to use the matching route with the longest prefix as the RPF route.

Examples

Specify the longest prefix match principle for RPF route selection.

```
<Switch> system-view
[Switch] multicast routing
[Switch-mrib] multicast longest-match
```

3.1.10. multicast boundary

Use **multicast boundary** to configure a multicast forwarding boundary.

Use **undo multicast boundary** to delete a multicast forwarding boundary.

Syntax

multicast boundary *group-address* { *mask-length* | *mask* }

undo multicast boundary { *group-address* { *mask-length* | *mask* } | **all** }

Default

No multicast forwarding boundaries are configured on an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

group-address: Specifies a multicast group address in the range of 224.0.0.0 to 239.255.255.255.

mask-length: Specifies an address mask length in the range of 4 to 32.

mask: Specifies an address mask.

all: Specifies all forwarding boundaries configured on the interface.

Usage guidelines

A multicast forwarding boundary sets the boundary condition for the multicast groups in the specified address range. If the destination address of a multicast packet matches the set boundary condition, the packet is not forwarded.

You can configure an interface as a multicast forwarding boundary for different multicast group ranges by executing this command multiple times on the interface.

You do not need to enable IP multicast routing before you execute this command.

Assume that Set A and Set B are multicast forwarding boundary sets with different address ranges, and B is a subset of A. A takes effect on the interface no matter whether A is configured earlier or later than B.

Examples

Configure VLAN-interface 100 as the forwarding boundary of multicast groups in the range of 239.2.0.0/16.

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] multicast boundary 239.2.0.0 16
```

Related commands

display multicast boundary

3.1.11. multicast routing

Use **multicast routing** to enable IP multicast routing and enter MRIB view.

Use **undo multicast routing** to disable IP multicast routing.

Syntax

multicast routing [**vpn-instance** *vpn-instance-name*]

undo multicast routing [**vpn-instance** *vpn-instance-name*]

Default

IP multicast routing is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command deletes all static multicast routes on the public network.

Usage guidelines

Other Layer 3 multicast commands take effect only when IP multicast routing is enabled.

The device does not forward multicast packets before IP multicast routing is enabled.

Examples

Enable IP multicast routing and enter MRIB view.

```
<Switch> system-view
[Switch] multicast routing
[Switch-mrib]
```

3.1.12. reset multicast forwarding-table

Use **reset multicast forwarding-table** to clear multicast forwarding entries.

Syntax

reset multicast [**vpn-instance** *vpn-instance-name*] **forwarding-table** { { *source-address* [**mask** { *mask-length* | *mask* }] | *group-address* [**mask** { *mask-length* | *mask* }] | **incoming-interface** { *interface-type interface-number* } } * | **all** }

Views

User view

Predefined user roles

network-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command deletes all static multicast routes on the public network.

source-address: Specifies a multicast source address.

group-address: Specifies a multicast group address in the range of 224.0.0.0 to 239.255.255.255.

mask-length: Specifies an address mask length. The default value is 32. For a multicast group address, the value range for this argument is 4 to 32. For a multicast source address, the value range for this argument is 0 to 32.

mask: Specifies an address mask. The default is 255.255.255.255.

incoming-interface: Specifies the multicast forwarding entries that contain the specified incoming interface.

interface-type interface-number: Specifies an incoming interface by its type and number.

all: Specifies all multicast forwarding entries.

Usage guidelines

When you clear a multicast forwarding entry, the associated multicast routing entry is also cleared.

Examples

Clear multicast forwarding entries for multicast group 225.5.4.3.

```
<Switch> reset multicast forwarding-table 225.5.4.3
```

Related commands

display multicast forwarding-table

3.1.13. reset multicast routing-table

Use **reset multicast routing-table** to clear multicast routing entries.

Syntax

reset multicast [**vpn-instance** *vpn-instance-name*] **routing-table** { { *source-address* [**mask** { *mask-length* | *mask* }] | *group-address* [**mask** { *mask* | *mask-length* }] | **incoming-interface** *interface-type interface-number* } * | **all** }

Views

User view

Predefined user roles

network-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command deletes all static multicast routes on the public network.

source-address: Specifies a multicast source address.

group-address: Specifies a multicast group address in the range of 224.0.0.0 to 239.255.255.255.

mask-length: Specifies an address mask length. The default value is 32. For a multicast group address, the value range for this argument is 4 to 32. For a multicast source address, the value range for this argument is 0 to 32.

mask: Specifies an address mask. The default is 255.255.255.255.

incoming-interface: Specifies the routing entries that contain the specified incoming interface.

interface-type interface-number: Specifies an incoming interface by its type and number.

all: Specifies all multicast routing entries.

Usage guidelines

When you clear a multicast routing entry, the associated multicast forwarding entry is also cleared.

Examples

Clear multicast routing entries for multicast group 225.5.4.3.

```
<Switch> reset multicast routing-table 225.5.4.3
```

Related commands

display multicast routing-table

Contents

A page of this section is **6-x-x**

4. IGMP commands ····· 4-1
4.1. IGMP commands ····· 4-1
4.1.1. display igmp group ····· 4-1
4.1.2. display igmp interface ····· 4-5
4.1.3. display igmp ssm-mapping ····· 4-7
4.1.4. igmp ····· 4-8
4.1.5. igmp enable ····· 4-9
4.1.6. igmp group-policy ····· 4-9
4.1.7. igmp last-member-query-interval ····· 4-10
4.1.8. igmp max-response-time ····· 4-11
4.1.9. igmp other-querier-present-interval ····· 4-12
4.1.10. igmp query-interval ····· 4-13
4.1.11. igmp robust-count ····· 4-13
4.1.12. igmp startup-query-count ····· 4-14
4.1.13. igmp startup-query-interval ····· 4-15
4.1.14. igmp static-group ····· 4-15
4.1.15. igmp version ····· 4-16
4.1.16. last-member-query-interval (IGMP view) ····· 4-17
4.1.17. max-response-time (IGMP view) ····· 4-17
4.1.18. other-querier-present-interval (IGMP view) ····· 4-18
4.1.19. query-interval (IGMP view) ····· 4-19
4.1.20. reset igmp group ····· 4-19
4.1.21. robust-count (IGMP view) ····· 4-20
4.1.22. ssm-mapping (IGMP view) ····· 4-21
4.1.23. startup-query-count (IGMP view) ····· 4-22
4.1.24. startup-query-interval (IGMP view) ····· 4-23

4. IGMP commands

MEMO:

The **vpn-instance** *vpn-instance-name* option for each command is supported by V7.2.18 and later software.

4.1. IGMP commands

4.1.1. display igmp group

Use **display igmp group** to display information about IGMP multicast groups (multicast groups that hosts have joined through IGMP).

Syntax

display igmp group [**vpn-instance** *vpn-instance-name*] [*group-address* | **interface** *interface-type interface-number*] [**static** | **verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays multicast boundary information on the public network.

group-address: Specifies a multicast group by its IP address in the range of 224.0.1.0 to 239.255.255.255. If you do not specify a multicast group, this command displays information about all IGMP multicast groups.

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays information about IGMP multicast groups for all interfaces.

static: Specifies IGMP multicast groups that hosts have joined statically. If you do not specify this keyword, the command displays information about IGMP multicast groups that hosts have joined dynamically.

verbose: Displays detailed information.

Examples

Display information about IGMP multicast groups that hosts have dynamically joined.

```
<Switch> display igmp group
IGMP groups in total: 3
 Vlan-interface1(10.10.1.20):
```

```
IGMP groups reported in total: 3
 Group address   Last reporter   Uptime      Expires
 225.1.1.1       10.10.1.10      00:02:04    00:01:15
 225.1.1.2       10.10.1.10      00:02:04    00:01:15
 225.1.1.3       10.10.1.10      00:02:04    00:01:15
```

Table 4-1 Command output

Field	Description
IGMP groups in total	Total number of IGMP multicast groups.
IGMP groups reported in total	Total number of IGMP multicast groups that hosts attached to the interface have joined dynamically.
Group address	Multicast group address.
Last reporter	Address of the last host that reported its membership to the multicast group.
Uptime	Length of time since the multicast group was reported.
Expire	Remaining lifetime for the multicast group. This field displays **Off** if the timer is disabled.

Display detailed information about IGMP multicast group 232.1.1.1 that hosts have dynamically joined. In this example, the switch is configured with IGMP SSM mappings.

```
<Switch> display igmp group 232.1.1.1 verbose
 Vlan-interface1(10.10.1.20):
  IGMP groups reported in total: 3
   Group: 232.1.1.1
     Uptime: 00:00:34
     Exclude expires: 00:04:16
     Mapping expires: 00:02:16
     Last reporter: 10.10.1.10
     Last-member-query-counter: 0
     Last-member-query-timer-expiry: Off
     Mapping last-member-query-counter: 0
     Mapping last-member-query-timer-expiry: Off
     Group mode: Exclude
     Version1-host-present-timer-expiry: Off
     Version2-host-present-timer-expiry: 00:02:11
     Mapping version1-host-present-timer-expiry: Off
     Source list (sources in total: 1):
       Source: 10.1.1.1
          Uptime: 00:00:03
          V3 expires: 00:04:16
          Mapping expires: 00:02:16
          Last-member-query-counter: 0
          Last-member-query-timer-expiry: Off
```

Table 4-2 Command output

Field	Description
IGMP groups reported in total	Total number of IGMP multicast groups that hosts

Field	Description
	attached to the interface have joined dynamically.
Group	Multicast group address.
Uptime	Length of time since the multicast group was reported.
Exclude expires	Remaining lifetime for the multicast group in Exclude mode. This field displays **Off** if the timer is disabled.
Mapping expires	Remaining time for the multicast group specified in IGMP SSM mappings. This field is displayed only when the device is configured with IGMP SSM mappings.
Last reporter	Address of the last host that reported its membership to this multicast group.
Last-member-query-counter	Number of IGMP group-specific queries or IGMP source-and-group-specific queries sent for the multicast group.
Last-member-query-timer-expiry	Remaining time for the last member query timer for the multicast group. This field displays **Off** if the timer is disabled.
Mapping last-member-query-counter	Number of IGMP group-specific queries or IGMP source-and-group-specific queries sent for the multicast group specified in IGMP SSM mappings. This field is displayed only when the device is configured with IGMP SSM mappings.
Mapping last-member-query-timer-expiry	Remaining time for the last member query timer of the multicast group specified in IGMP SSM mappings. This field displays **Off** if the timer is disabled. This field is displayed only when the device is configured with IGMP SSM mappings.
Group mode	Multicast source filtering mode: • **Include**—Include mode. • **Exclude**—Exclude mode. For a device that runs IGMPv1 or IGMPv2: • If IGMP SSM mappings are not configured, this field displays **Exclude**. • If IGMP SSM mappings are configured, this field displays **Include** or **Exclude** depending on the SSM mappings and the multicast groups that the host joins.
Version1-host-present-timer-expiry	Remaining time for the IGMPv1 host present timer. This field displays **Off** if the timer is disabled. This field is displayed only when the device runs IGMPv2 or IGMPv3.
Version2-host-present-timer-expiry	Remaining time for the IGMPv2 host present timer. This field displays **Off** if the timer is disabled. This field is displayed only when the device runs IGMPv3.
Mapping version1-host-present-timer-expiry	Remaining time for the IGMPv1 host present timer when the device is configured with IGMP SSM mappings. This field displays **Off** if the timer is disabled. This field is displayed only when the device is configured

Field	Description
	with IGMP SSM mappings.
Source list (sources in total)	List of multicast sources and total number of multicast sources. This field is displayed only when the device runs IGMPv3 or when the device is configured with IGMP SSM mappings.
Source	Multicast source address. This field is displayed only when the device runs IGMPv3 or when the device is configured with IGMP SSM mappings.
Uptime	Length of time since the multicast source was reported. This field is displayed only when the device runs IGMPv3 or when the device is configured with IGMP SSM mappings.
V3 expires	Remaining time for the multicast source when the device runs IGMPv3. This field displays **Off** if the timer is disabled and displays three hyphens (---) if the multicast source is specified in IGMP SSM mappings. This field is displayed only when the device runs IGMPv3 or when the device is configured with IGMP SSM mappings.
Mapping expires	Remaining time for the multicast source specified in IGMP SSM mappings. This field is displayed only when the device is configured with IGMP SSM mappings.
Last-member-query-counter	Number of IGMP group-specific queries or IGMP group-and-source-specific queries sent for the multicast source and group. This field is displayed only when the device runs IGMPv3 or is configured with IGMP SSM mappings.
Last-member-query-timer-expiry	Remaining time for the last member query timer for the multicast source and group. This field displays **Off** if the timer is disabled. This field is displayed only when the device runs IGMPv3 or is configured with IGMP SSM mappings.

Display information about IGMP multicast groups that hosts have statically joined.

```
<Switch> display igmp group static
 Entries in total: 2
   Group address   Source address  Interface           Expires
   225.1.1.1       0.0.0.0         Vlan1               Never
   225.2.2.2       1.1.1.1         Vlan1               Never
```

Table 4-3 Command output

Field	Description
Entries in total	Total number of the multicast groups that hosts have joined statically.
Group address	Multicast group address.

Field	Description
Source address	Multicast source address.
Interface	Interface name.
Expires	Remaining lifetime for the multicast group. This field always displays **Never** because the multicast group never expires.

Related commands

reset igmp group

4.1.2. display igmp interface

Use **display igmp interface** to display IGMP information for interfaces.

Syntax

display igmp [**vpn-instance** *vpn-instance-name*] **interface** [*interface-type interface-number*] [**host**] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays multicast boundary information on the public network.

interface-type interface-number: Specifies an interface by its type and number. If you do not specify an interface, this command displays IGMP information for all IGMP-enabled interfaces.

host: Displays information about the interfaces enabled with the IGMP host feature. If you do not specify this keyword, the command displays IGMP information for interfaces enabled with IGMP and those enabled with the IGMP host feature. For more information about the IGMP host feature, see *VXLAN Configuration Guide*.

verbose: Displays detailed IGMP information.

Examples

Display detailed IGMP information for VLAN-interface 1 (non-proxy interface).

```
<Switch> display igmp interface vlan-interface 1 verbose
 Vlan-interface1(10.10.1.20):
   IGMP is enabled.
   IGMP version: 2
   Query interval for IGMP: 125s
   Other querier present time for IGMP: 255s
   Maximum query response time for IGMP: 10s
   Last member query interval: 1s
   Last member query count: 2
   Startup query interval: 31s
```

```
  Startup query count: 2
  General query timer expiry (hh:mm:ss): 00:00:54
  Querier for IGMP: 10.10.1.20 (This router)
  IGMP activity: 1 join(s), 0 leave(s)
  Multicast routing on this interface: Enabled
  Robustness: 2
  Require-router-alert: Disabled
  Fast-leave: Disabled
  Startup-query: Off
  Other-querier-present-timer-expiry (hh:mm:ss): Off
  IGMP groups reported in total: 1
```

Display detailed IGMP information for all interfaces enabled with the IGMP host feature.

```
<Switch> display igmp interface host verbose
 Vlan-interface3(30.10.1.20):
   IGMP host is enabled.
   IGMP version: 2
   Multicast routing on this interface: Enabled
   Require-router-alert: Disabled
   Version1-querier-present-timer-expiry (hh:mm:ss): Off
```

Table 4-4 Command output

Field	Description
Vlan-interface1(10.10.1.20)	Interface and its IP address.
IGMP is enabled	IGMP is enabled on the interface.
IGMP version	Version of IGMP that the interface runs.
Query interval for IGMP	IGMP general query interval, in seconds.
Other querier present time for IGMP	IGMP other querier present interval, in seconds.
Maximum query response time for IGMP	Maximum response time for IGMP general queries, in seconds.
Last member query interval	Interval for sending IGMP group-specific queries or IGMP group-and-source-specific queries, in seconds.
Last member query count	Number of IGMP group-specific queries or IGMP group-and-source-specific queries sent for the multicast group.
Startup query interval	Interval for sending IGMP general queries on startup, in seconds.
Startup query count	Number of IGMP general queries that the device sends on startup.
General query timer expiry	Remaining time for the IGMP general query timer. This field displays **Off** if the timer is disabled.
Querier for IGMP	IP address of the IGMP querier. This field is not displayed when the device runs IGMPv1 and the device is not the IGMP querier. NOTE: In IGMPv1, the PIM DR acts as the IGMP querier. You can use the **display pim interface**

Field	Description
	command to display PIM information.
No querier elected	No IGMP querier election is performed. This field is displayed when the device runs IGMPv1 and is not the IGMP querier. NOTE: In IGMPv1, the PIM DR acts as the IGMP querier. You can use the **display pim interface** command to display PIM information.
IGMP activity: 1 join(s), 0 leave(s)	Statistics of IGMP activities: • **join(s)**—Total number of multicast groups that this interface has joined. • **leave(s)**—Total number of multicast groups that this interface has left.
Multicast routing on this interface	Whether IP multicast routing is enabled: Enabled or Disabled.
Robustness	Robustness variable of the IGMP querier.
Require-router-alert	Whether the feature of dropping IGMP messages without Router-Alert is enabled: Enabled or Disabled,
Fast-leave	Whether the fast-leave processing feature is enabled: Enabled or Disabled.
Startup-query	Whether the IGMP querier sends IGMP general queries at the startup query interval on startup: • **On**—The IGMP querier performs the above action. • **Off**—The IGMP querier does not perform the above action.
Other-querier-present-timer-expiry	Remaining time for the other querier present timer. This field displays **Off** if the timer is disabled.
IGMP groups reported in total	Total number of multicast groups that the interface has joined dynamically. This field is not displayed if the interface does not join multicast groups.
IGMP proxy is enabled	IGMP proxying is enabled on the interface.
IGMP host is enabled	The IGMP host feature is enabled on the interface.
Version1-querier-present-timer-expiry	Remaining time for the IGMPv1 querier present timer. This field displays **Off** if the timer is disabled.

4.1.3. display igmp ssm-mapping

Use **display igmp ssm-mapping** to display IGMP SSM mappings.

Syntax

display igmp [**vpn-instance** *vpn-instance-name*] **ssm-mapping** *group-address*

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays multicast boundary information on the public network.

group-address: Specifies a multicast group by its IP address in the range of 224.0.1.0 to 239.255.255.255.

Examples

Display IGMP SSM mappings for multicast group 232.1.1.1.

```
<Switch> display igmp ssm-mapping 232.1.1.1
 Group: 232.1.1.1
 Source list:
        1.2.3.4
        5.5.5.5
        10.1.1.1
        100.1.1.10
```

Table 4-5 Command output

Field	Description
Group	Multicast group address.
Source list	List of multicast source addresses.

4.1.4. igmp

Use **igmp** to enter IGMP view.

Use **undo igmp** to delete the configurations in IGMP view.

Syntax

igmp [**vpn-instance** *vpn-instance-name*]

undo igmp [**vpn-instance** *vpn-instance-name*]

Views

System view

Predefined user roles

network-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays multicast boundary information on the public network.

Examples

Enter IGMP view.

```
<Switch> system-view
```

```
[Switch] igmp
[Switch-igmp]
```

4.1.5. igmp enable

Use **igmp enable** to enable IGMP on an interface.

Use **undo igmp enable** to disable IGMP on an interface.

Syntax

igmp enable

undo igmp enable

Default

IGMP is disabled on an interface.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

This command takes effect only when IP multicast routing is enabled.

Other IGMP configurations on the interface take effects only when IGMP is enabled on the interface.

Examples

Enable IP multicast routing, and enable IGMP on VLAN-interface 100.

```
<Switch> system-view
[Switch] multicast routing
[Switch-mrib] quit
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] igmp enable
```

Related commands

multicast routing

4.1.6. igmp group-policy

Use **igmp group-policy** to configure a multicast group policy on an interface to control the multicast groups that hosts attached to the interface can join.

Use **undo igmp group-policy** to delete the multicast group policy on an interface.

Syntax

igmp group-policy *ipv4-acl-number* [*version-number*]

undo igmp group-policy

Default

No multicast group policy exists on an interface. Hosts attached to the interface can join any multicast groups.

Views

Interface view

Predefined user roles

network-admin

Parameters

ipv4-acl-number: Specifies an IPv4 basic or advanced ACL by its number in the range of 2000 to 3999. Hosts can join only the multicast groups that the ACL permits. If the ACL does not exist or does not have valid rules, hosts cannot join any multicast groups.

version-number: Specifies an IGMP version in the range of 1 to 3. By default, this command takes effect on IGMP reports of all versions.

Usage guidelines

A multicast group policy filters IGMP reports to control the multicast groups that the hosts can join.

This command does not take effect on static member interfaces because static member interfaces do not send IGMP reports.

When you configure a rule in the IPv4 ACL, follow these restrictions and guidelines:

- For the rule to take effect, do not specify the **vpn-instance** *vpn-instance* option.
- In a basic ACL, the **source** *source-address source-wildcard* option specifies a multicast group address.
- In an advanced ACL, the **source** *source-address source-wildcard* option specifies a multicast source address. The **destination** *dest-address dest-wildcard* option specifies a multicast group address.

  To match the following IGMP reports, set the **source** *source-address source-wildcard* option to 0.0.0.0:

  - IGMPv1 and IGMPv2 reports.
  - IGMPv3 IS_EX and IGMPv3 TO_EX reports that do not carry multicast source addresses.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure a multicast group policy on VLAN-interface 100 so that hosts attached to the interface can join only multicast group 225.1.1.1.

```
<Switch> system-view
[Switch] acl basic 2005
[Switch-acl-ipv4-basic-2005] rule permit source 225.1.1.1 0
[Switch-acl-ipv4-basic-2005] quit
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] igmp group-policy 2005
```

4.1.7. igmp last-member-query-interval

Use **igmp last-member-query-interval** to set the IGMP last member query interval on an interface.

Use **undo igmp last-member-query-interval** to restore the default.

Syntax

igmp last-member-query-interval *interval*

undo igmp last-member-query-interval

Default

The IGMP last member query interval is 1 second.

Views

Interface view

Predefined user roles

network-admin

Parameters

interval: Specifies an IGMP last member query interval in the range of 1 to 25 seconds.

Usage guidelines

You can set the IGMP last member query interval for an interface in interface view or globally for all interfaces in IGMP view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the IGMP last member query interval to 6 seconds on VLAN-interface 100.

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] igmp last-member-query-interval 6
```

Related commands

last-member-query-interval (IGMP view)

4.1.8. igmp max-response-time

Use **igmp max-response-time** to set the maximum response time for IGMP general queries on an interface.

Use **undo igmp max-response-time** to restore the default.

Syntax

igmp max-response-time *time*

undo igmp max-response-time

Default

The maximum response time for IGMP general queries is 10 seconds.

Views

Interface view

Predefined user roles

network-admin

Parameters

time: Specifies the maximum response time for IGMP general queries, in the range of 1 to 3174 seconds.

Usage guidelines

You can set the maximum response time for an interface in interface view or globally for all interfaces in IGMP view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the maximum response time for IGMP general queries to 25 seconds on VLAN-interface 100.

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] igmp max-response-time 25
```

Related commands

max-response-time (IGMP view)

4.1.9. igmp other-querier-present-interval

Use **igmp other-querier-present-interval** to set the IGMP other querier present timer on an interface.

Use **undo igmp other-querier-present-interval** to restore the default.

Syntax

igmp other-querier-present-interval *interval*

undo igmp other-querier-present-interval

Default

The IGMP other querier present timer is calculated by using the following formula:

[IGMP general query interval] × [IGMP querier's robustness variable] + [maximum response time for IGMP general queries] / 2.

Views

Interface view

Predefined user roles

network-admin

Parameters

interval: Specifies an IGMP other querier present timer in the range of 1 to 31744 seconds.

Usage guidelines

You can set the IGMP other querier present timer for an interface in interface view or globally for all interfaces in IGMP view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the IGMP other querier present timer to 125 seconds on VLAN-interface 100.

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] igmp other-querier-present-interval 125
```

Related commands

other-querier-present-interval (IGMP view)

4.1.10. igmp query-interval

Use **igmp query-interval** to set the IGMP general query interval on an interface.

Use **undo igmp query-interval** to restore the default.

Syntax

igmp query-interval *interval*

undo igmp query-interval

Default

The IGMP general query interval is 125 seconds.

Views

Interface view

Predefined user roles

network-admin

Parameters

interval: Specifies an IGMP general query interval in the range of 1 to 31744 seconds.

Usage guidelines

You can set the IGMP general query interval for an interface in interface view or globally for all interfaces in IGMP view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the IGMP general query interval to 60 seconds on VLAN-interface 100.

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] igmp query-interval 60
```

Related commands

query-interval (IGMP view)

4.1.11. igmp robust-count

Use **igmp robust-count** to set the IGMP querier's robustness variable on an interface.

Use **undo igmp robust-count** to restore the default.

Syntax

igmp robust-count *count*

undo igmp robust-count

Default

The IGMP querier's robustness variable is 2.

Views

Interface view

Predefined user roles

network-admin

Parameters

count: Specifies an IGMP querier's robustness variable in the range of 1 to 255.

Usage guidelines

The IGMP querier's robustness variable defines the number of times to retransmit queries if packet loss occurs. A higher robustness variable makes the IGMP querier more robust, but it increases timeout time for multicast groups.

You can set the IGMP querier's robustness variable for an interface in interface view or globally for all interfaces in IGMP view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the IGMP querier's robustness variable to 5 on VLAN-interface 100.

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] igmp robust-count 5
```

Related commands

robust-count (IGMP view)

4.1.12. igmp startup-query-count

Use **igmp startup-query-count** to set the IGMP startup query count on an interface.

Use **undo igmp startup-query-count** to restore the default.

Syntax

igmp startup-query-count *count*

undo igmp startup-query-count

Default

The IGMP startup query count equals the IGMP querier's robustness variable.

Views

Interface view

Predefined user roles

network-admin

Parameters

count: Specifies an IGMP startup query count in the range of 1 to 255.

Usage guidelines

You can set the IGMP startup query count for an interface in interface view or globally for all interfaces in IGMP view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the IGMP startup query count to 5 on VLAN-interface 100.

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] igmp startup-query-count 5
```

Related commands

startup-query-count (IGMP view)

4.1.13. igmp startup-query-interval

Use **igmp startup-query-interval** to set the IGMP startup query interval on an interface.

Use **undo igmp startup-query-interval** to restore the default.

Syntax

igmp startup-query-interval *interval*

undo igmp startup-query-interval

Default

The IGMP startup query interval equals one quarter of the IGMP general query interval.

Views

Interface view

Predefined user roles

network-admin

Parameters

interval: Specifies an IGMP startup query interval in the range of 1 to 31744 seconds.

Usage guidelines

You can set the IGMP startup query interval for an interface in interface view or globally for all interfaces in IGMP view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the IGMP startup query interval to 100 seconds on VLAN-interface 100.

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] igmp startup-query-interval 100
```

Related commands

startup-query-interval (IGMP view)

4.1.14. igmp static-group

Use **igmp static-group** to configure an interface as a static group member of a multicast group.

Use **undo igmp static-group** to restore the default.

Syntax

igmp static-group *group-address* [**source** *source-address*]

undo igmp static-group { **all** | *group-address* [**source** *source-address*]

Default

An interface is not a static group member of multicast groups.

Views

Interface view

Predefined user roles

network-admin

Parameters

group-address: Specifies a multicast group by its IP address in the range of 224.0.1.0 to 239.255.255.255.

source *source-address*: Specifies a multicast source by its IP address. If you do not specify a multicast source, this command configures an interface as a static member of the multicast groups with all multicast source addresses.

all: Specifies all multicast groups that the interface has statically joined.

Usage guidelines

For multicast routing entries to be created, you must specify a multicast source if the specified multicast group is in the SSM group range.

Examples

Configure VLAN-interface 100 as a static group member of multicast group 224.1.1.1.

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] igmp static-group 224.1.1.1
```

Configure VLAN-interface 100 as a static group member of multicast source and group (192.168.1.1, 232.1.1.1).

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] igmp static-group 232.1.1.1 source 192.168.1.1
```

4.1.15. igmp version

Use **igmp version** to specify an IGMP version on an interface.

Use **undo igmp version** to restore the default.

Syntax

igmp version *version-number*

undo igmp version

Default

The IGMP version on an interface is 2.

Views

Interface view

Predefined user roles

network-admin

Parameters

version-number: Specifies an IGMP version in the range of 1 to 3.

Examples

Specify IGMP version 1 on VLAN-interface 100.

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] igmp version 1
```

4.1.16. last-member-query-interval (IGMP view)

Use **last-member-query-interval** to set the IGMP last member query interval globally.

Use **undo last-member-query-interval** to restore the default.

Syntax

last-member-query-interval *interval*

undo last-member-query-interval

Default

The IGMP last member query interval is 1 second.

Views

IGMP view

Predefined user roles

network-admin

Parameters

interval: Specifies an IGMP last member query interval in the range of 1 to 25 seconds.

Usage guidelines

You can set the IGMP last member query interval globally for all interfaces in IGMP view or for an interface in interface view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the global IGMP last member query interval to 6 seconds.

```
<Switch> system-view
[Switch] igmp
[Switch-igmp] last-member-query-interval 6
```

Related commands

igmp last-member-query-interval

4.1.17. max-response-time (IGMP view)

Use **max-response-time** to set the maximum response time for IGMP general queries globally.

Use **undo max-response-time** to restore the default.

Syntax

max-response-time *time*

undo max-response-time

Default

The maximum response time for IGMP general queries is 10 seconds.

Views

IGMP view

Predefined user roles

network-admin

Parameters

time: Specifies the maximum response time for IGMP general queries in the range of 1 to 3174 seconds.

Usage guidelines

You can set the maximum response time globally for all interfaces in IGMP view or for an interface in interface view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

#Set the global maximum response time for IGMP general queries to 25 seconds.

```
<Switch> system-view
[Switch] igmp
[Switch-igmp] max-response-time 25
```

Related commands

igmp max-response-time

4.1.18. other-querier-present-interval (IGMP view)

Use **other-querier-present-interval** to set the IGMP other querier present timer globally.

Use **undo other-querier-present-interval** to restore the default.

Syntax

other-querier-present-interval *interval*

undo other-querier-present-interval

Default

The IGMP other querier present timer is calculated by using the following formula:

[IGMP general query interval] × [IGMP querier's robustness variable] + [maximum response time for IGMP general queries] / 2.

Views

IGMP view

Predefined user roles

network-admin

Parameters

interval: Specifies an IGMP other querier present timer in the range of 1 to 31744 seconds.

Usage guidelines

You can set the IGMP other querier present timer globally for all interfaces in IGMP view or for an interface in interface view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the global IGMP other querier present timer to 125 seconds.

```
<Switch> system-view
[Switch] igmp
[Switch-igmp] other-querier-present-interval 125
```

Related commands

igmp other-querier-present-interval

4.1.19. query-interval (IGMP view)

Use **query-interval** to set the IGMP general query interval globally.

Use **undo query-interval** to restore the default.

Syntax

query-interval *interval*

undo query-interval

Default

The IGMP general query interval is 125 seconds.

Views

IGMP view

Predefined user roles

network-admin

Parameters

interval: Specifies an IGMP general query interval in the range of 1 to 31744 seconds.

Usage guidelines

You can set the IGMP general query interval globally for all interfaces in IGMP view or for an interface in interface view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the global IGMP general query interval to 60 seconds.

```
<Switch> system-view
[Switch] igmp
[Switch-igmp] query-interval 60
```

Related commands

igmp query-interval

4.1.20. reset igmp group

Use **reset igmp group** to clear dynamic IGMP multicast group entries.

Syntax

reset igmp [**vpn-instance** *vpn-instance-name*] **group** { **all** | **interface** *interface-type interface-number* { **all** | *group-address* [**mask** { *mask* | *mask-length* }] [*source-address* [**mask** { *mask* | *mask-length* }]] } }

Views

User view

Predefined user roles

network-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays multicast boundary information on the public network.

all: Specifies all interfaces (the first **all**), or all IGMP multicast groups (the second **all**).

interface-type interface-number: Specifies an interface by its type and number.

group-address: Specifies a multicast group by its IP address in the range of 224.0.0.0 to 239.255.255.255.

source-address: Specifies a multicast source address. If you do not specify a multicast source, this command clears dynamic IGMP multicast group entries for all multicast source addresses.

mask: Specifies an address mask. The default is 255.255.255.255.

mask-length: Specifies an address mask length. The default is 32. For a multicast group address, the value range for this argument is 4 to 32. For a multicast source address, the value range for this argument is 0 to 32.

Usage guidelines

This command might interrupt the multicast information transmission.

Examples

Clear dynamic IGMP multicast group entries for all interfaces.

```
<Switch> reset igmp group all
```

Clear all dynamic IGMP multicast group entries for VLAN-interface 100.

```
<Switch> reset igmp group interface vlan-interface 100 all
```

Clear the dynamic IGMP multicast group entry of group 225.0.0.1 for VLAN-interface 100.

```
<Switch> reset igmp group interface vlan-interface 100 225.0.0.1
```

Related commands

display igmp group

4.1.21. robust-count (IGMP view)

Use **robust-count** to set the IGMP querier's robustness variable globally.

Use **undo robust-count** to restore the default.

Syntax

robust-count *count*

undo robust-count

Default

The IGMP querier's robustness variable is 2.

Views

IGMP view

Predefined user roles

network-admin

Parameters

count: Specifies an IGMP querier's robustness variable in the range of 1 to 255.

Usage guidelines

The IGMP querier's robustness variable defines the number of times to retransmit queries if packet loss occurs. A higher robustness variable makes the IGMP querier more robust, but it increases the timeout time for multicast groups.

You can set the IGMP querier's robustness variable globally for all interfaces in IGMP view or for an interface in interface view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the global IGMP querier's robustness variable to 5.

```
<Switch> system-view
[Switch] igmp
[Switch-igmp] robust-count 5
```

Related commands

igmp robust-count

4.1.22. ssm-mapping (IGMP view)

Use **ssm-mapping** to configure an IGMP SSM mapping.

Use **undo ssm-mapping** to delete IGMP SSM mappings.

Syntax

ssm-mapping *source-address ipv4-acl-number*

undo ssm-mapping { *source-address* | **all** }

Default

No IGMP SSM mappings exist.

Views

IGMP view

Predefined user roles

network-admin

Parameters

source-address: Specifies a multicast source by its IP address.

ipv4-acl-number: Specifies a basic ACL number in the range of 2000 to 2999. Multicast groups in IGMP reports permitted by the ACL are associated with the IPv6 multicast source. If the ACL does

not exist or does not have valid rules, no multicast groups are associated with the IPv6 multicast source.

all: Specifies all IGMP SSM mappings.

Usage guidelines

When you configure a rule in the IPv4 basic ACL, follow these restrictions and guidelines:

- For the rule to take effect, do not specify the **vpn-instance** *vpn-instance* option.
- The **source** *source-address source-wildcard* option specifies a multicast group address.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

Examples

Configure an IGMP SSM mapping with multicast source 125.1.1.1 and multicast group range 232.1.1.0/24.

```
<Switch> system-view
[Switch] acl basic 2001
[Switch-acl-ipv4-basic-2001] rule permit source 232.1.1.1 0.0.0.255
[Switch-acl-ipv4-basic-2001] quit
[Switch] igmp
[Switch-igmp] ssm-mapping 125.1.1.1 2001
```

Related commands

display igmp ssm-mapping

4.1.23. startup-query-count (IGMP view)

Use **startup-query-count** to set the IGMP startup query count globally.

Use **undo startup-query-count** to restore the default.

Syntax

startup-query-count *count*

undo startup-query-count

Default

The IGMP startup query count equals the IGMP querier's robustness variable.

Views

IGMP view

Predefined user roles

network-admin

Parameters

count: Specifies an IGMP startup query count in the range of 1 to 255.

Usage guidelines

You can set the IGMP startup query count globally for all interfaces in IGMP view or for an interface in interface view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the global IGMP startup query count to 5.

```
<Switch> system-view
[Switch] igmp
[Switch-igmp] startup-query-count 5
```

Related commands

igmp startup-query-count

4.1.24. startup-query-interval (IGMP view)

Use **startup-query-interval** to set the IGMP startup query interval globally.

Use **undo startup-query-interval** to restore the default.

Syntax

startup-query-interval *interval*

undo startup-query-interval

Default

The IGMP startup query interval equals one quarter of the IGMP general query interval.

Views

IGMP view

Predefined user roles

network-admin

Parameters

interval: Specifies an IGMP startup query interval in the range of 1 to 31744 seconds.

Usage guidelines

You can set the IGMP startup query interval globally for all interfaces in IGMP view or for an interface in interface view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the global IGMP startup query interval to 100 seconds.

```
<Switch> system-view
[Switch] igmp
[Switch-igmp] startup-query-interval 100
```

Related commands

igmp startup-query-interval

Contents

A page of this section is **6-x-x**

5. PIM commands 5-1
5.1. PIM commands 5-1
5.1.1. bsm-reflection enable (PIM view) 5-1
5.1.2. bsr-policy (PIM view) 5-1
5.1.3. c-bsr (PIM view) 5-2
5.1.4. c-rp (PIM view) 5-3
5.1.5. crp-policy (PIM view) 5-4
5.1.6. display pim bsr-info 5-5
5.1.7. display pim claimed-route 5-7
5.1.8. display pim c-rp 5-8
5.1.9. display pim interface 5-9
5.1.10. display pim neighbor 5-12
5.1.11. display pim routing-table 5-14
5.1.12. display pim rp-info 5-16
5.1.13. hello-option dr-priority (PIM view) 5-18
5.1.14. hello-option holdtime (PIM view) 5-19
5.1.15. hello-option lan-delay (PIM view) 5-20
5.1.16. hello-option neighbor-tracking (PIM view) 5-21
5.1.17. hello-option override-interval (PIM view) 5-21
5.1.18. holdtime join-prune (PIM view) 5-22
5.1.19. jp-pkt-size (PIM view) 5-23
5.1.20. pim 5-23
5.1.21. pim bsr-boundary 5-24
5.1.22. pim hello-option dr-priority 5-24
5.1.23. pim hello-option holdtime 5-25
5.1.24. pim hello-option lan-delay 5-26
5.1.25. pim hello-option neighbor-tracking 5-26
5.1.26. pim hello-option override-interval 5-27
5.1.27. pim holdtime join-prune 5-28
5.1.28. pim neighbor-policy 5-29
5.1.29. pim passive 5-30
5.1.30. pim require-genid 5-30
5.1.31. pim sm 5-31
5.1.32. pim state-refresh-capable 5-31
5.1.33. pim timer hello 5-32
5.1.34. pim timer join-prune 5-33
5.1.35. pim triggered-hello-delay 5-33
5.1.36. register-policy (PIM view) 5-34
5.1.37. register-whole-checksum (PIM view) 5-35
5.1.38. snmp-agent trap enable pim 5-35
5.1.39. source-lifetime (PIM view) 5-36
5.1.40. source-policy (PIM view) 5-37
5.1.41. spt-switch-threshold (PIM view) 5-38
5.1.42. ssm-policy (PIM view) 5-39
5.1.43. state-refresh-interval (PIM view) 5-39
5.1.44. state-refresh-rate-limit (PIM view) 5-40
5.1.45. state-refresh-ttl (PIM view) 5-41
5.1.46. static-rp (PIM view) 5-41
5.1.47. timer hello (PIM view) 5-43
5.1.48. timer join-prune (PIM view) 5-43

5. PIM commands

MEMO:

The **vpn-instance** *vpn-instance-name* option for each command is supported by V7.2.18 and later software.

5.1. PIM commands

5.1.1. bsm-reflection enable (PIM view)

Use **bsm-reflection enable** to enable the device to forward BSMs out of their incoming interfaces.

Use **undo bsm-reflection enable** to disable the device from forwarding BSMs out of their incoming interfaces.

Syntax

bsm-reflection enable

undo bsm-reflection enable

Default

The device forwards BSMs out of their incoming interfaces.

Views

PIM view

Predefined user roles

network-admin

Usage guidelines

Disable this feature if all the devices in the PIM-SM domain have consistent routing information.

Examples

Disable the device from forwarding BSMs out of their incoming interfaces.

```
<Switch> system-view
[Switch] pim
[Switch-pim] undo bsm-reflection enable
```

5.1.2. bsr-policy (PIM view)

Use **bsr-policy** to configure a BSR policy.

Use **undo bsr-policy** to restore the default.

Syntax

bsr-policy *ipv4-acl-number*

undo bsr-policy

Default

No BSR policy exists, and all bootstrap messages are regarded as legal.

Views

PIM view

Predefined user roles

network-admin

Parameters

ipv4-acl-number: Specifies an IPv4 basic ACL by its number in the range of 2000 to 2999.

Usage guidelines

A BSR policy filters bootstrap messages to guard against BSR spoofing.

When you configure a rule in the IPv4 basic ACL, follow these restrictions and guidelines:

- For the rule to take effect, do not specify the **vpn-instance** *vpn-instance* option.
- The **source** *source-address source-wildcard* option specifies a BSR address.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure a BSR policy so that only the devices on subnet 10.1.1.0/24 can act as the BSR.

```
<Switch> system-view
[Switch] acl basic 2000
[Switch-acl-ipv4-basic-2000] rule permit source 10.1.1.0 0.0.0.255
[Switch-acl-ipv4-basic-2000] quit
[Switch] pim
[Switch-pim] bsr-policy 2000
```

Related commands

c-bsr (PIM view)

5.1.3. c-bsr (PIM view)

Use **c-bsr** to configure a candidate-BSR (C-BSR).

Use **undo c-bsr** to remove the configuration of a C-BSR.

Syntax

c-bsr *ip-address* [**scope** *group-address* { *mask-length* | *mask* }] [**hash-length** *hash-length* | **priority** *priority*] *

undo c-bsr *ip-address* [**scope** *group-address* { *mask-length* | *mask* }]

Default

No C-BSRs exist.

Views

PIM view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the IP address of a C-BSR. You must specify the IP address of a local PIM interface.

scope *group-address*: Specifies a multicast group by its IP address in the range of 239.0.0.0 to 239.255.255.255. If you do not specify a multicast group, this command designates the C-BSR to the global-scoped zone.

mask-length: Specifies an address mask length in the range of 8 to 32.

mask: Specifies an address mask.

hash-length *hash-length*: Specifies a hash mask length in the range of 0 to 32. The default setting is 30.

priority *priority*: Specifies a C-BSR priority in the range of 0 to 255. The default setting is 64. The greater the value, the higher the priority.

Usage guidelines

If you execute this command for a zone multiple times, the most recent configuration takes effect.

You can configure the same C-BSR for different zones.

Examples

Configure the interface with IP address 1.1.1.1 as a C-BSR for the global-scoped zone.

```
<Switch> system-view
[Switch] pim
[Switch-pim] c-bsr 1.1.1.1
```

5.1.4. c-rp (PIM view)

Use **c-rp** to configure a candidate-RP (C-RP).

Use **undo c-rp** to remove the configuration of a C-RP.

Syntax

c-rp *ip-address* [**advertisement-interval** *adv-interval* | **group-policy** *ipv4-acl-number* | **holdtime** *hold-time* | **priority** *priority*] *

undo c-rp *ip-address*

Default

No C-RPs exist.

Views

PIM view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the IP address of a C-RP. You must specify the IP address of a local PIM interface.

advertisement-interval *adv-interval*: Specifies a C-RP advertisement interval in the range of 1 to 65535 seconds. The default value is 60 seconds.

group-policy *ipv4-acl-number*: Specifies an IPv4 basic ACL by its number in the range of 2000 to 2999. If you specify an ACL, this command designates the C-RP to IPv4 multicast groups in C-RP advertisement messages that the ACL permits. The C-RP is designated to all IPv4 multicast groups when one of the following conditions exists:

- You do not specify an ACL.
- The specified ACL does not exist.
- The specified ACL does not have valid rules.

holdtime *hold-time*: Specifies a C-RP lifetime in the range of 1 to 65535 seconds. The default value is 150 seconds.

priority *priority*: Specifies a C-RP priority in the range of 0 to 255. The default setting is 192. The greater the value, the lower the priority.

Usage guidelines

To designate a C-RP to multiple multicast group ranges, create multiple rules that specify different multicast group ranges in the ACL.

When you configure a rule in the IPv4 basic ACL, follow these restrictions and guidelines:

- For the rule to take effect, do not specify the **vpn-instance** *vpn-instance* option.
- The **source** *source-address source-wildcard* option specifies a multicast group range.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

If you execute this command by using the same C-RP address multiple times, the most recent configuration takes effect.

Examples

Configure the interface with IP address 1.1.1.1 as a C-RP for multicast group ranges 225.1.0.0/16 and 226.2.0.0/16 and set its priority to 10.

```
<Switch> system-view
[Switch] acl basic 2000
[Switch-acl-ipv4-basic-2000] rule permit source 225.1.0.0 0.0.255.255
[Switch-acl-ipv4-basic-2000] rule permit source 226.2.0.0 0.0.255.255
[Switch-acl-ipv4-basic-2000] quit
[Switch] pim
[Switch-pim] c-rp 1.1.1.1 group-policy 2000 priority 10
```

5.1.5. crp-policy (PIM view)

Use **crp-policy** to configure a C-RP policy.

Use **undo crp-policy** to restore the default.

Syntax

crp-policy *ipv4-acl-number*

undo crp-policy

Default

No C-RP policy exists, and all C-RP messages are regarded as legal.

Views

PIM view

Predefined user roles

network-admin

Parameters

ipv4-acl-number: Specifies an IPv4 advanced ACL number in the range of 3000 to 3999.

Usage guidelines

A C-RP policy filters C-RP advertisement messages to guard against C-RP spoofing.

The device uses only the prefixes of the multicast group ranges in advertisement messages to match the destination field in ACL rules. For example, the multicast group range in an advertisement message is 224.1.0.0/16. If the prefix 224.1.0.0 is in the range specified by the destination field of an ACL rule, the specified C-RPs are designated to this multicast group range.

When you configure a rule in the IPv4 advanced ACL, follow these restrictions and guidelines:

- For the rule to take effect, do not specify the **vpn-instance** *vpn-instance* option.
- The **source** *source-address source-wildcard* option specifies an RP address.
- The **destination** *dest-address dest-wildcard* option specifies a multicast group address.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure a C-RP policy so that only devices in the range of 1.1.1.1/24 can be C-RPs for the groups in the range of 225.1.1.0/24.

```
<Switch> system-view
[Switch] acl advanced 3000
[Switch-acl-ipv4-adv-3000] rule permit ip source 1.1.1.1 0.0.0.255 destination 225.1.1.0
0.0.0.255
[Switch-acl-ipv4-adv-3000] quit
[Switch] pim
[Switch-pim] crp-policy 3000
```

Related commands

c-rp (PIM view)

5.1.6. display pim bsr-info

Use **display pim bsr-info** to display BSR information.

Syntax

display pim [**vpn-instance** *vpn-instance-name*] **bsr-info**

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays multicast boundary information on the public network.

Examples

Display BSR information.

```
<Switch> display pim bsr-info
 Scope: non-scoped
     State: Accept Preferred
     Bootstrap timer: 00:01:44
     Elected BSR address: 12.12.12.1
       Priority: 64
       Hash mask length: 30
       Uptime: 00:21:56

 Scope: 239.4.0.0/16
     State: Accept Any
     Scope-zone expiry timer: 00:21:12

 Scope: 239.1.0.0/16
     State: Elected
     Bootstrap timer: 00:00:26
     Elected BSR address: 17.1.11.1
       Priority: 64
       Hash mask length: 30
       Uptime: 02:53:37
     Candidate BSR address: 17.1.11.1
       Priority: 64
       Hash mask length: 30

 Scope: 239.2.2.0/24
     State: Candidate
     Bootstrap timer: 00:01:56
     Elected BSR address: 61.2.37.1
       Priority: 64
       Hash mask length: 30
       Uptime: 02:53:32
     Candidate BSR address: 17.1.12.1
       Priority: 64
       Hash mask length: 30

 Scope: 239.3.3.0/24
     State: Pending
     Bootstrap timer: 00:00:07
     Candidate BSR address: 17.1.13.1
       Priority: 64
```

```
Hash mask length: 30
```

Table 5-1 Command output

Field	Description
Bootstrap timer	Aging timer for the BSR.
Scope-zone expiry timer	Aging timer for the scoped zone.
Elected BSR address	Address of the elected BSR.
Candidate BSR address	Address of the C-BSR.
Priority	BSR priority.
Uptime	Length of time the BSR has been up.

5.1.7. display pim claimed-route

Use **display pim claimed-route** to display information about all routes that PIM uses.

Syntax

display pim [**vpn-instance** *vpn-instance-name*] **claimed-route** [*source-address*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays multicast boundary information on the public network.

source-address: Specifies a multicast source by its IP address. If you do not specify a multicast source, this command displays information about all routes that PIM uses.

Examples

Display information about all routes that PIM uses.

```
<Switch> display pim claimed-route
 RPF-route selecting rule: longest-match

 Route/mask: 7.11.0.0/16 (unicast (direct))
     RPF interface: Vlan-interface2, RPF neighbor: 8.0.0.2
     Total number of (S,G) or (*,G) dependent on this route entry: 4
     (7.11.0.10, 225.1.1.1)
     (7.11.0.10, 226.1.1.1)
     (7.11.0.10, 227.1.1.1)
     (*, 228.1.1.1)
 Route/mask: 7.12.0.0/16 (multicast static)
     RPF interface: Vlan-interface2, RPF neighbor: 8.0.0.3,
     Config NextHop: 8.0.0.5
```

```
Total number of (S,G) or (*,G) dependent on this route entry: 2
(7.12.0.10, 226.1.1.1)
(7.12.0.10, 225.1.1.1)
```

Table 5-2 Command output

Field	Description
Route/mask	Route entry. Route types in parentheses include: • **igp**—IGP unicast route. • **egp**—EGP unicast route. • **unicast (direct)**—Direct unicast route. • **unicast**—Other unicast route, such as static unicast route. • **mbgp**—MBGP route. • **multicast static**—Static multicast route.
RPF interface	Name of the RPF interface.
RPF neighbor	IP address of the RPF neighbor.
Config NextHop	Address of the configured next hop. This field is displayed only when the static multicast route is configured with a next hop.
Total number of (S,G) or (*,G) dependent on this route entry	Total number of (S, G) or (*, G) entries associated with the RPF route and the entry list.

5.1.8. display pim c-rp

Use **display pim c-rp** to display C-RP information.

Syntax

display pim [**vpn-instance** *vpn-instance-name*] **c-rp** [**local**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays multicast boundary information on the public network.

local: Specifies local C-RPs. If you do not specify this keyword, the command displays information about all C-RPs.

Usage guidelines

You can view information about learned C-RPs only on the BSR. On other devices, you can view information about the locally configured C-RPs.

Examples

Display information about learned C-RPs.

```
<Switch> display pim c-rp
```

```
Scope: non-scoped
    Group/MaskLen: 224.0.0.0/4
      C-RP address             Priority  HoldTime  Uptime    Expires
      1.1.1.1 (local)          192       150       03:01:36  00:02:29
      2.2.2.2                  192       150       1d:13h    00:02:02
    Group/MaskLen: 226.1.1.0/24 [B] Expires: 00:00:33
    Group/MaskLen: 225.1.0.0/16 [B]
      C-RP Address             Priority  HoldTime  Uptime    Expires
      3.3.3.3                  192       150       12w:5d    00:02:05
```

Display information about the locally configured C-RPs.

```
<Switch> display pim c-rp local
 Candidate RP: 12.12.12.9(Loop1)
    Priority: 192
    HoldTime: 150
    Advertisement interval: 60
    Next advertisement scheduled at: 00:00:48
```

Table 5-3 Command output

Field	Description
Group/MaskLen	Multicast group to which the C-RP is designated.
[B]	This field is not supported in the current software version. BIDIR-PIM C-RP. This field is not displayed if the C-RP is a PIM-SM C-RP.
C-RP address	IP address of the C-RP. If the C-RP resides on the device where the command is executed, this field displays **(local)** after the address.
Priority	Priority of the C-RP.
HoldTime	Lifetime of the C-RP.
Uptime	Length of time the C-RP has been up: • **w**—Weeks. • **d**—Days. • **h**—Hours.
Expires	Remaining lifetime for the C-RP and the multicast group.
Candidate RP	IP address of the locally configured C-RP.
Advertisement interval	Interval between two advertisement messages sent by the locally configured C-RP.
Next advertisement scheduled at	Remaining time for the locally configured C-RP to send the next advertisement message.

5.1.9. display pim interface

Use **display pim interface** to display PIM information for interfaces.

Syntax

display pim [**vpn-instance** *vpn-instance-name*] **interface** [*interface-type interface-number*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays multicast boundary information on the public network.

interface-type interface-number: Specifies an interface by its type and number. If you do not specify an interface, this command displays PIM information for all interfaces.

verbose: Displays detailed PIM information. If you do not specify this keyword, the command displays brief PIM information.

Examples

Display brief PIM information for all interfaces.

```
<Switch> display pim interface
 Interface          NbrCnt  HelloInt  DR-Pri     DR-Address
 Vlan1              1       30        1          10.1.1.2
 Vlan2              0       30        1          172.168.0.2     (local)
 Vlan3              1       30        1          20.1.1.2
```

Table 5-4 Command output

Field	Description
NbrCnt	Number of PIM neighbors.
HelloInt	Interval for sending hello messages.
DR-Pri	Priority for DR election.
DR-Address	IP address of the DR. If the DR resides on the device where the command is executed, this field displays **(local)** after the address.

Display detailed PIM information for VLAN-interface 1.

```
<Switch> display pim interface vlan-interface 1 verbose
 Interface: Vlan-interface1, 10.1.1.1
     PIM version: 2
     PIM mode: Sparse
     PIM DR: 10.1.1.2
     PIM DR Priority (configured): 1
     PIM neighbors count: 1
     PIM hello interval: 30 s
     PIM LAN delay (negotiated): 500 ms
     PIM LAN delay (configured): 500 ms
     PIM override interval (negotiated): 2500 ms
     PIM override interval (configured): 2500 ms
     PIM neighbor tracking (negotiated): disabled
     PIM neighbor tracking (configured): disabled
```

```
PIM generation ID: 0xF5712241
PIM require generation ID: disabled
PIM hello hold interval: 105 s
PIM assert hold interval: 180 s
PIM triggered hello delay: 5 s
PIM J/P interval: 60 s
PIM J/P hold interval: 210 s
PIM BSR domain border: disabled
PIM BFD: disabled
PIM passive: disabled
Number of routers on network not using DR priority: 0
Number of routers on network not using LAN delay: 0
Number of routers on network not using neighbor tracking: 2
```

Table 5-5 Command output

Field	Description
PIM version	Version of the PIM protocol.
PIM mode	PIM mode: dense or sparse.
PIM DR	IP address of the DR.
PIM DR Priority (configured)	Configured priority for DR election.
PIM neighbors count	Total number of PIM neighbors.
PIM hello interval	Interval between two hello messages.
PIM LAN delay (negotiated)	Negotiated PIM message propagation delay.
PIM LAN delay (configured)	Configured PIM message propagation delay.
PIM override interval (negotiated)	Negotiated interval for overriding prune messages.
PIM override interval (configured)	Configured interval for overriding prune messages.
PIM neighbor tracking (negotiated)	Negotiated neighbor tracking status: enabled or disabled.
PIM neighbor tracking (configured)	Configured neighbor tracking status: enabled or disabled.
PIM require generation ID	Whether the feature of discarding hello messages without Generation_ID is enabled.
PIM hello hold interval	PIM neighbor lifetime.
PIM assert hold interval	Assert holdtime timer.
PIM triggered hello delay	Maximum delay for sending hello messages.
PIM J/P interval	Interval between two join/prune messages.
PIM J/P hold interval	Joined/pruned state holdtime timer.
PIM BSR domain border	Whether a PIM domain border is configured.
PIM BFD	Whether PIM is enabled to work with BFD.
PIM passive	Whether PIM passive mode is enabled on the interface.
Number of routers on network not using DR priority	Number of routers that do not use the DR priority field on the subnet where the interface resides.

Field	Description
Number of routers on network not using LAN delay	Number of routers that do not use the LAN delay field on the subnet where the interface resides.
Number of routers on network not using neighbor tracking	Number of routers that are not enabled with neighbor tracking on the subnet where the interface resides.

5.1.10. display pim neighbor

Use **display pim neighbor** to display PIM neighbor information.

Syntax

display pim [**vpn-instance** *vpn-instance-name*] **neighbor** [*neighbor-address* | **interface** *interface-type interface-number* | **verbose**] *

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays multicast boundary information on the public network.

neighbor-address: Specifies a PIM neighbor by its IP address. If you do not specify a PIM neighbor, this command displays information about all PIM neighbors.

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays PIM neighbor information on all interfaces.

verbose: Displays detailed PIM neighbor information. If you do not specify this keyword, the command displays brief PIM neighbor information.

Examples

Display brief information about all PIM neighbors.

```
<Switch> display pim neighbor
 Total Number of Neighbors = 2

 Neighbor        Interface           Uptime   Expires  DR-Priority Mode
 10.1.1.2        Vlan1               02:50:49 00:01:31 1           B
 20.1.1.2        Vlan2               02:49:39 00:01:42 1
```

Display detailed information about the PIM neighbor with IP address 11.110.0.20.

```
<Switch> display pim neighbor 11.110.0.20 verbose
 Neighbor: 11.110.0.20
     Interface: Vlan-interface3
     Uptime: 00:00:10
     Expiry time: 00:00:30
     DR Priority: 1
```

```
Generation ID: 0x2ACEFE15
Holdtime: 105 s
LAN delay: 500 ms
Override interval: 2500 ms
State refresh interval: 60 s
Neighbor tracking: Disabled
Bidirectional PIM: Disabled
RPF proxy vector: Disabled
Secondary address(es):
22.1.1.2
22.1.1.3
22.1.1.4
22.1.1.5
22.1.1.6
22.1.1.7
22.1.1.8
```

Table 5-6 Command output

Field	Description
Total Number of Neighbors	Total number of PIM neighbors.
Neighbor	IP address of the PIM neighbor.
Interface	Interface that connects to the PIM neighbor.
Uptime	Length of time the PIM neighbor has been up.
Expires/Expiry time	Remaining lifetime for the PIM neighbor. If the PIM neighbor is always up and reachable, this field displays **never**.
DR-Priority/DR Priority	Priority of the PIM neighbor.
Mode	PIM mode. **B**—The PIM mode is BIDIR-PIM. This mode is not supported in the current software version. This field is empty if the PIM mode is not BIDIR-PIM and the RPF vector is disabled.
Generation ID	Generation ID of the PIM neighbor. (A random value represents a status change of the PIM neighbor.)
Holdtime	Lifetime of the PIM neighbor. If the PIM neighbor is always up and reachable, this field displays **forever**.
LAN delay	PIM message propagation delay on a shared-media LAN.
Override interval	Interval for overriding prune messages.
State refresh interval	Interval for refreshing state. This field is displayed only when the PIM neighbor operates in the PIM-DM mode and the state refresh capability is enabled.
Neighbor tracking	Neighbor tracking status: enabled or disabled.
Bidirectional PIM	This field is not supported in the current software version. Whether BIDIR-PIM is enabled.
RPF proxy vector	Whether the RPF vector feature is enabled.
Secondary address(es)	Secondary addresses of the PIM neighbor.

5.1.11. display pim routing-table

Use **display pim routing-table** to display PIM routing entries.

Syntax

display pim [**vpn-instance** *vpn-instance-name*] **routing-table** [*group-address* [**mask** { *mask-length* | *mask* }] | *source-address* [**mask** { *mask-length* | *mask* }] | **flags** *flag-value* | **fsm** | **incoming-interface** *interface-type interface-number* | **mode** *mode-type* | **outgoing-interface** { **exclude** | **include** | **match** } *interface-type interface-number*] *

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays multicast boundary information on the public network.

group-address: Specifies a multicast group by its IP address in the range of 224.0.0.0 to 239.255.255.255. If you do not specify a multicast group, this command displays PIM routing entries for all multicast groups.

source-address: Specifies a multicast source by its IP address.

mask-length: Specifies an address mask length in the range of 0 to 32. The default value is 32.

mask: Specifies an address mask. The default value is 255.255.255.255.

flags *flag-value*: Specifies a flag. If you do not specify a flag, this command displays PIM routing entries that contain all flags. The following lists the values for the *flag-value* argument and their meanings:

- **2msdp**: Specifies PIM routing entries to be contained in the next SA message to notify an MSDP peer.
- **act**: Specifies PIM routing entries that have been used for routing data.
- **del**: Specifies PIM routing entries to be deleted.
- **exprune**: Specifies PIM routing entries containing outgoing interfaces pruned by other multicast routing protocols.
- **ext**: Specifies PIM routing entries containing outgoing interfaces provided by other multicast routing protocols.
- **loc**: Specifies PIM routing entries on the devices that reside on the same subnet as the multicast source.
- **msdp**: Specifies PIM routing entries learned from MSDP SA messages.
- **niif**: Specifies PIM routing entries containing unknown incoming interfaces.
- **nonbr**: Specifies PIM routing entries with PIM neighbor lookup failure.
- **rpt**: Specifies PIM routing entries on the RPT branches where (S, G) prunes have been sent to the RP.

- **rq**: Specifies PIM routing entries of the receiving side of the data-MDT switchover.
- **spt**: Specifies PIM routing entries on the SPT.
- **sq**: Specifies PIM routing entries of the originator side of data-MDT switchover.
- **swt**: Specifies PIM routing entries in the process of RPT-to-SPT switchover.
- **vxlan**: Specifies VXLAN overlay entries maintained by PIM.
- **wc**: Specifies PIM routing entries with wildcards.

fsm: Displays detailed information about the finite state machine.

incoming-interface *interface-type interface-number*: Specifies an incoming interface. If you do not specify an incoming interface, this command displays PIM routing entries that contain all incoming interfaces.

mode *mode-type*: Specifies a PIM mode. If you do not specify a PIM mode, this command displays PIM routing entries in all PIM modes. The available PIM modes include:

- **sm**: Specifies PIM-SM.
- **ssm**: Specifies PIM-SSM.

outgoing-interface { **exclude** | **include** | **match** } *interface-type interface-number*: Specifies an outgoing interface. If you do not specify an outgoing interface, this command displays PIM routing entries that contain all outgoing interfaces. Whether an outgoing interface is contained in the PIM routing table depends on the following conditions:

- If you specify an excluded interface, this command displays PIM routing entries that do not contain the specified outgoing interface.
- If you specify an included interface, this command displays PIM routing entries that contain the specified outgoing interface.
- If you specify a matching interface, this command displays PIM routing entries that contain only the specified outgoing interface.

Examples

Display PIM routing entries.

```
<Switch> display pim routing-table
 Total 0 (*, G) entries; 1 (S, G) entries

 (172.168.0.12, 227.0.0.1)
     RP: 2.2.2.2
     Protocol: pim-sm, Flag: SPT LOC ACT
     UpTime: 02:54:43
     Upstream interface: Vlan-interface1
         Upstream neighbor: NULL
         RPF prime neighbor: NULL
     Downstream interface information:
     Total number of downstream interfaces: 1
         1: Vlan-interface2
             Protocol: pim-sm, UpTime: 02:54:43, Expires: 00:02:47
```

Table 5-7 Command output

Field	Description
Total 0 (*, G) entries; 1 (S, G) entries	Total number of (*, G) entries, and the total number of (S, G) entries.

Field	Description
(172.168.0.12, 227.0.0.1)	(S, G) entry.
Protocol	PIM mode.
Flag	Flag of the (S, G) entry or (*, G) entry: • **2MSDP**—The entry is to be advertised by the MSDP module in the next (S, A) message. • **ACT**—The entry has been used for routing data. • **DEL**—The entry is to be removed. • **EXPRUNE**—Some outgoing interfaces are pruned by other multicast routing protocols. • **EXT**—The entry contains outgoing interfaces provided by other multicast routing protocols. • **LOC**—The entry is on a router directly connected to the same subnet with the multicast source. • **MSDP**—The entry is learned from an MSDP (S, A) message. • **NIIF**—The entry contains unknown incoming interfaces. • **NONBR**—The entry has a PIM neighbor lookup failure. • **RPT**—The entry is on an RPT branch where (S, G) prunes have been sent to the RP. • **SPT**—The entry is on the SPT. • **SQ**—The entry triggers the default-MDT to data-MDT switchover. • **SWT**—The entry is in the process of RPT-to-SPT switchover. • **VXLAN**—The entry is a VXLAN overlay entry. • **WC**—The entry contains a wildcard.
Uptime	Length of time for which the (S, G) entry or (*, G) entry has been up.
Upstream interface	Upstream (incoming) interface of the (S, G) entry or (*, G) entry.
Upstream neighbor	Upstream neighbor of the (S, G) entry or (*, G) entry.
RPF prime neighbor	RPF neighbor of the (S, G) or (*, G) entry: • For a (*, G) entry, if the RPF neighbor is the RP, the field displays **NULL**. • For an (S, G) entry, if the RPF neighbor is a router that directly connects to the multicast source, this field displays **NULL**.
Downstream interface information	Information about the downstream interfaces: • Total number of downstream interfaces. • Names of the downstream interfaces. • Protocol type on the downstream interfaces. • Uptime of the downstream interfaces. • Expiration time of the downstream interfaces.

5.1.12. display pim rp-info

Use **`display pim rp-info`** to display PIM RP information.

Syntax

display pim [**vpn-instance** *vpn-instance-name*] **rp-info** [*group-address*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays multicast boundary information on the public network.

group-address: Specifies a multicast group by its IP address in the range of 224.0.1.0 to 239.255.255.255. If you do not specify a multicast group, this command displays RP information for all multicast groups.

Examples

Display RP information for multicast group 224.0.1.1.

```
<Switch> display pim rp-info 224.0.1.1
 BSR RP address is: 2.2.2.2
     Priority: 192
     HoldTime: 180
     Uptime: 03:01:10
     Expires: 00:02:30

 Static RP address is: 3.3.3.5
     Preferred: Yes
     Configured ACL: 2003

 RP mapping for this group is: 3.3.3.5

 Anycast-RP 3.3.3.5 members:
     Member address           State
     1.1.0.1                  Active
     1.2.0.2                  Local
     1.2.0.1                  Remote
```

Display RP information for all multicast groups.

```
<Switch> display pim rp-info
 BSR RP information:
   Scope: non-scoped
     Group/MaskLen: 224.0.0.0/4
       RP address               Priority  HoldTime  Uptime    Expires
       1.1.1.1 (local)          192       180       03:01:36  00:02:29
       2.2.2.2                  192       180       1d:13h    00:02:02

 Static RP information:
       RP address               ACL   Mode    Preferred
```

```
      3.3.3.1                 2000  pim-sm  No
      3.3.3.2                 2001  bidir   Yes
      3.3.3.3                 2002  pim-sm  No
      3.3.3.4                       pim-sm  No
      3.3.3.5                 2002  pim-sm  Yes

Anycast-RP information:
      RP address              Member address          State
      3.3.3.5                 1.1.0.1                 Active
      3.3.3.5                 1.1.0.2                 Local
      3.3.3.5                 1.2.0.1                 Remote
```

Table 5-8 Command output

Field	Description
BSR RP address is	IP address of the RP.
BSR RP information	Information about the RP.
Group/MaskLen	Multicast group to which the RP is designated.
[B]	This field is not supported in the current software version. The RP is a BIDIR-PIM RP. This field is not displayed if the RP is a PIM-SM RP.
RP address	IP address of the RP. If the RP resides on the device where the command is executed, this field displays **(local)** after the address.
Priority	Priority of the RP.
HoldTime	RP lifetime.
Uptime	Length of time the RP has been up.
Expires	Remaining lifetime for the RP.
Preferred	Whether the static RP is preferred.
Configured ACL/ACL	ACL defining the multicast groups to which the static RP is designated.
Mode	RP service mode: PIM-SM or BIDIR-PIM. BIDIR-PIM is not supported in the current software version.
RP mapping for this group	IP address of the RP that provides services for the multicast group.
Anycast-RP 3.3.3.5 members	Members of Anycast RP 3.3.3.5.
Member address	IP address of the Anycast RP member.
State	State of the interface from which the member address originates: • **Active**—Activated local interface. • **Local**—Inactivated local interface. • **Remote**—Remote interface.

5.1.13. hello-option dr-priority (PIM view)

Use **hello-option dr-priority** to set the DR priority globally.

Use **undo hello-option dr-priority** to restore the default.

Syntax

hello-option dr-priority *priority*

undo hello-option dr-priority

Default

The DR priority is 1.

Views

PIM view

Predefined user roles

network-admin

Parameters

priority: Specifies a DR priority in the range of 0 to 4294967295. The greater the value, the higher the priority.

Usage guidelines

You can set the DR priority globally for all interfaces in PIM view or for an interface in interface view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the global DR priority to 3.

```
<Switch> system-view
[Switch] pim
[Switch-pim] hello-option dr-priority 3
```

Related commands

pim hello-option dr-priority

5.1.14. hello-option holdtime (PIM view)

Use **hello-option holdtime** to set the PIM neighbor lifetime globally.

Use **undo hello-option holdtime** to restore the default.

Syntax

hello-option holdtime *time*

undo hello-option holdtime

Default

The PIM neighbor lifetime is 105 seconds.

Views

PIM view

Predefined user roles

network-admin

Parameters

time: Specifies a PIM neighbor lifetime in the range of 1 to 65535 seconds. If you set the value to 65535 seconds, PIM neighbors are always reachable.

Usage guidelines

You can set the PIM neighbor lifetime globally for all interfaces in PIM view or for an interface in interface view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the global PIM neighbor lifetime to 120 seconds.

```
<Switch> system-view
[Switch] pim
[Switch-pim] hello-option holdtime 120
```

Related commands

pim hello-option holdtime

5.1.15. hello-option lan-delay (PIM view)

Use **hello-option lan-delay** to set the PIM message propagation delay on a shared-media LAN globally.

Use **undo hello-option lan-delay** to restore the default.

Syntax

hello-option lan-delay *delay*

undo hello-option lan-delay

Default

The PIM message propagation delay on a shared-media LAN is 500 milliseconds.

Views

PIM view

Predefined user roles

network-admin

Parameters

delay: Specifies a PIM message propagation delay on a shared-media LAN, in the range of 1 to 32767 milliseconds.

Usage guidelines

You can set the PIM message propagation delay globally for all interfaces in PIM view or for an interface in interface view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the global PIM message propagation delay on a shared-media LAN to 200 milliseconds.

```
<Switch> system-view
[Switch] pim
[Switch-pim] hello-option lan-delay 200
```

Related commands

hello-option override-interval (PIM view)

pim hello-option lan-delay

pim hello-option override-interval

5.1.16. hello-option neighbor-tracking (PIM view)

Use **hello-option neighbor-tracking** to enable neighbor tracking globally.

Use **undo hello-option neighbor-tracking** to disable neighbor tracking globally.

Syntax

hello-option neighbor-tracking

undo hello-option neighbor-tracking

Default

Neighbor tracking is disabled.

Views

PIM view

Predefined user roles

network-admin

Usage guidelines

You can enable neighbor tracking globally for all interfaces in PIM view or for an interface in interface view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Enable neighbor tracking globally.

```
<Switch> system-view
[Switch] pim
[Switch-pim] hello-option neighbor-tracking
```

Related commands

pim hello-option neighbor-tracking

5.1.17. hello-option override-interval (PIM view)

Use **hello-option override-interval** to set the override interval globally.

Use **undo hello-option override-interval** to restore the default.

Syntax

hello-option override-interval *interval*

undo hello-option override-interval

Default

The override interval is 2500 milliseconds.

Views

PIM view

Predefined user roles

network-admin

Parameters

interval: Specifies an override interval in the range of 1 to 65535 milliseconds.

Usage guidelines

You can set the override interval globally for all interfaces in PIM view or for an interface in interface view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the global override interval to 2000 milliseconds.

```
<Switch> system-view
[Switch] pim
[Switch-pim] hello-option override-interval 2000
```

Related commands

hello-option lan-delay (PIM view)

pim hello-option lan-delay

pim hello-option override-interval

5.1.18. holdtime join-prune (PIM view)

Use **holdtime join-prune** to set the joined/pruned state holdtime globally.

Use **undo holdtime join-prune** to restore the default.

Syntax

holdtime join-prune *time*

undo holdtime join-prune

Default

The joined/pruned state holdtime is 210 seconds.

Views

PIM view

Predefined user roles

network-admin

Parameters

time: Specifies a joined/pruned state holdtime in the range of 1 to 65535 seconds.

Usage guidelines

You can set the joined/pruned state holdtime globally for all interfaces in PIM view or for an interface in interface view. For an interface, the interface-specific configuration takes priority over the global configuration.

To prevent the upstream neighbors from aging out, you must set the join/prune interval to be less than the joined/pruned state holdtime.

Examples

Set the global joined/pruned state holdtime to 280 seconds.

```
<Switch> system-view
[Switch] pim
[Switch-pim] holdtime join-prune 280
```

Related commands

pim holdtime join-prune

timer join-prune (PIM view)

5.1.19. jp-pkt-size (PIM view)

Use **jp-pkt-size** to set the maximum size of a join/prune message.

Use **undo jp-pkt-size** to restore the default.

Syntax

jp-pkt-size *size*

undo jp-pkt-size

Default

The maximum size of a join/prune message is 8100 bytes.

Views

PIM view

Predefined user roles

network-admin

Parameters

size: Specifies the maximum size of a join/prune message, in the range of 100 to 8100 bytes.

Examples

Set the maximum size of a join/prune message to 1500 bytes.

```
<Switch> system-view
[Switch] pim
[Switch-pim] jp-pkt-size 1500
```

5.1.20. pim

Use **pim** to enter PIM view.

Use **undo pim** to remove all configurations in PIM view.

Syntax

pim [**vpn-instance** *vpn-instance-name*]

undo pim [**vpn-instance** *vpn-instance-name*]

Views

System view

Predefined user roles

network-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays multicast boundary information on the public network.

Examples

Enable IP multicast routing and enter PIM view.

```
<Switch> system-view
[Switch] multicast routing
[Switch-mrib] quit
[Switch] pim
[Switch-pim]
```

Related commands

multicast routing-enable

5.1.21. pim bsr-boundary

Use **pim bsr-boundary** to configure a PIM-SM domain border (a bootstrap message boundary).

Use **undo pim bsr-boundary** to restore the default.

Syntax

pim bsr-boundary

undo pim bsr-boundary

Default

An interface is not a PIM-SM domain border.

Views

Interface view

Predefined user roles

network-admin

Examples

Configure VLAN-interface 100 as a PIM-SM domain border.

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] pim bsr-boundary
```

Related commands

c-bsr (PIM view)

multicast boundary

5.1.22. pim hello-option dr-priority

Use **pim hello-option dr-priority** to set the DR priority on an interface.

Use **undo pim hello-option dr-priority** to restore the default.

Syntax

pim hello-option dr-priority *priority*

undo pim hello-option dr-priority

Default

The DR priority is 1.

Views

Interface view

Predefined user roles

network-admin

Parameters

priority: Specifies a DR priority in the range of 0 to 4294967295. The greater the value, the higher the priority.

Usage guidelines

You can set the DR priority for an interface in interface view or globally for all interfaces in PIM view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the DR priority to 3 on VLAN-interface 100.

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] pim hello-option dr-priority 3
```

Related commands

hello-option dr-priority (PIM view)

5.1.23. pim hello-option holdtime

Use **pim hello-option holdtime** to set the PIM neighbor lifetime on an interface.

Use **undo pim hello-option holdtime** to restore the default.

Syntax

pim hello-option holdtime *time*

undo pim hello-option holdtime

Default

The PIM neighbor lifetime is 105 seconds.

Views

Interface view

Predefined user roles

network-admin

Parameters

time: Specifies a PIM neighbor lifetime in the range of 1 to 65535 seconds. If you set the value to 65535 seconds, the PIM neighbor is always reachable.

Usage guidelines

You can set the PIM neighbor lifetime for an interface in interface view or globally for all interfaces in PIM view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the PIM neighbor lifetime to 120 seconds on VLAN-interface 100.

```
<Switch> system-view
```

```
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] pim hello-option holdtime 120
```

Related commands

hello-option holdtime (PIM view)

5.1.24. pim hello-option lan-delay

Use **pim hello-option lan-delay** to set the PIM message propagation delay on a shared-media LAN for an interface.

Use **undo pim hello-option lan-delay** to restore the default.

Syntax

pim hello-option lan-delay *delay*

undo pim hello-option lan-delay

Default

The PIM message propagation delay on a shared-media LAN is 500 milliseconds.

Views

Interface view

Predefined user roles

network-admin

Parameters

delay: Specifies a PIM message propagation delay on a shared-media LAN in the range of 1 to 32767 milliseconds.

Usage guidelines

You can set the PIM message propagation delay for an interface in interface view or globally for all interfaces in PIM view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the PIM message propagation delay on a shared-media LAN to 200 milliseconds on VLAN-interface 100.

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] pim hello-option lan-delay 200
```

Related commands

hello-option lan-delay (PIM view)

hello-option override-interval (PIM view)

pim hello-option override-interval

5.1.25. pim hello-option neighbor-tracking

Use **pim hello-option neighbor-tracking** to enable neighbor tracking on an interface.

Use **pim hello-option neighbor-tracking disable** to disable neighbor tracking on an interface when neighbor tracking is enabled globally.

Use **undo pim hello-option neighbor-tracking** to restore neighbor tracking setting on an interface to be consistent with the global setting.

Syntax

pim hello-option neighbor-tracking

pim hello-option neighbor-tracking disable

undo pim hello-option neighbor-tracking

Default

Neighbor tracking is disabled on an interface.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

You can enable neighbor tracking for an interface in interface view or globally for all interfaces in PIM view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Enable neighbor tracking on VLAN-interface 100.

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] pim hello-option neighbor-tracking
```

Disable neighbor tracking on VLAN-interface 100 when neighbor tracking is enabled globally.

```
<Switch> system-view
[Switch] pim
[Switch-pim] hello-option neighbor-tracking
[Switch-pim] quit
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] pim hello-option neighbor-tracking disable
```

Related commands

hello-option neighbor-tracking (PIM view)

5.1.26. pim hello-option override-interval

Use **pim hello-option override-interval** to set the override interval on an interface.

Use **undo pim hello-option override-interval** to restore the default.

Syntax

pim hello-option override-interval *interval*

undo pim hello-option override-interval

Default

The override interval is 2500 milliseconds.

Views

Interface view

Predefined user roles

network-admin

Parameters

interval: Specifies an override interval in the range of 1 to 65535 milliseconds.

Usage guidelines

You can set the override interval for an interface in interface view or globally for all interfaces in PIM view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the override interval to 2000 milliseconds on VLAN-interface 100.

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] pim hello-option override-interval 2000
```

Related commands

hello-option lan-delay (PIM view)

hello-option override-interval (PIM view)

pim hello-option lan-delay

5.1.27. pim holdtime join-prune

Use **pim holdtime join-prune** to set the joined/pruned state holdtime on an interface.

Use **undo pim holdtime join-prune** to restore the default.

Syntax

pim holdtime join-prune *time*

undo pim holdtime join-prune

Default

The joined/pruned state holdtime is 210 seconds.

Views

Interface view

Predefined user roles

network-admin

Parameters

time: Specifies a joined/pruned state holdtime in the range of 1 to 65535 seconds.

Usage guidelines

You can set the joined/pruned state holdtime for an interface in interface view or globally for all interfaces in PIM view. For an interface, the interface-specific configuration takes priority over the global configuration.

To prevent the upstream neighbors from aging out, you must configure the join/prune interval to be less than the joined/pruned state holdtime.

Examples

Set the joined/pruned state holdtime to 280 seconds on VLAN-interface 100.

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] pim holdtime join-prune 280
```

Related commands

holdtime join-prune (PIM view)

pim timer join-prune

5.1.28. pim neighbor-policy

Use **pim neighbor-policy** to configure a PIM hello policy.

Use **undo pim neighbor-policy** to restore the default.

Syntax

pim neighbor-policy *ipv4-acl-number*

undo pim neighbor-policy

Default

No PIM hello policy exists on an interface, and all PIM hello messages are regarded as legal.

Views

Interface view

Predefined user roles

network-admin

Parameters

ipv4-acl-number: Specifies an IPv4 basic ACL number in the range of 2000 to 2999.

Usage guidelines

A PIM hello policy filters PIM hello messages to guard against hello message spoofing.

When you configure a rule in the IPv4 basic ACL, follow these restrictions and guidelines:

- For the rule to take effect, do not specify the **vpn-instance** *vpn-instance* option.
- The **source** *source-address source-wildcard* option specifies a source IP address.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure a PIM hello policy on VLAN-interface 100 so that only the devices on subnet 10.1.1.0/24 can become PIM neighbors of this switch.

```
<Switch> system-view
[Switch] acl basic 2000
[Switch-acl-ipv4-basic-2000] rule permit source 10.1.1.0 0.0.0.255
[Switch-acl-ipv4-basic-2000] quit
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] pim neighbor-policy 2000
```

5.1.29. pim passive

Use **pim passive** to enable PIM passive mode on an interface.

Use **undo pim passive** to disable PIM passive mode on an interface.

Syntax

pim passive

undo pim passive

Default

PIM passive mode is disabled on an interface.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

This command takes effect only when PIM-SM is enabled on the interface.

Examples

Enable IP multicast routing. Then, enable PIM-SM and PIM passive mode on VLAN-interface 100.

```
<Switch> system-view
[Switch] multicast routing
[Switch-mrib] quit
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] pim sm
[Switch-Vlan-interface100] pim passive
```

5.1.30. pim require-genid

Use **pim require-genid** to enable dropping hello messages without the generation ID options.

Use **undo pim require-genid** to restore the default.

Syntax

pim require-genid

undo pim require-genid

Default

Hello messages without the generation ID options are accepted.

Views

Interface view

Predefined user roles

network-admin

Examples

Enable VLAN-interface 100 to drop hello messages without the generation ID options.

```
<Switch> system-view
```

```
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] pim require-genid
```

5.1.31. pim sm

Use **pim sm** to enable PIM-SM.

Use **undo pim sm** to disable PIM-SM.

Syntax

pim sm

undo pim sm

Default

PIM-SM is disabled.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

This command takes effect only when IP multicast routing is enabled.

Examples

Enable IP multicast routing, and enable PIM-SM on VLAN-interface 100.

```
<Switch> system-view
[Switch] multicast routing
[Switch-mrib] quit
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] pim sm
```

Related commands

multicast routing

5.1.32. pim state-refresh-capable

Use **pim state-refresh-capable** to enable the state refresh feature on an interface.

Use **undo pim state-refresh-capable** to disable the state refresh feature.

Syntax

pim state-refresh-capable

undo pim state-refresh-capable

Default

The state refresh feature is enabled.

Views

Interface view

Predefined user roles

network-admin

Examples

Disable the state refresh feature on VLAN-interface 100.

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] undo pim state-refresh-capable
```

Related commands

state-refresh-interval (PIM view)

state-refresh-rate-limit (PIM view)

state-refresh-ttl (PIM view)

5.1.33. pim timer hello

Use **pim timer hello** to set the hello interval on an interface.

Use **undo pim timer hello** to restore the default.

Syntax

pim timer hello *interval*

undo pim timer hello

Default

The hello interval is 30 seconds.

Views

Interface view

Predefined user roles

network-admin

Parameters

interval: Specifies a hello interval in the range of 0 to 18000 seconds. If you set the value to 0 seconds, the interface does not send hello messages.

Usage guidelines

You can set the hello interval for an interface in interface view or globally for all interfaces in PIM view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the hello interval to 40 seconds on VLAN-interface 100.

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] pim timer hello 40
```

Related commands

timer hello (PIM view)

5.1.34. pim timer join-prune

Use **pim timer join-prune** to set the join/prune interval on an interface.

Use **undo pim timer join-prune** to restore the default.

Syntax

pim timer join-prune *interval*

undo pim timer join-prune

Default

The join/prune interval is 60 seconds.

Views

Interface view

Predefined user roles

network-admin

Parameters

interval: Specifies a join/prune interval in the range of 0 to 18000 seconds. If you set the value to 0 seconds, the interface does not send join or prune messages.

Usage guidelines

You can set the join/prune interval for an interface in interface view or globally for all interfaces in PIM view. For an interface, the interface-specific configuration takes priority over the global configuration.

The configuration takes effect after the current interval ends.

To prevent the upstream neighbors from aging out, you must set the join/prune interval to be less than the joined/pruned state holdtime.

Examples

Set the join/prune interval to 80 seconds on VLAN-interface 100.

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] pim timer join-prune 80
```

Related commands

pim holdtime join-prune

timer join-prune (PIM view)

5.1.35. pim triggered-hello-delay

Use **pim triggered-hello-delay** to set the triggered hello delay (maximum delay for sending a hello message).

Use **undo pim triggered-hello-delay** to restore the default.

Syntax

pim triggered-hello-delay *delay*

undo pim triggered-hello-delay

Default

The triggered hello delay is 5 seconds.

Views

Interface view

Predefined user roles

network-admin

Parameters

delay: Specifies a triggered hello delay in the range of 1 to 60 seconds.

Examples

Set the triggered hello delay to 3 seconds on VLAN-interface 100.

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] pim triggered-hello-delay 3
```

5.1.36. register-policy (PIM view)

Use **register-policy** to configure a PIM register policy.

Use **undo register-policy** to restore the default.

Syntax

register-policy *ipv4-acl-number*

undo register-policy

Default

No PIM register policy exists, and all PIM register messages are regarded as legal.

Views

PIM view

Predefined user roles

network-admin

Parameters

ipv4-acl-number: Specifies an IPv4 advanced ACL number in the range of 3000 to 3999.

Usage guidelines

A PIM register policy enables an RP to filter PIM register messages so that the RP is designated only to multicast groups permitted by the ACL.

When you configure a rule in the IPv4 advanced ACL, follow these restrictions and guidelines:

- For the rule to take effect, do not specify the **vpn-instance** *vpn-instance* option.
- The **source** *source-address source-wildcard* option specifies a multicast source address.
- The **destination** *dest-address dest-wildcard* option specifies a multicast group range.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure a PIM register policy. Then, the device accepts only register messages from the sources on the subnet 10.10.0.0/16 to the groups on the subnet 225.1.0.0/16.

```
<Switch> system-view
[Switch] acl advanced 3000
[Switch-acl-ipv4-adv-3000] rule permit ip source 10.10.0.0 0.0.255.255 destination
225.1.0.0 0.0.255.255
[Switch-acl-ipv4-adv-3000] quit
[Switch] pim
[Switch-pim] register-policy 3000
```

5.1.37. register-whole-checksum (PIM view)

Use **register-whole-checksum** to configure the device to calculate the checksum based on an entire register message.

Use **undo register-whole-checksum** to restore the default.

Syntax

register-whole-checksum

undo register-whole-checksum

Default

The device calculates the checksum based on the register message header.

Views

PIM view

Predefined user roles

network-admin

Examples

Configure the device to calculate the checksum based on an entire register message.

```
<Switch> system-view
[Switch] pim
[Switch-pim] register-whole-checksum
```

5.1.38. snmp-agent trap enable pim

Use **snmp-agent trap enable pim** to enable SNMP notifications for PIM.

Use **undo snmp-agent trap enable pim** to disable SNMP notifications for PIM.

Syntax

snmp-agent trap enable pim [**candidate-bsr-win-election** | **elected-bsr-lost-election** | **neighbor-loss**] *

undo snmp-agent trap enable pim [**candidate-bsr-win-election** | **elected-bsr-lost-election** | **neighbor-loss**] *

Default

SNMP notifications for PIM are enabled.

Views

System view

Predefined user roles

network-admin

Parameters

candidate-bsr-win-election: Specifies notifications about winning the BSR election.

elected-bsr-lost-election: Specifies notifications about losing the BSR election.

neighbor-loss: Specifies notifications about losing neighbors.

Usage guidelines

If you do not specify an optional keyword, this command enables or disables PIM to generate SNMP notifications.

To report critical PIM events to an NMS, enable SNMP notifications for PIM. For PIM event notifications to be sent correctly, you must also configure SNMP as described in *Network Management and Monitoring Configuration Guide*.

Examples

Disable SNMP notifications for PIM.

```
<Switch> system-view
[Switch] undo snmp-agent trap enable pim
```

5.1.39. source-lifetime (PIM view)

Use **source-lifetime** to set the multicast source lifetime.

Use **undo source-lifetime** to restore the default.

Syntax

source-lifetime *time*

undo source-lifetime

Default

The multicast source lifetime is 210 seconds.

Views

PIM view

Predefined user roles

network-admin

Parameters

time: Specifies a multicast source lifetime in the range of 0 to 31536000 seconds. If you set the value to 0 seconds, multicast sources never age out.

Examples

Set the multicast source lifetime to 200 seconds.

```
<Switch> system-view
[Switch] pim
[Switch-pim] source-lifetime 200
```

5.1.40. source-policy (PIM view)

Use **source-policy** to configure a multicast source policy.

Use **undo source-policy** to restore the default.

Syntax

source-policy *ipv4-acl-number*

undo source-policy

Default

No multicast source policy exists. The device does not filter multicast data packets.

Views

PIM view

Predefined user roles

network-admin

Parameters

ipv4-acl-number: Specifies an IPv4 basic or advanced ACL number in the range of 2000 to 3999.

Usage guidelines

A multicast source policy filters multicast data packets to control information available to downstream receivers.

When you configure a rule in the IPv4 ACL, follow these restrictions and guidelines:

- For the rule to take effect, do not specify the **vpn-instance** *vpn-instance* option.
- In a basic ACL, the **source** *source-address source-wildcard* option specifies a source IP address.
- In an advanced ACL, the **source** *source-address source-wildcard* option specifies a source IP address. The **destination** *dest-address dest-wildcard* option specifies a multicast group address.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure a multicast source policy to accept multicast data from source 10.10.1.2 and to deny multicast data from source 10.10.1.1.

```
<Switch> system-view
[Switch] acl basic 2000
[Switch-acl-ipv4-basic-2000] rule permit source 10.10.1.2 0
[Switch-acl-ipv4-basic-2000] rule deny source 10.10.1.1 0
[Switch-acl-ipv4-basic-2000] quit
[Switch] pim
[Switch-pim] source-policy 2000
```

5.1.41. spt-switch-threshold (PIM view)

Use **spt-switch-threshold** to configure a criterion for an RPT-to-SPT switchover.

Use **undo spt-switch-threshold** to remove criteria for RPT-to-SPT switchovers.

Syntax

spt-switch-threshold { **immediacy** | **infinity** } [**group-policy** *ipv4-acl-number*]

undo spt-switch-threshold [**immediacy** | **infinity**] [**group-policy** *ipv4-acl-number*]

Default

The first multicast packet triggers an RPT-to-STP switchover.

Views

PIM view

Predefined user roles

network-admin

Parameters

immediacy: Triggers an RPT-to-STP switchover immediately.

infinity: Disables RPT-to-STP switchover.

group-policy *ipv4-acl-number*: Specifies an IPv4 basic ACL number in the range of 2000 to 2999. If you specify an ACL, the configuration applies to the multicast groups that the ACL permits. The configuration applies to all multicast groups when one of the following conditions exists:

- You do not specify an ACL.
- The specified ACL does not exist.
- The specified ACL does not have valid rules.

Usage guidelines

CAUTION:
If the device is an RP, disabling RPT-to-STP switchover might cause multicast traffic forwarding failures on the source-side DR. When disabling RPT-to-SPT switchover, make sure you fully understand its impact on your network.

When you configure a rule in the IPv4 basic ACL, follow these restrictions and guidelines:

- For the rule to take effect, do not specify the **vpn-instance** *vpn-instance* option.
- The **source** *source-address source-wildcard* option specifies a multicast group address.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

Examples

Disable RPT-to-STP switchover on a receiver-side DR.

```
<Switch> system-view
[Switch] pim
[Switch-pim] spt-switch-threshold infinity
```

5.1.42. ssm-policy (PIM view)

Use **ssm-policy** to configure the SSM group range.

Use **undo ssm-policy** to restore the default.

Syntax

ssm-policy *ipv4-acl-number*

undo ssm-policy

Default

The SSM group range is 232.0.0.0/8.

Views

PIM view

Predefined user roles

network-admin

Parameters

ipv4-acl-number: Specifies an IPv4 basic ACL number in the range of 2000 to 2999.

Usage guidelines

This command defines a multicast group range that is used by PIM-SSM. For multicast packets that are permitted by the ACL, the PIM-SSM mode is used. For multicast packets that are not permitted by the ACL, the PIM-SM mode is used.

When you configure a rule in the IPv4 basic ACL, follow these restrictions and guidelines:

- For the rule to take effect, do not specify the **vpn-instance** *vpn-instance* option.
- The **source** *source-address source-wildcard* option specifies a multicast group range.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure the SSM group range as 232.1.0.0/16.

```
<Switch> system-view
[Switch] acl basic 2000
[Switch-acl-ipv4-basic-2000] rule permit source 232.1.0.0 0.0.255.255
[Switch-acl-ipv4-basic-2000] quit
[Switch] pim
[Switch-pim] ssm-policy 2000
```

5.1.43. state-refresh-interval (PIM view)

Use **state-refresh-interval** to set the state refresh interval.

Use **undo state-refresh-interval** to restore the default.

Syntax

state-refresh-interval *interval*

undo state-refresh-interval

Default

The state refresh interval is 60 seconds.

Views

PIM view

Predefined user roles

network-admin

Parameters

interval: Specifies a state refresh interval in the range of 1 to 255 seconds.

Examples

Set the state refresh interval to 70 seconds.

```
<Switch> system-view
[Switch] pim
[Switch-pim] state-refresh-interval 70
```

Related commands

pim state-refresh-capable

state-refresh-rate-limit (PIM view)

state-refresh-ttl (PIM view)

5.1.44. state-refresh-rate-limit (PIM view)

Use **state-refresh-rate-limit** to set the waiting time to accept a new state refresh message.

Use **undo state-refresh-rate-limit** to restore the default.

Syntax

state-refresh-rate-limit *time*

undo state-refresh-rate-limit

Default

The device waits 30 seconds before it accepts a new state refresh message.

Views

PIM view

Predefined user roles

network-admin

Parameters

time: Specifies the waiting time to accept a new refresh message, in the range of 1 to 65535 seconds.

Examples

Set the waiting time to 45 seconds to accept a new state refresh message.

```
<Switch> system-view
[Switch] pim
```

```
[Switch-pim] state-refresh-rate-limit 45
```

Related commands

pim state-refresh-capable

state-refresh-interval (PIM view)

state-refresh-ttl (PIM view)

5.1.45. state-refresh-ttl (PIM view)

Use **state-refresh-ttl** to set the TTL value for state refresh messages.

Use **undo state-refresh-ttl** to restore the default.

Syntax

state-refresh-ttl *ttl-value*

undo state-refresh-ttl

Default

The TTL value for state refresh messages is 255.

Views

PIM view

Predefined user roles

network-admin

Parameters

ttl-value: Specifies the TTL value for state refresh messages, in the range of 1 to 255.

Examples

Set the TTL value to 45 for state refresh messages.

```
<Switch> system-view
[Switch] pim
[Switch-pim] state-refresh-ttl 45
```

Related commands

pim state-refresh-capable (PIM view)

state-refresh-interval (PIM view)

state-refresh-rate-limit (PIM view)

5.1.46. static-rp (PIM view)

Use **static-rp** to configure a static RP.

Use **undo static-rp** to delete a static RP.

Syntax

static-rp *rp-address* [*ipv4-acl-number* | **preferred**] *

undo static-rp *rp-address*

Default

No static RPs exist.

Views

PIM view

Predefined user roles

network-admin

Parameters

rp-address: Specifies the IP address of the static RP. The IP address must be valid and cannot be on the subnet 127.0.0.0/8. For a static PIM-SM RP, you must specify a used IP address.

ipv4-acl-number: Specifies an IPv4 basic ACL number in the range of 2000 to 2999. If you specify an ACL, the static RP is designated only to multicast groups that the ACL permits. The static RP is designated to all multicast groups when one of the following conditions exists:

- You do not specify an ACL.
- The specified ACL does not exist.
- The specified ACL does not have valid rules.

preferred: Gives priority to the static RP if a dynamic RP also exists on the network. The dynamic RP takes effect only when the static RP fails. If you do not specify this keyword, the dynamic RP has priority, and the static RP takes effect only when the dynamic RP fails.

Usage guidelines

You do not need to enable PIM on an interface that acts as a static RP.

When you configure a rule in the IPv4 basic ACL, follow these restrictions and guidelines:

- For the rule to take effect, do not specify the **vpn-instance** *vpn-instance* option.
- The **source** *source-address source-wildcard* option specifies a multicast group address.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

When rules in the ACL used by a static RP change, new RPs are dynamically elected for all multicast groups.

You can configure multiple static RPs by using this command multiple times. However, if you specify the same static RP address or use the same ACL in the command, the most recent configuration takes effect. If you configure multiple static RPs for the same multicast group, the static RP with the highest IP address is used.

Examples

Configure the interface with IP address 11.110.0.6 as a static RP for multicast group range 225.1.1.0/24 and give priority to this static RP.

```
<Switch> system-view
[Switch] acl basic 2001
[Switch-acl-ipv4-basic-2001] rule permit source 225.1.1.0 0.0.0.255
[Switch-acl-ipv4-basic-2001] quit
[Switch] pim
[Switch-pim] static-rp 11.110.0.6 2001 preferred
```

Related commands

display pim rp-info

5.1.47. timer hello (PIM view)

Use **timer hello** to set the hello interval globally.

Use **undo timer hello** to restore the default.

Syntax

timer hello *interval*

undo timer hello

Default

The hello interval is 30 seconds.

Views

PIM view

Predefined user roles

network-admin

Parameters

interval: Specifies a hello interval in the range of 0 to 18000 seconds. If you set the value to 0 seconds, the device does not send hello messages.

Usage guidelines

You can set the hello interval globally for all interfaces in PIM view or for an interface in interface view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the global hello interval to 40 seconds.

```
<Switch> system-view
[Switch] pim
[Switch-pim] timer hello 40
```

Related commands

pim timer hello

5.1.48. timer join-prune (PIM view)

Use **timer join-prune** to set the join/prune interval globally.

Use **undo timer join-prune** to restore the default.

Syntax

timer join-prune *interval*

undo timer join-prune

Default

The join/prune interval is 60 seconds.

Views

PIM view

Predefined user roles

network-admin

Parameters

interval: Specifies a join/prune interval in the range of 0 to 18000 seconds. If you set the value to 0 seconds, the device does not send join or prune messages.

Usage guidelines

You can set the join/prune interval globally for all interfaces in PIM view or for an interface in interface view. For an interface, the interface-specific configuration takes priority over the global configuration.

The configuration takes effect after the current interval ends.

To prevent the upstream neighbors from expiring, you must set the join/prune interval to be less than the joined/pruned state holdtime.

Examples

Set the global join/prune interval to 80 seconds.

```
<Switch> system-view
[Switch] pim
[Switch-pim] timer join-prune 80
```

Related commands

holdtime join-prune (PIM view)

pim timer join-prune

Contents

A page of this section is **6-x-x**

6. MSDP commands ····· 6-1
6.1. MSDP commands ····· 6-1
6.1.1. cache-sa-enable ····· 6-1
6.1.2. display msdp brief ····· 6-1
6.1.3. display msdp peer-status ····· 6-3
6.1.4. display msdp sa-cache ····· 6-6
6.1.5. display msdp sa-count ····· 6-7
6.1.6. encap-data-enable ····· 6-8
6.1.7. import-source ····· 6-9
6.1.8. msdp ····· 6-10
6.1.9. originating-rp ····· 6-10
6.1.10. peer ····· 6-11
6.1.11. peer description ····· 6-12
6.1.12. peer mesh-group ····· 6-12
6.1.13. peer request-sa-enable ····· 6-13
6.1.14. peer sa-cache-maximum ····· 6-13
6.1.15. peer sa-policy ····· 6-14
6.1.16. peer sa-request-policy ····· 6-15
6.1.17. reset msdp peer ····· 6-16
6.1.18. reset msdp sa-cache ····· 6-17
6.1.19. reset msdp statistics ····· 6-17
6.1.20. shutdown (MSDP view) ····· 6-18
6.1.21. static-rpf-peer ····· 6-18
6.1.22. timer retry ····· 6-19

6. MSDP commands

6.1. MSDP commands

6.1.1. cache-sa-enable

Use **cache-sa-enable** to enable the SA message cache mechanism to cache the (S, G) entries contained in SA messages.

Use **undo cache-sa-enable** to disable the SA message cache mechanism.

Syntax

cache-sa-enable

undo cache-sa-enable

Default

The SA message cache mechanism is enabled, and the device caches the (S, G) entries contained in received SA messages.

Views

MSDP view

Predefined user roles

network-admin

Examples

Enable the SA message cache mechanism, so that the device caches the (S, G) entries contained in the received SA messages.

```
<Switch> system-view
[Switch] msdp
[Switch-msdp] cache-sa-enable
```

Related commands

display msdp sa-cache

display msdp sa-count

6.1.2. display msdp brief

Use **display msdp brief** to display brief information about MSDP peers.

Syntax

display msdp brief [**state** { **connect** | **disabled** | **established** | **listen** | **shutdown** }]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

state: Specifies a state. If you do not specify this keyword, the command displays brief information about MSDP peers in all states.

connect: Specifies the connecting state.

disabled: Specifies the connection failure state.

established: Specifies the session state.

listen: Specifies the listening state.

shutdown: Specifies the shutdown state.

Examples

Display brief information about MSDP peers in all states.

```
<Switch> display msdp brief
Configured    Established  Listen       Connect      Shutdown     Disabled
1             1            0            0            0            0

Peer address     State       Up/Down time    AS          SA count    Reset count
20.20.20.20      Established 00:00:13        100         0           0
```

Table 6-1 Command output

Field	Description
Configured	Number of MSDP peers that have been configured.
Established	Number of MSDP peers in established state.
Listen	Number of MSDP peers in listening state.
Connect	Number of MSDP peers in connecting state.
Shutdown	Number of MSDP peers in shutdown state.
Disabled	Number of MSDP peers in connection failure state.
Peer address	MSDP peer address.
State	MSDP peer status: • **Established**—A session has been established and the MSDP peer is in session. • **Listen**—A session has been established and the local device acts as the server in listening state. • **Connect**—A session is not established and the local device acts as a client in connecting state. • **Shutdown**—The session has been torn down. • **Down**—The connection failed.
Up/Down time	Length of time since the MSDP peering connection was established or torn down.
AS	Number of the AS where the MSDP peer is located. If the system could not obtain the AS number, this field displays a question mark (?).
SA count	Number of (S, G) entries in the SA cache.
Reset count	MSDP peering connection reset times.

6.1.3. display msdp peer-status

Use **display msdp peer-status** to display detailed status information for MSDP peers.

Syntax

display msdp peer-status [*peer-address*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

peer-address: Specifies an MSDP peer by its address. If you do not specify an MSDP peer, this command displays detailed status information for all MSDP peers.

Examples

Display detailed status information for MSDP peer 20.20.20.20.

```
<Switch> display msdp peer-status 20.20.20.20
MSDP peer 20.20.20.20; AS 100
 Description:
 Information about connection status:
   State: Disabled
   Up/down time: 14:41:08
   Resets: 0
   Connection interface: LoopBack0 (20.20.20.30)
   Received/sent messages: 867/867
   Discarded input messages: 0
   Discarded output messages: 0
   Elapsed time since last connection or counters clear: 14:42:40
   Mesh group peer joined: momo
   Last disconnect reason: Hold timer expired with truncated message
   Truncated packet: 5 bytes in buffer, type: 1, length: 20, without packet time: 75s
 Information about (Source, Group)-based SA filtering policy:
   Import policy: None
   Export policy: None
 Information about SA-Requests:
   Policy to accept SA-Requests: None
   Sending SA-Requests status: Disable
 Minimum TTL to forward SA with encapsulated data: 0
 SAs learned from this peer: 0, SA cache maximum for the peer: 4294967295
 Input queue size: 0, Output queue size: 0
 Counters for MSDP messages:
   RPF check failure: 0
   Incoming/outgoing SA: 0/0
   Incoming/outgoing SA-Request: 0/0
   Incoming/outgoing SA-Response: 0/0
```

```
Incoming/outgoing Keepalive: 867/867
Incoming/outgoing Notification: 0/0
Incoming/outgoing Traceroutes in progress: 0/0
Incoming/outgoing Traceroute reply: 0/0
Incoming/outgoing Unknown: 0/0
Incoming/outgoing data packet: 0/0
```

Table 6-2 Command output

Field	Description
MSDP peer	MSDP peer address.
AS	Number of the AS where the MSDP peer is located. If the system could not obtain the AS number, this field displays a question mark (?).
State	MSDP peer status: • **Established**—A session has been established and the MSDP peer is in session. • **Listen**—A session has been established and the local device acts as the server in listening state. • **Connect**—A session is not established and the local device acts as a client in connecting state. • **Shutdown**—The session has been torn down. • **Disabled**—The connection failed.
Up/Down time	Length of time since the MSDP peering connection was established or torn down.
Resets	MSDP peering connection reset times.
Connection interface	Interface and IP address used for setting up a TCP connection with the remote MSDP peer.
Received/sent messages	Number of SA messages sent and received through this connection.
Discarded input messages	Number of discarded incoming messages.
Discarded output messages	Number of discarded outgoing messages.
Elapsed time since last connection or counters clear	Elapsed time since the MSDP peer information was last cleared.
Mesh group peer joined	Mesh group that the MSDP peer has joined. This field is not displayed if the MSDP peer does not join a mesh group.

Last disconnect reason	Reason why last MSDP peering connection was torn down. If the connection is not terminated, this field does not display a value.
	• **Hold timer expired without message**—Hold timer expires and the receiving cache has no messages.
	• **Hold timer expired with truncated message**—Hold timer expires and messages in the receiving buffer are not intact.
	  ○ **bytes in buffer**—Size of data in the receiving buffer when the connection was terminated.
	  ○ **type**—Type of packets in the receiving buffer when the connection was terminated.
	  ○ **length**—Length of packets in the receiving buffer when the connection was terminated. If the packet is too small in size, this field cannot be resolved and

Field	Description
	is not displayed. ○ **without packet time**—Length of time since packets were last processed. • **Remote peer has been closed**—The MSDP peering connection has been torn down. • **TCP ERROR/HUP event received**—Error/hup event received by the TCP socket when the MSDP peer sent messages. • **Illegal message received**—The MSDP peer received illegal messages. • **Notification received**—The MSDP peer received notification messages. • **Reset command executed**—The user executed the **reset msdp peer** command. • **Shutdown command executed**—The user executed the **shutdown** command. • **Interface downed**—The MSDP peer received the interface down event when connecting to the remote MSDP peer.
Information about (Source, Group)-based SA filtering policy	SA message filtering list information: • **Import policy**—Filter list for receiving SA messages from the specified MSDP peer. • **Export policy**—Filter list for forwarding SA messages from the specified MSDP peer.
Information about SA-Requests	SA request information: • **Policy to accept SA request messages**—Filtering rule for receiving or forwarding SA request messages from the specified MSDP peer. If SA request messages are not filtered, this field displays **None**. • **Sending SA requests status**—Whether the MSDP peer is enabled to send an SA request message to the designated MSDP peer after receiving a new join message.
Minimum TTL to forward SA with encapsulated data	Lower TTL threshold for the multicast packets encapsulated in SA messages.
SAs learned from this peer	Number of cached (S, G) entries learned from the specified MSDP peer.
SA-cache maximum for the peer	Maximum number of (S, G) entries learned from the specified MSDP peer that the device can cache.
Input queue size	Data size cached in the input queue.
Output queue size	Data size cached in the output queue.
Counters for MSDP message	MSDP peer statistics: • **RPF check failure**—Number of SA messages discarded because of RPF check failure. • **Incoming/outgoing SA**—Number of received and sent SA messages. • **Incoming/outgoing SA-Request**—Number of received and sent SA requests. • **Incoming/outgoing SA-Response**—Number of received and sent SA responses. • **Incoming/outgoing Keepalive**—Number of received and sent keepalive messages.

Field	Description
	• **Incoming/outgoing Notification**—Number of received and sent notification messages. • **Incoming/outgoing Traceroutes in progress**—Number of received and sent traceroute-in-progress messages. • **Incoming/outgoing Traceroute reply**—Number of received and sent traceroute replies. • **Incoming/outgoing Unknown**—Number of received and sent unknown messages. • **Incoming/outgoing data packet**—Number of received and sent SA messages encapsulated with multicast data.

6.1.4. display msdp sa-cache

Use **display msdp sa-cache** to display (S, G) entries in the SA cache.

Syntax

display msdp sa-cache [*group-address* | *source-address* | *as-number*] *

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

group-address: Specifies a multicast group by its IP address in the range of 224.0.1.0 to 239.255.255.255. If you do not specify a multicast group, this command displays (S, G) entries in the SA cache for all multicast groups.

source-address: Specifies a multicast source by its IP address. If you do not specify a multicast source, this command displays (S, G) entries in the SA cache for all sources.

as-number: Specifies an AS number in the range of 1 to 4294967295. If you do not specify an AS number, this command displays (S, G) entries in the SA cache for all ASs.

Usage guidelines

For this command to display output, you must first execute the **cache-sa-enable** command before you execute this command.

Examples

Display (S, G) entries in the SA cache.

```
<Switch> display msdp sa-cache
Total Source-Active Cache - 5 entries
Matched 5 entries

Source          Group           Origin RP       Pro  AS         Uptime   Expires
10.10.1.2       225.0.0.1       10.10.10.10     BGP  100        00:00:11 00:05:49
10.10.1.2       225.0.0.2       10.10.10.10     BGP  100        00:00:11 00:05:49
10.10.1.2       225.0.0.3       10.10.10.10     BGP  100        00:00:11 00:05:49
```

```
10.10.1.2       225.0.0.4       10.10.10.10     BGP  100        00:00:11 00:05:49
10.10.1.2       225.0.0.5       10.10.10.10     BGP  100        00:00:11 00:05:49
```

Table 6-3 Command output

Field	Description
Total Source-Active Cache	Total number of multicast sources in the SA cache.
Matched	Total number of (S, G) entries that match a multicast sources.
Source	Multicast source address.
Group	Multicast group address.
Origin RP	Address of the RP that generated the (S, G) entry.
Pro	Type of protocol from which the AS number of the origin RP originates. If the system could not obtain the AS number, this field displays a question mark (?).
AS	AS number of the origin RP. If the system could not obtain the AS number, this field displays a question mark (?).
Uptime	Length of time for which the cached (S, G) entry has existed.
Expires	Length of time in which the cached (S, G) entry will expire.

Related commands

cache-sa-enable

6.1.5. display msdp sa-count

Use **display msdp sa-count** to display the number of (S, G) entries in the SA cache.

Syntax

display msdp sa-count [*as-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

as-number: Specifies an AS number in the range of 1 to 4294967295. If you do not specify an AS number, this command displays the number of (S, G) entries in the SA cache for all ASs.

Usage guidelines

For this command to display output, you must first execute the **cache-sa-enable** command before you execute this command.

Examples

Display the number of (S, G) entries in the SA cache.

```
<Switch> display msdp sa-count
(S, G) entries statistics, counted by peer
  Peer address       SA count
  10.10.10.10        5

(S, G) entries statistics, counted by AS
  AS          Source count        Group count
  ?           3                   3

5 (S, G) entries in total
```

Table 6-4 Command output

Field	Description
(S, G) entries statistics, counted by peer	Number of (S, G) entries on an MSDP peer basis.
Peer address	Address of the MSDP peer that sent SA messages.
SA count	Number of (S, G) entries from the MSDP peer.
(S, G) entries statistics, counted by AS	Number of cached (S, G) entries on an AS basis.
AS	AS number. If the system could not obtain the AS number, this field displays a question mark (?).
Source count	Number of multicast sources in the AS.
Group count	Number of multicast groups in the AS.
(S, G) entries in total	Total number of (S, G) entries.

Related commands

cache-sa-enable

6.1.6. encap-data-enable

Use **encap-data-enable** to enable multicast data encapsulation in SA messages.

Use **undo encap-data-enable** to restore the default.

Syntax

encap-data-enable

undo encap-data-enable

Default

An SA message contains only (S, G) entries. Multicast data is not encapsulated in an SA message.

Views

MSDP view

Predefined user roles

network-admin

Examples

Enable multicast data encapsulation in SA messages.

```
<Switch> system-view
[Switch] msdp
[Switch-msdp] encap-data-enable
```

6.1.7. import-source

Use **import-source** to configure an SA message creation policy.

Use **undo import-source** to restore the default.

Syntax

import-source [**acl** *ipv4-acl-number*]

undo import-source

Default

When an SA message is created, all the (S, G) entries within the domain are advertised in the SA message.

Views

MSDP view

Predefined user roles

network-admin

Parameters

ipv4-acl-number: Specifies an IPv4 basic or advanced ACL number in the range of 2000 to 3999. If you specify an ACL, this command advertises only the (S, G) entries that the ACL permits. This command does not advertise (S, G) entries when one of the following conditions exists:

- You do not specify an ACL.
- The specified ACL does not exist.
- The specified ACL does not have valid rules.

Usage guidelines

This command controls the creation of SA messages. To control forwarding or acceptance of SA messages, use the **peer sa-policy** command.

When you configure a rule in the IPv4 ACL, follow these restrictions and guidelines:

- For the rule to take effect, do not specify the **vpn-instance** *vpn-instance* option.
- In a basic ACL, the **source** *source-address source-wildcard* option specifies a multicast group address.
- In an advanced ACL, the **source** *source-address source-wildcard* option specifies a multicast source address. The **destination** *dest-address dest-wildcard* option specifies a multicast group address.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

If you configure this command multiple times, the most recent configuration takes effect.

Examples

Configure an SA creation policy to advertise only (10.10.0.0/16, 225.1.0.0/16) entries in SA messages.

```
<Switch> system-view
```

```
[Switch] acl advanced 3101
[Switch-acl-ipv4-adv-3101] rule permit ip source 10.10.0.0 0.0.255.255 destination
225.1.0.0 0.0.255.255
[Switch-acl-ipv4-adv-3101] quit
[Switch] msdp
[Switch-msdp] import-source acl 3101
```

Related commands

peer sa-policy

6.1.8. msdp

Use **msdp** to enable MSDP and enter MSDP view.

Use **undo msdp** to disable MSDP and delete the configurations in MSDP view.

Syntax

msdp

undo msdp

Default

MSDP is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command takes effect only when IP multicast routing is enabled.

Examples

Enable IP multicast routing. Then, enable MSDP and enter MSDP view.

```
<Switch> system-view
[Switch] multicast routing
[Switch-mrib] quit
[Switch] msdp
[Switch-msdp]
```

Related commands

multicast routing

6.1.9. originating-rp

Use **originating-rp** to configure the originating RP of SA messages.

Use **undo originating-rp** to restore the default.

Syntax

originating-rp *interface-type interface-number*

undo originating-rp

Default

SA messages are originated by real RPs.

Views

MSDP view

Predefined user roles

network-admin

Parameters

interface-type interface-number: Specifies an interface by its type and number.

Examples

Configure VLAN-interface 100 as the originating RP of SA messages.

```
<Switch> system-view
[Switch] msdp
[Switch-msdp] originating-rp vlan-interface 100
```

6.1.10. peer

Use **peer** to specify an MSDP peer.

Use **undo peer** to remove an MSDP peer.

Syntax

peer *peer-address* **connect-interface** *interface-type interface-number*

undo peer *peer-address*

Default

No MSDP peers exist.

Views

MSDP view

Predefined user roles

network-admin

Parameters

peer-address: Specifies an MSDP peer by its IP address.

connect-interface *interface-type interface-number*: Specifies an interface by its type and number. The local device uses the primary IP address of the specified interface to establish a TCP connection with the remote MSDP peer.

Usage guidelines

You must execute this command before you use any other **peer** commands.

Examples

Specify the router with IP address 125.10.7.6 as an MSDP peer and VLAN-interface 100 as the local connection port.

```
<Switch> system-view
[Switch] msdp
[Switch-msdp] peer 125.10.7.6 connect-interface vlan-interface 100
```

6.1.11. peer description

Use **peer description** to configure a description for an MSDP peer.

Use **undo peer description** to delete the description for an MSDP peer.

Syntax

peer *peer-address* **description** *text*

undo peer *peer-address* **description**

Default

No description exists.

Views

MSDP view

Predefined user roles

network-admin

Parameters

peer-address: Specifies an MSDP peer by its IP address.

text: Specifies a description, a case-sensitive string of 1 to 80 characters.

Examples

Configure the description **CustomerA** for the MSDP peer with IP address 125.10.7.6.

```
<Switch> system-view
[Switch] msdp
[Switch-msdp] peer 125.10.7.6 description CustomerA
```

6.1.12. peer mesh-group

Use **peer mesh-group** to assign an MSDP peer to a mesh group.

Use **undo peer mesh-group** to remove an MSDP peer from a mesh group.

Syntax

peer *peer-address* **mesh-group** *name*

undo peer *peer-address* **mesh-group**

Default

An MSDP peer does not belong to a mesh group.

Views

MSDP view

Predefined user roles

network-admin

Parameters

peer-address: Specifies an MSDP peer by its IP address.

name: Specifies a mesh group, a case-sensitive string of 1 to 32 characters. A mesh group name must not contain spaces.

Examples

Assign the MSDP peer with IP address 125.10.7.6 to mesh group **Group1**.

```
<Switch> system-view
[Switch] msdp
[Switch-msdp] peer 125.10.7.6 mesh-group Group1
```

6.1.13. peer request-sa-enable

Use **peer request-sa-enable** to enable the device to send an SA request message to an MSDP peer after receiving a new join message.

Use **undo peer request-sa-enable** to disable the device from sending an SA request message to an MSDP peer.

Syntax

peer *peer-address* **request-sa-enable**

undo peer *peer-address* **request-sa-enable**

Default

After receiving a new join message, the device does not send an SA request message to MSDP peers. Instead, it waits for an SA message.

Views

MSDP view

Predefined user roles

network-admin

Parameters

peer-address: Specifies an MSDP peer by its IP address.

Usage guidelines

For the device to send out SA request messages, you must disable the SA message cache mechanism before you execute this command.

Examples

Disable the SA message cache mechanism.

```
<Switch> system-view
[Switch] msdp
[Switch-msdp] undo cache-sa-enable
```

Enable the device to send an SA request message to MSDP peer 125.10.7.6 after it receives a new join message.

```
[Switch-msdp] peer 125.10.7.6 request-sa-enable
```

Related commands

cache-sa-enable

display msdp peer-status

6.1.14. peer sa-cache-maximum

Use **peer sa-cache-maximum** to set the maximum number of (S, G) entries in the SA cache learned from an MSDP peer.

Use **undo peer sa-cache-maximum** to restore the default.

Syntax

peer *peer-address* **sa-cache-maximum** *sa-limit*

undo peer *peer-address* **sa-cache-maximum**

Default

The device can cache a maximum of 4294967295 (S, G) entries learned from an MSDP peer.

Views

MSDP view

Predefined user roles

network-admin

Parameters

peer-address: Specifies an MSDP peer by its IP address.

sa-limit: Specifies the maximum number of (S, G) entries in the SA cache, in the range of 1 to 4294967295.

Examples

Set the maximum number to 100 for (S, G) entries in the SA cache learned from MSDP peer 125.10.7.6.

```
<Switch> system-view
[Switch] msdp
[Switch-msdp] peer 125.10.7.6 sa-cache-maximum 100
```

Related commands

display msdp brief

display msdp peer-status

display msdp sa-count

6.1.15. peer sa-policy

Use **peer sa-policy** to configure an SA incoming or outgoing policy for an MSDP peer.

Use **undo peer sa-policy** to delete the SA incoming or outgoing policy for an MSDP peer.

Syntax

peer *peer-address* **sa-policy** { **export** | **import** } [**acl** *ipv4-acl-number*]

undo peer *peer-address* **sa-policy** { **export** | **import** }

Default

No SA incoming or outgoing policy exists, and all SA messages from an MSDP peer are accepted or forwarded.

Views

MSDP view

Predefined user roles

network-admin

Parameters

peer-address: Specifies an MSDP peer by its IP address.

export: Specifies the outgoing direction.

import: Specifies the incoming direction.

ipv4-acl-number: Specifies an IPv4 advanced ACL number in the range of 3000 to 3999. If you specify an ACL, the device accepts and forwards only SA messages that the ACL permits. The device discards all SA messages when one of the following conditions exists:

- You do not specify an ACL.
- The specified ACL does not exist.
- The specified ACL does not have valid rules.

Usage guidelines

This command filters SA messages from a specified MSDP peer to control the acceptance or forwarding of SA messages. To control the creation of SA messages, use the **import-source** command.

When you configure a rule in the IPv4 advanced ACL, follow these restrictions and guidelines:

- For the rule to take effect, do not specify the **vpn-instance** *vpn-instance* option.
- The **source** *source-address source-wildcard* option specifies a multicast source address.
- The **destination** *dest-address dest-wildcard* option specifies a multicast group address.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

If you configure this command multiple times, the most recent configuration takes effect.

Examples

Configure an SA outgoing policy to forward only SA messages that ACL 3100 permits to MSDP peer 125.10.7.6.

```
<Switch> system-view
[Switch] acl advanced 3100
[Switch-acl-ipv4-adv-3100] rule permit ip source 170.15.0.0 0.0.255.255 destination
225.1.0.0 0.0.255.255
[Switch-acl-ipv4-adv-3100] quit
[Switch] msdp
[Switch-msdp] peer 125.10.7.6 connect-interface vlan-interface 100
[Switch-msdp] peer 125.10.7.6 sa-policy export acl 3100
```

Related commands

display msdp peer-status

import-source

6.1.16. peer sa-request-policy

Use **peer sa-request-policy** to configure an SA request policy for an MSDP peer.

Use **undo peer sa-request-policy** to delete the SA request policy for an MSDP peer.

Syntax

peer *peer-address* **sa-request-policy** [**acl** *ipv4-acl-number*]

undo peer *peer-address* **sa-request-policy**

Default

No SA request policy exists, and all SA request messages from an MSDP peer are accepted.

Views

MSDP view

Predefined user roles

network-admin

Parameters

peer-address: Specifies an MSDP peer by its IP address.

ipv4-acl-number: Specifies an IPv4 basic ACL number in the range of 2000 to 2999. If you specify an ACL, the device accepts only SA requests that the ACL permits. The device discards all SA requests when one of the following conditions exists:

- You do not specify an ACL.
- The specified ACL does not exist.
- The specified ACL does not have valid rules.

Usage guidelines

When you configure a rule in the IPv4 basic ACL, follow these restrictions and guidelines:

- For the rule to take effect, do not specify the **vpn-instance** *vpn-instance* option.
- The **source** *source-address source-wildcard* option specifies a multicast group address.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

If you configure this command multiple times, the most recent configuration takes effect.

Examples

Configure an SA request policy. Then, the device accepts only SA requests that are from MSDP peer 175.58.6.5 and for multicast groups in the range 225.1.1.0/24.

```
<Switch> system-view
[Switch] acl basic 2001
[Switch-acl-ipv4-basic-2001] rule permit source 225.1.1.0 0.0.0.255
[Switch-acl-ipv4-basic-2001] quit
[Switch] msdp
[Switch-msdp] peer 175.58.6.5 sa-request-policy acl 2001
```

6.1.17. reset msdp peer

Use **reset msdp peer** to reset the TCP connection with an MSDP peer and clear statistics for the MSDP peer.

Syntax

reset msdp peer [*peer-address*]

Views

User view

Predefined user roles

network-admin

Parameters

peer-address: Specifies an MSDP peer by its IP address. If you do not specify an MSDP peer, this command resets the TCP connections with all MSDP peers and clears statistics for all MSDP peers.

Examples

Reset the TCP connection with MSDP peer 125.10.7.6 and clear all statistics for the MSDP peer.

```
<Switch> reset msdp peer 125.10.7.6
```

6.1.18. reset msdp sa-cache

Use **reset msdp sa-cache** to clear (S, G) entries in the SA cache.

Syntax

reset msdp sa-cache [*group-address*]

Views

User view

Predefined user roles

network-admin

Parameters

group-address: Specifies a multicast group by its IP address in the range of 224.0.1.0 to 239.255.255.255. If you do not specify a multicast group, this command clears (S, G) entries for all multicast groups in the SA cache.

Examples

Clear (S, G) entries for multicast group 225.5.4.3 in the SA cache.

```
<Switch> reset msdp sa-cache 225.5.4.3
```

Related commands

cache-sa-enable

display msdp sa-cache

6.1.19. reset msdp statistics

Use **reset msdp statistics** to clear statistics for an MSDP peer without resetting the TCP connection with the MSDP peer.

Syntax

reset msdp statistics [*peer-address*]

Views

User view

Predefined user roles

network-admin

Parameters

peer-address: Specifies an MSDP peer by its IP address. If you do not specify an MSDP peer, this command clears statistics for all MSDP peers without resetting the TCP connection with all MSDP peers.

Examples

Clear statistics for MSDP peer 125.10.7.6 without resetting the TCP connection with the peer.

```
<Switch> reset msdp statistics 125.10.7.6
```

6.1.20. shutdown (MSDP view)

Use **shutdown** to tear down the connection with an MSDP peer.

Use **undo shutdown** to re-establish the connection with an MSDP peer.

Syntax

shutdown *peer-address*

undo shutdown *peer-address*

Default

The connection with an MSDP peer is active.

Views

MSDP view

Predefined user roles

network-admin

Parameters

peer-address: Specifies an MSDP peer by its IP address.

Examples

Tear down the connection with the MSDP peer 125.10.7.6.

```
<Switch> system-view
[Switch] msdp
[Switch-msdp] shutdown 125.10.7.6
```

Related commands

display msdp brief

display msdp peer-status

6.1.21. static-rpf-peer

Use **static-rpf-peer** to configure a static RPF peer.

Use **undo static-rpf-peer** to remove a static RPF peer.

Syntax

static-rpf-peer *peer-address* [**rp-policy** *ip-prefix-name*]

undo static-rpf-peer *peer-address*

Default

No static RPF peers exist.

Views

MSDP view

Predefined user roles

network-admin

Parameters

peer-address: Specifies an MSDP peer by its IP address.

rp-policy *ip-prefix-name*: Specifies a filtering policy based on RP addresses in SA messages by its name, a case-sensitive string of 1 to 63 characters. If you specify a filtering policy, the device does not perform RPF checks on SA messages permitted by the policy. If you do not specify a filtering policy, the device performs RPF checks on all SA messages.

Usage guidelines

This feature exempts SA messages forwarded by the static RPF peer from RPF checks.

Examples

Specify 130.10.7.6 as the static RPF peer to exempt SA messages originated by RPs on subnet 130.10.0.0/16 from RPF checks.

```
<Switch> system-view
[Switch] ip prefix-list list1 permit 130.10.0.0 16 greater-equal 16 less-equal 32
[Switch] msdp
[Switch-msdp] peer 130.10.7.6 connect-interface vlan-interface 100
[Switch-msdp] static-rpf-peer 130.10.7.6 rp-policy list1
```

Related commands

display msdp peer-status

ip prefix-list

6.1.22. timer retry

Use **timer retry** to set the MSDP connection retry interval.

Use **undo timer retry** to restore the default.

Syntax

timer retry *interval*

undo timer retry

Default

The MSDP connection retry interval is 30 seconds.

Views

MSDP view

Predefined user roles

network-admin

Parameters

interval: Specifies an MSDP connection retry interval in the range of 1 to 60 seconds.

Examples

Set the MSDP connection retry interval to 60 seconds.

```
<Switch> system-view
[Switch] msdp
[Switch-msdp] timer retry 60
```

Contents

A page of this section is **6-x-x**

7. MLD snooping commands ····· 7-1
7.1. MLD snooping commands ····· 7-1
7.1.1. display ipv6 l2-multicast ip ····· 7-1
7.1.2. display ipv6 l2-multicast ip forwarding ····· 7-3
7.1.3. display ipv6 l2-multicast mac ····· 7-4
7.1.4. display ipv6 l2-multicast mac forwarding ····· 7-6
7.1.5. display mld-snooping ····· 7-8
7.1.6. display mld-snooping group ····· 7-11
7.1.7. display mld-snooping router-port ····· 7-13
7.1.8. display mld-snooping static-group ····· 7-15
7.1.9. display mld-snooping static-router-port ····· 7-16
7.1.10. display mld-snooping statistics ····· 7-17
7.1.11. dot1p-priority (MLD-snooping view) ····· 7-18
7.1.12. enable (MLD-snooping view) ····· 7-19
7.1.13. entry-limit (MLD-snooping view) ····· 7-20
7.1.14. fast-leave (MLD-snooping view) ····· 7-20
7.1.15. group-policy (MLD-snooping view) ····· 7-21
7.1.16. host-aging-time (MLD-snooping view) ····· 7-22
7.1.17. last-listener-query-interval (MLD-snooping view) ····· 7-23
7.1.18. max-response-time (MLD-snooping view) ····· 7-24
7.1.19. mld-snooping ····· 7-25
7.1.20. mld-snooping done source-ip ····· 7-25
7.1.21. mld-snooping dot1p-priority ····· 7-26
7.1.22. mld-snooping drop-unknown ····· 7-27
7.1.23. mld-snooping enable ····· 7-28
7.1.24. mld-snooping fast-leave ····· 7-29
7.1.25. mld-snooping general-query source-ip ····· 7-30
7.1.26. mld-snooping group-limit ····· 7-31
7.1.27. mld-snooping group-policy ····· 7-32
7.1.28. mld-snooping host-aging-time ····· 7-33
7.1.29. mld-snooping host-join ····· 7-34
7.1.30. mld-snooping last-listener-query-interval ····· 7-35
7.1.31. mld-snooping max-response-time ····· 7-36
7.1.32. mld-snooping overflow-replace ····· 7-37
7.1.33. mld-snooping querier ····· 7-38
7.1.34. mld-snooping query-interval ····· 7-39
7.1.35. mld-snooping report source-ip ····· 7-40
7.1.36. mld-snooping router-aging-time ····· 7-41
7.1.37. mld-snooping source-deny ····· 7-42
7.1.38. mld-snooping special-query source-ip ····· 7-43
7.1.39. mld-snooping static-group ····· 7-44
7.1.40. mld-snooping static-router-port ····· 7-45
7.1.41. mld-snooping version ····· 7-46
7.1.42. overflow-replace (MLD-snooping view) ····· 7-47
7.1.43. report-aggregation (MLD-snooping view) ····· 7-47
7.1.44. reset mld-snooping group ····· 7-48
7.1.45. reset mld-snooping router-port ····· 7-49
7.1.46. reset mld-snooping statistics ····· 7-49
7.1.47. router-aging-time (MLD-snooping view) ····· 7-49
7.1.48. source-deny (MLD-snooping view) ····· 7-50
7.1.49. version (MLD-snooping view) ····· 7-51

7. MLD snooping commands

7.1. MLD snooping commands

7.1.1. display ipv6 l2-multicast ip

Use **display ipv6 l2-multicast ip** to display information about Layer 2 IPv6 multicast groups.

Syntax

display ipv6 l2-multicast ip [**group** *ipv6-group-address* | **source** *ipv6-source-address*] * [**vlan** *vlan-id* | **vsi** *vsi-name*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

group *ipv6-group-address*: Specifies an IPv6 multicast group by its IPv6 address. If you do not specify an IPv6 multicast group, this command displays information about all Layer 2 IPv6 multicast groups.

source *ipv6-source-address*: Specifies an IPv6 multicast source by its IPv6 address. If you do not specify an IPv6 multicast source, this command displays information about Layer 2 IPv6 multicast groups for all IPv6 multicast sources.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays information about Layer 2 IPv6 multicast groups for all VLANs.

vsi *vsi-name*: Specifies a VSI by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VSI, this command displays information about Layer 2 IPv6 multicast groups for all VSIs.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information about Layer 2 IP multicast groups for the master device.

Examples

Display information about Layer 2 IPv6 multicast groups for VLAN 2.

```
<Switch> display ipv6 l2-multicast ip vlan 2
Total 1 entries.

VLAN 2: Total 1 entries.
   (::, FF1E::101)
    Attribute: static, success
    Host ports (1 in total):
      GE1/0/1                                 (S, SUC)
```

Display information about Layer 2 IPv6 multicast groups for VSI **aaa**.

```
<Switch> display ipv6 l2-multicast ip vsi aaa
Total 1 entries.

VSI aaa: Total 1 entries.
  (::, FF1E::101)
    Attribute: dynamic, success
    Host ports (3 in total):
      GE1/0/3 (Link ID 0)                  (D, SUC)
      NPW (Link ID 8)                      (D, SUC)
      UPW (Link ID 9)                      (D, SUC)
```

Display information about Layer 2 IPv6 multicast groups for VSI **bbb**.

```
<Switch> display ipv6 l2-multicast ip vsi bbb
Total 1 entries.

VSI bbb: Total 1 entries.
  (::, FF1E::101)
    Attribute: dynamic, success
    Host ports (2 in total):
      GE1/0/3 (Link ID 0)                  (D, SUC)
      Tun0 (VXLAN ID 0)                    (D, SUC)
```

Table 7-1 Command output

Field	Description
Total 1 entries	Total number of Layer 2 IPv6 multicast groups.
VLAN 2: Total 1 entries	Total number of Layer 2 IPv6 multicast groups in VLAN 2.
VSI aaa: Total 1 entries	Total number of Layer 2 IPv6 multicast groups in VSI **aaa**.
(::, FF1E::101)	(S, G) entry, where a double colon (::) in the S position means all IPv6 multicast sources.
Attribute	Entry attribute: • **dynamic**—The entry is created by a dynamic protocol. • **static**—The entry is created by a static protocol. • **pim**—The entry is created by IPv6 PIM. • **kernel**—The entry is obtained from the kernel. • **success**—Processing has succeeded. • **fail**—Processing has failed.
Host ports (1 in total)	Member ports and total number of member ports.
(S, SUC)	Port attribute: • **D**—Dynamic port. • **S**—Static port. • **P**—IPv6 PIM port. • **K**—Port obtained from the kernel. • **R**—Port learned from (*, *) entries. • **W**—Port learned from (*, G) entries. • **SUC**—Processing has succeeded. • **F**—Processing has failed.
GE1/0/3 (Link ID 0)	AC and its link ID.

Field	Description
NPW (Link ID 8)	N-PW and its link ID.
UPW (Link ID 9)	U-PW and its link ID.
Tun0 (VXLAN ID 0)	VXLAN tunnel and its VXLAN ID.

7.1.2. display ipv6 l2-multicast ip forwarding

Use **display ipv6 l2-multicast ip forwarding** to display Layer 2 IPv6 multicast IP forwarding entries.

Syntax

display ipv6 l2-multicast ip forwarding [**group** *ipv6-group-address* | **source** *ipv6-source-address*] * [**vlan** *vlan-id* | **vsi** *vsi-name*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

group *ipv6-group-address*: Specifies an IPv6 multicast group by its IPv6 address. If you do not specify an IPv6 multicast group, this command displays Layer 2 IPv6 multicast IP forwarding entries for all IPv6 multicast groups.

source *ipv6-source-address*: Specifies an IPv6 multicast source by its IPv6 address. If you do not specify an IPv6 multicast source, this command displays Layer 2 IPv6 multicast IP forwarding entries for all IPv6 multicast sources.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays Layer 2 IPv6 multicast IP forwarding entries for all VLANs.

vsi *vsi-name*: Specifies a VSI by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VSI, this command displays Layer 2 IPv6 multicast IP forwarding entries for all VSIs.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays Layer 2 IPv6 multicast IP forwarding entries for the master device.

Examples

Display Layer 2 IPv6 multicast IP forwarding entries for VLAN 2.

```
<Switch> display ipv6 l2-multicast ip forwarding vlan 2
Total 1 entries.

VLAN 2: Total 1 entries.
   (::, FF1E::101)
    Host ports (3 in total):
      GigabitEthernet1/0/1
      GigabitEthernet1/0/2
      GigabitEthernet1/0/3
```

Display Layer 2 IPv6 multicast IP forwarding entries for VSI **aaa**.

```
<Switch> display ipv6 l2-multicast ip forwarding vsi aaa
Total 1 entries.

VSI aaa: Total 1 entries.
  (::, FF1E::101)
    Host ports (3 in total):
      GigabitEthernet1/0/3 (Link ID 0)
      NPW (Link ID 8)
      UPW (Link ID 9)
```

Display Layer 2 IPv6 multicast IP forwarding entries for VSI **bbb**.

```
<Switch> display ipv6 l2-multicast ip forwarding vsi bbb
Total 1 entries.

VSI bbb: Total 1 entries.
  (::, FF1E::101)
    Host ports (2 in total):
      GigabitEthernet1/0/3 (Link ID 0)
      Tunnel0 (VXLAN ID 0)
```

Table 7-2 Command output

Field	Description
Total 1 entries	Total number of Layer 2 IPv6 multicast IP forwarding entries.
VLAN 2: Total 1 entries	Total number of Layer 2 IPv6 multicast IP forwarding entries in VLAN 2.
VSI aaa: Total 1 entries	Total number of Layer 2 IPv6 multicast IP forwarding entries in VSI **aaa**.
(::, FF1E::101)	(S, G) entry, where a double colon (::) in the S position means all IPv6 multicast sources.
Host ports (3 in total)	Member ports and total number of member ports.
GigabitEthernet1/0/3 (Link ID 0)	AC and its link ID.
NPW (Link ID 8)	N-PW and its link ID.
UPW (Link ID 9)	U-PW and its link ID.
Tunnel0 (VXLAN ID 0)	VXLAN tunnel and its VXLAN ID.

7.1.3. display ipv6 l2-multicast mac

Use **display ipv6 l2-multicast mac** to display information about Layer 2 IPv6 multicast MAC multicast groups.

Syntax

display ipv6 l2-multicast mac [*mac-address*] [**vlan** *vlan-id* | **vsi** *vsi-name*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

mac-address: Specifies an IPv6 multicast MAC address. If you do not specify an IPv6 multicast MAC address, this command displays information about all Layer 2 IPv6 multicast MAC multicast groups.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays information about Layer 2 IPv6 multicast MAC multicast groups for all VLANs.

vsi *vsi-name*: Specifies a VSI by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VSI, this command displays information about Layer 2 IPv6 multicast MAC multicast groups for all VSIs.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information about Layer 2 IPv6 multicast MAC multicast groups for the master device.

Examples

Display information about Layer 2 IPv6 multicast MAC multicast groups for VLAN 2.

```
<Switch> display ipv6 l2-multicast mac vlan 2
Total 1 entries.

VLAN 2: Total 1 entries.
  MAC group address: 3333-0000-0101
    Attribute: success
    Host ports (1 in total):
      GE1/0/1
```

Display information about Layer 2 IPv6 MAC multicast groups for VSI **aaa**.

```
<Switch> display ipv6 l2-multicast mac vsi aaa
Total 1 MAC entries.

VSI aaa: Total 1 entries.
  MAC group address: 0100-5e01-0101
    Attribute: success
    Host ports (3 in total):
      GE1/0/3 ( Link ID 0)
      NPW (Link ID 8)
      UPW (Link ID 9)
```

Display information about Layer 2 IPv6 MAC multicast groups for VSI **bbb**.

```
<Switch> display ipv6 l2-multicast mac vsi bbb
Total 1 entries.

VSI bbb: Total 1 entries.
  MAC group address: 0100-5e01-0101
```

```
Attribute: success
Host ports (2 in total):
  GE1/0/3 ( Link ID 0)
  Tun0 (VXLAN ID 0)
```

Table 7-3 Command output

Field	Description
Total 1 entries	Total number of Layer 2 IPv6 MAC multicast groups.
VLAN 2: Total 1 entries	Total number of Layer 2 IPv6 MAC multicast groups in VLAN 2.
VSI aaa: Total 1 entries	Total number of Layer 2 IPv6 MAC multicast groups in VSI **aaa**.
MAC group address	IPv6 address of the Layer 2 IPv6 MAC multicast group.
Attribute	Entry attribute: • **success**—Processing has succeeded. • **fail**—Processing has failed.
Host ports (1 in total)	Member ports and total number of member ports.
GE1/0/3 (Link ID 0)	AC and its link ID.
NPW (Link ID 8)	N-PW and its link ID.
UPW (Link ID 9)	U-PW and its link ID.
Tun0 (VXLAN ID 0)	VXLAN tunnel and its VXLAN ID.

7.1.4. display ipv6 l2-multicast mac forwarding

Use **display ipv6 l2-multicast mac forwarding** to display Layer 2 IPv6 multicast MAC forwarding entries.

Syntax

display ipv6 l2-multicast mac forwarding [*mac-address*] [**vlan** *vlan-id* | **vsi** *vsi-name*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

mac-address: Specifies an IPv6 MAC multicast group by its IPv6 MAC address. If you do not specify an IPv6 MAC multicast group, this command displays Layer 2 IPv6 multicast MAC forwarding entries for all IPv6 MAC multicast groups.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays Layer 2 IPv6 multicast MAC forwarding entries for all VLANs.

vsi *vsi-name*: Specifies a VSI by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VSI, this command displays Layer 2 IPv6 multicast MAC forwarding entries for all VSIs.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays Layer 2 IPv6 multicast MAC forwarding entries for the master device.

Examples

Display Layer 2 IPv6 multicast MAC forwarding entries for VLAN 2.

```
<Switch> display ipv6 l2-multicast mac forwarding vlan 2
Total 1 entries.

VLAN 2: Total 1 entries.
  MAC group address: 3333-0000-0101
    Host ports (3 in total):
      GigabitEthernet1/0/1
      GigabitEthernet1/0/2
      GigabitEthernet1/0/3
```

Display Layer 2 IPv6 multicast MAC forwarding entries for VSI **aaa**.

```
<Switch> display ipv6 l2-multicast mac forwarding vsi aaa
Total 1 entries.

VSI aaa: Total 1 entries.
  MAC group address: 0100-5e01-0101
    Host ports (3 in total):
      GigabitEthernet1/0/3 (Link ID 0)
      NPW (Link ID 8)
      UPW (Link ID 9)
```

Display Layer 2 IPv6 multicast MAC forwarding entries for VSI **bbb**.

```
<Switch> display ipv6 l2-multicast mac forwarding vsi bbb
Total 1 entries.

VSI bbb: Total 1 entries.
  MAC group address: 0100-5e01-0101
    Host ports (2 in total):
      GigabitEthernet1/0/3 (Link ID 0)
      Tunnel0 (VXLAN ID 0)
```

Table 7-4 Command output

Field	Description
Total 1 MAC entries	Total number of Layer 2 IPv6 multicast MAC forwarding entries.
VLAN 2: Total 1 entries	Total number of Layer 2 IPv6 multicast MAC forwarding entries in VLAN 2.
VSI aaa: Total 1 entries	Total number of Layer 2 IPv6 multicast MAC forwarding entries in VSI **aaa**.
MAC group address	Address of the IPv6 MAC multicast group.
Host ports (3 in total)	Member ports, and the total number of member ports.
GigabitEthernet1/0/3 (Link ID 0)	AC and its link ID.

Field	Description
NPW (Link ID 8)	N-PW and its link ID.
UPW (Link ID 9)	U-PW and its link ID.
Tunnel0 (VXLAN ID 0)	VXLAN tunnel and its VXLAN ID.

7.1.5. display mld-snooping

Use **display mld-snooping** to display MLD snooping status.

Syntax

display mld-snooping [**global** | **vlan** *vlan-id* | **vsi** *vsi-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

global: Displays the global MLD snooping status.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094.

vsi *vsi-name*: Specifies a VSI by its name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

If you do not specify any parameters, this command displays the global MLD snooping status and the MLD snooping status in all VLANs and VSIs.

Examples

Display the global MLD snooping status and the MLD snooping status for all VLANs and VSIs.

```
<Switch> display mld-snooping
MLD snooping information: Global
  Global-enable: Enabled
 Host-aging-time: 260s
 Router-aging-time: 260s
 Max-response-time: 10s
 Last-listener-query-interval: 1s
 Report-aggregation: Enabled
 Host-tracking: Disabled
 Dot1p-priority: --

MLD snooping information: VLAN 1
 MLD snooping: Enabled
 Drop-unknown: Disabled
 Version: 1
 Host-aging-time: 260s
 Router-aging-time: 260s
 Max-response-time: 10s
```

```
 Last-listener-query-interval: 1s
 Querier: Enabled (IP: FE80::2FF:FFFF:FE00:1, Expires: 00:02:05)
 Querier-election: Enabled
 Query-interval: 125s
 General-query source IP: FE80::2FF:FFFF:FE00:1
 Special-query source IP: FE80::2FF:FFFF:FE00:1
 Report source IP: FE80::2FF:FFFF:FE00:2
 Done source IP: FE80::2FF:FFFF:FE00:3
 Host-tracking: Disabled
 Dot1p-priority: 2
 Proxy: Disabled

MLD snooping information: VLAN 10
 MLD snooping: Enabled
 Drop-unknown: Enabled
 Version: 1
 Host-aging-time: 260s
 Router-aging-time: 260s
 Max-response-time: 10s
 Last-listener-query-interval: 1s
 Querier: Enabled (IP: FE80::2FF:FFFF:FE00:1, Expires: 00:02:05)
 Querier-election: Enabled
 Query-interval: 125s
 General-query source IP: FE80::2FF:FFFF:FE00:1
 Special-query source IP: FE80::2FF:FFFF:FE00:1
 Report source IP: FE80::2FF:FFFF:FE00:2
 Done source IP: FE80::2FF:FFFF:FE00:3
 Host-tracking: Disabled
 Dot1p-priority: --
 Proxy: Disabled

MLD snooping information: VSI aaa
 MLD snooping: Enabled
 Drop-unknown: Enabled
 Version: 1
 Host-aging-time: 260s
 Router-aging-time: 260s
 Max-response-time: 10s
 Last-listener-query-interval: 1s
 Querier: Disabled
 Querier-election: Disabled
 Query-interval: 125s
 General-query source IP: FE80::2FF:FFFF:FE00:1
 Special-query source IP: FE80::2FF:FFFF:FE00:1
```

Table 7-5 Command output

Field	Description
MLD snooping	MLD snooping status in a VLAN or VSI: • **Enabled**. • **Disabled**.
Drop-unknown	Status of dropping unknown IPv6 multicast data: • Enabled. • Disabled.
Version	MLD snooping version.
Host-aging-time	Aging timer for the dynamic member port.
Router-aging-time	Aging timer for the dynamic router port.
Max-response-time	Maximum time for responding to MLD general queries.
Last-listener-query-interval	Interval for sending MLD multicast-address-specific queries.
Report-aggregation	Status of MLD report suppression: • Enabled. • Disabled.
Dot1p-priority	802.1p priority for MLD messages. This field displays two hyphens (--) if the 802.1p priority is not configured.
Querier	Status of MLD snooping querier: • Enabled. • Disabled.
(IP: FE80::2FF:FFFF:FE00:1, Expires: 00:02:05)	MLD snooping querier information: • **IP**—IP address of the MLD snooping querier. • **Expire**—Remaining aging time for the MLD snooping querier. This field is not displayed if MLD snooping querier election is disabled.
Querier-election	Status of IGMP snooping querier election: • Enabled. • Disabled.
Query-interval	Interval for sending MLD general queries.
General-query source IP	Source IPv6 address of MLD general queries.
Special-query source IP	Source IPv6 address of MLD multicast-address-specific queries.
Report source IP	Source IPv6 address of MLD reports.
Done source IP	Source IPv6 address of MLD done messages.
Host-tracking	Status of host tracking: • Enabled. • Disabled.
Proxy	Status of MLD snooping proxying: • Enabled. • Disabled.

7.1.6. display mld-snooping group

Use **display mld-snooping group** to display information about dynamic MLD snooping group entries.

Syntax

display mld-snooping group [*ipv6-group-address* | *ipv6-source-address*] * [**vlan** *vlan-id* | **vsi** *vsi-name*] [**verbose**] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ipv6-group-address: Specifies an IPv6 multicast group address. The value range for this argument is FFxy::/16 (excluding FFx1::/16 and FFx2::/16), where "x" and "y" represent any hexadecimal numbers in the range of 0 to F. If you do not specify an IPv6 multicast group, this command displays information about all dynamic MLD snooping group entries.

ipv6-source-address: Specifies an IPv6 multicast source by its IPv6 address. If you do not specify an IPv6 multicast source, this command displays information about dynamic MLD snooping group entries for all IPv6 multicast sources.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays information about dynamic MLD snooping group entries for all VLANs.

vsi *vsi-name*: Specifies a VSI by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VSI, this command displays information about dynamic MLD snooping group entries for all VSIs.

verbose: Displays detailed information about dynamic MLD snooping group entries. If you do not specify this keyword, the command displays brief information about dynamic MLD snooping group entries.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information about dynamic MLD snooping group entries for the master device.

Examples

Display detailed information about dynamic MLD snooping group entries for VLAN 2.

```
<Switch> display mld-snooping group vlan 2 verbose
Total 1 entries.

VLAN 2: Total 1 entries.
  (::,FF1E::101)
    Attribute: local port
    FSM information: dummy
    Host slots (0 in total):
    Host ports (1 in total):
      GE1/0/2                          (00:03:23)
```

Display brief information about dynamic MLD snooping group entries for VSI **aaa**.

```
<Switch> display mld-snooping group vsi aaa
```

```
Total 1 entries.
VSI aaa: Total 1 entries.
  (::,FF1E::101)
    Host ports (1 in total):
      GE1/0/3 (Link ID 1)                (00:03:35)
      NPW (Link ID 8)                    (00:02:35)
      UPW (Link ID 9)                    (00:01:35)
```

Display detailed information about dynamic MLD snooping group entries for VSI **bbb**.

```
<Switch> display mld-snooping group vsi bbb verbose
Total 1 entries.

VSI bbb: Total 1 entries.
  (::,FF1E::101)
    Attribute: global port
    FSM information: dummy
    Host slots (0 in total):
    Host ports (2 in total):
      GE1/0/3 (Link ID 0)                          (00:03:35)
        VLAN pairs (1 in total):
          Outer VLAN 5     Inner VLAN 2            (00:03:35)
      Tun0 (VXLAN ID 0)                            (00:03:35)
        VLAN pairs (1 in total):
          Outer VLAN 5     Inner VLAN 2            (00:03:35)
```

Table 7-6 Command output

Field	Description
Total 1 entries	Total number of dynamic MLD snooping group entries.
VLAN 2: Total 1 entries	Total number of dynamic MLD snooping group entries in VLAN 2.
VSI aaa: Total 1 entries	Total number of dynamic MLD snooping group entries in VSI **aaa**.
(::, FF1E::101)	(S, G) entry, where a double colon (::) in the S position means all IPv6 multicast sources.
Attribute	Entry attribute: • **global port**—The entry has a global port. • **local port**—The entry has a port that resides on the member device for which the information is displayed. • **slot**—The entry has ports that reside on other member devices, but not on the member device for which the information is displayed.
FSM information	Finite state machine information of the entry: • **delete**—The entry attributes have been deleted. • **dummy**—The entry is a new temporary entry. • **no info**—The entry does not exist.
Host slots (0 in total)	Member IDs and total number of the member devices that have member ports, except for the specified member device or the master device when no member device is specified.
Host ports (1 in total)	Member ports and total number of member ports.

Field	Description
(00:03:23)	Remaining aging time for the dynamic member port. This field is always displayed for a global port (such as Layer 2 aggregate interfaces, ACs, N-PWs, and U-PWs). For a non-global port, this field is displayed when one of the following conditions exists: • The port is on the specified member device. • The port is on the master device and no member device is specified.
GE1/0/3 (Link ID 0)	AC and its link ID.
NPW (Link ID 8)	N-PW and its link ID.
UPW (Link ID 9)	U-PW and its link ID.
Tun0 (VXLAN ID 0)	VXLAN tunnel and its VXLAN ID.
VLAN pairs (1 in total)	VLAN pairs and total number of VLAN pairs.
Outer VLAN 5 Inner VLAN 2	Outer VLAN ID and inner VLAN ID.

Related commands

reset mld-snooping group

7.1.7. display mld-snooping router-port

Use **display mld-snooping router-port** to display dynamic router port information.

Syntax

display mld-snooping router-port [**vlan** *vlan-id* | **vsi** *vsi-name*] [**verbose**] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

verbose: Displays detailed information about dynamic router ports. If you do not specify this keyword, the command displays brief information about dynamic router ports.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays dynamic router port information for all VLANs.

vsi *vsi-name*: Specifies a VSI by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VSI, this command displays dynamic router port information for all VSIs.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays dynamic router port information for the master device.

Examples

Display brief information about dynamic router ports for VLAN 2.

```
<Switch> display mld-snooping router-port vlan 2
```

```
VLAN 2:
  Router ports (2 in total):
    GE1/0/1                                (00:01:30)
    GE1/0/2                                (00:00:23)
```

Display detailed information about dynamic router ports for VSI **aaa**.

```
<Switch> display mld-snooping router-port vsi aaa verbose
VSI aaa:
  Router slots (0 in total):
  Router ports (3 in total):
    GE1/0/3 (Link ID 0)                                (00:03:35)
      VLAN pairs (1 in total):
        Outer VLAN 5     Inner VLAN 2                  (00:03:35)
    NPW (Link ID 8)                                    (00:03:35)
      VLAN pairs (1 in total):
        Outer VLAN 5     Inner VLAN 2                  (00:03:35)
    UPW (Link ID 9)                                    (00:03:35)
      VLAN pairs (1 in total):
        Outer VLAN 5     Inner VLAN 2                  (00:03:35)
```

Display detailed information about dynamic router ports for VSI **bbb**.

```
<Switch> display mld-snooping router-port vsi bbb verbose
VSI bbb:
  Router slots (0 in total):
  Router ports (2 in total):
    GE1/0/3 (Link ID 0)                                (00:03:35)
      VLAN pairs (1 in total):
        Outer VLAN 5     Inner VLAN 2                  (00:03:35)
    Tun0 (VXLAN ID 0)                                  (00:03:35)
      VLAN pairs (1 in total)
        Outer VLAN 5     Inner VLAN 2                  (00:03:35)
```

Table 7-7 Command output

Field	Description
VLAN 2	VLAN ID.
VSI aaa	VSI name.
Router slots (0 in total)	Member IDs and total number of the member devices that have dynamic router ports, except for the specified member device or the master device when no member device is specified.
Router ports (2 in total)	Dynamic router ports and total number of dynamic router ports.
(00:01:30)	Remaining aging time for the dynamic router port. This field is always displayed for a global port (including Layer 2 aggregate interfaces). For a non-global port, this field is displayed when one of the following conditions exists: • The port is on the specified member device. • The port is on the master device and no member device is specified.
GE1/0/3 (Link ID 0)	AC and its link ID.

Field	Description
NPW (Link ID 8)	N-PW and its link ID.
UPW (Link ID 9)	U-PW and its link ID.
Tun0 (VXLAN ID 0)	Name of the VXLAN tunnel and the VXLAN ID.
VLAN pairs (1 in total)	VLAN pairs and total number of VLAN pairs.
Outer VLAN 5 Inner VLAN 2	Outer VLAN ID and inner VLAN ID.

Related commands

reset mld-snooping router-port

7.1.8. display mld-snooping static-group

Use **display mld-snooping static-group** to display information about static MLD snooping group entries.

Syntax

display mld-snooping static-group [*ipv6-group-address* | *ipv6-source-address*] * [**vlan** *vlan-id*] [**verbose**] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ipv6-group-address: Specifies an IPv6 multicast group by its IPv6 address. The value range for this argument is FFxy::/16 (excluding FFx1::/16 and FFx2::/16), where "x" and "y" represent any hexadecimal numbers in the range of 0 to F. If you do not specify an IPv6 multicast group, this command displays information about static MLD snooping group entries for all IPv6 multicast groups.

ipv6-source-address: Specifies an IPv6 multicast source by its IPv6 address. If you do not specify an IPv6 multicast source, this command displays information about static MLD snooping group entries for all IPv6 multicast sources.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays information about static MLD snooping group entries for all VLANs.

verbose: Displays detailed information. If you do not specify this keyword, the command displays brief information.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information about static MLD snooping group entries for the master device.

Examples

Display detailed information about static MLD snooping group entries for VLAN 2.

```
<Switch> display mld-snooping static-group vlan 2 verbose
Total 1 entries.
```

```
VLAN 2: Total 1 entries.
  (::,FF1E::101)
    Attribute: local port
    FSM information: dummy
    Host slots (0 in total):
    Host ports (1 in total):
      GE1/0/2
```

Table 7-8 Command output

Field	Description
Total 1 entries	Total number of static MLD snooping group entries.
VLAN 2: Total 1 entries	Total number of static MLD snooping group entries in VLAN 2.
(::, FF1E::101)	(S, G) entry, where a double colon (::) in the S position means all IPv6 multicast sources.
Attribute	Entry attribute: • **global port**—The entry has a global port. • **local port**—The entry has a port that resides on the member device for which the information is displayed. • **slot**—The entry has ports that reside on other member devices, but not on the member device for which the information is displayed.
FSM information	Finite state machine information of the entry: • **delete**—The entry attributes have been deleted. • **dummy**—The entry is a new temporary entry. • **no info**—The entry does not exist.
Host slots (0 in total)	Member IDs and total number of the member devices that have member ports, except for the specified member device or the master device when no member device is specified.
Host ports (1 in total)	Member ports and total number of member ports.

7.1.9. display mld-snooping static-router-port

Use **display mld-snooping static-router-port** to display static router port information.

Syntax

display mld-snooping static-router-port [**vlan** *vlan-id*] [**verbose**] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094.

verbose: Displays detailed information about static router ports. If you do not specify this keyword, the command displays brief information about static router ports.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays static router port information for the master device.

Examples

Display brief information about static router ports for VLAN 2.

```
<Switch> display mld-snooping static-router-port vlan 2
VLAN 2:
  Router ports (2 in total):
    GE1/0/1
    GE1/0/2
```

Display detailed information about static router ports for VLAN 2.

```
<Switch> display mld-snooping static-router-port vlan 2 verbose
VLAN 2:
  Router slots (0 in total):
  Router ports (2 in total):
    GE1/0/1
    GE1/0/2
```

Table 7-9 Command output

Field	Description
VLAN 2	VLAN ID.
Router slots (0 in total)	Member IDs and total number of the member devices that have static router ports, except for the specified member device or the master device when no member device is specified.
Router ports (2 in total)	Static router ports and total number of static router ports.

7.1.10. display mld-snooping statistics

Use **display mld-snooping statistics** to display statistics for the MLD messages and IPv6 PIM hello messages learned through MLD snooping.

Syntax

display mld-snooping statistics

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display statistics for the MLD messages and IPv6 PIM hello messages learned through MLD snooping.

```
<Switch> display mld-snooping statistics
Received MLD general queries:  0
```

```
Received MLDv1 specific queries:  0
Received MLDv1 reports:  0
Received MLD dones:  0
Sent     MLDv1 specific queries:  0
Received MLDv2 reports:  0
Received MLDv2 reports with right and wrong records:  0
Received MLDv2 specific queries:  0
Received MLDv2 specific sg queries:  0
Sent     MLDv2 specific queries:  0
Sent     MLDv2 specific sg queries:  0
Received IPv6 PIM hello:  0
Received error MLD messages:  0
```

Table 7-10 Command output

Field	Description
general queries	Number of MLD general queries.
specific queries	Number of MLD multicast-address-specific queries.
reports	Number of MLD reports.
dones	Number of MLD done messages.
reports with right and wrong records	Number of MLD reports with correct and incorrect records.
specific sg queries	Number of MLD multicast-address-and-source-specific queries.
IPv6 PIM hello	Number of IPv6 PIM hello messages.
error MLD messages	Number of MLD messages with errors.

Related commands

reset mld-snooping statistics

7.1.11. dot1p-priority (MLD-snooping view)

Use **dot1p-priority** to set the 802.1p priority for MLD messages globally.

Use **undo dot1p-priority** to restore the default.

Syntax

dot1p-priority *priority*

undo dot1p-priority

Default

The 802.1p priority for MLD messages is not configured. For MLD messages created by the device, the 802.1p priority is 0. For MLD messages to be forwarded, the device does not change the 802.1p priority.

Views

MLD-snooping view

Predefined user roles

network-admin

Parameters

priority: Specifies an 802.1p priority for MLD messages, in the range of 0 to 7. The greater the value, the higher the priority.

Usage guidelines

You can set the 802.1p priority globally for all VLANs and VSIs in MLD-snooping view or for a VLAN in VLAN view. For a VLAN, the VLAN-specific configuration takes priority over the global configuration.

Examples

Set the 802.1p priority for MLD messages to 3 globally.

```
<Switch> system-view
[Switch] mld-snooping
[Switch-mld-snooping] dot1p-priority 3
```

Related commands

mld-snooping dot1p-priority

7.1.12. enable (MLD-snooping view)

Use **enable** to enable MLD snooping for VLANs.

Use **undo enable** to disable MLD snooping for VLANs.

Syntax

enable vlan *vlan-list*

undo enable vlan *vlan-list*

Default

MLD snooping is disabled in a VLAN.

Views

MLD-snooping view

Predefined user roles

network-admin

Parameters

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The VLAN ID is in the range of 1 to 4094.

Usage guidelines

You must enable the MLD snooping feature by using the **mld-snooping** command before you enable MLD snooping for VLANs.

You can enable MLD snooping for multiple VLANs by using this command in MLD-snooping view or for a VLAN by using the **mld-snooping enable** command in VLAN view. The configuration in VLAN view has the same priority as the configuration in MLD-snooping view, and the most recent configuration takes effect.

Examples

Enable the MLD snooping feature, and then enable MLD snooping for VLAN 2 through VLAN 10.

```
<Switch> system-view
[Switch] mld-snooping
[Switch-mld-snooping] enable vlan 2 to 10
```

Related commands

mld-snooping

mld-snooping enable

7.1.13. entry-limit (MLD-snooping view)

Use **entry-limit** to globally set the maximum number of MLD snooping forwarding entries, including dynamic entries and static entries.

Use **undo entry-limit** to restore the default.

Syntax

entry-limit *limit*

undo entry-limit

Default

The maximum number of MLD snooping forwarding entries is 4294967295.

Views

MLD-snooping view

Predefined user roles

network-admin

Parameters

limit: Specifies the maximum number of MLD snooping forwarding entries, in the range of 0 to 4294967295.

Examples

Set the global maximum number of MLD snooping forwarding entries to 512.

```
<Switch> system-view
[Switch] mld-snooping
[Switch-mld-snooping] entry-limit 512
```

7.1.14. fast-leave (MLD-snooping view)

Use **fast-leave** to enable fast-leave processing globally.

Use **undo fast-leave** to disable fast-leave processing globally.

Syntax

fast-leave [**vlan** *vlan-list*]

undo fast-leave [**vlan** *vlan-list*]

Default

Fast-leave processing is disabled.

Views

MLD-snooping view

Predefined user roles

network-admin

Parameters

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The VLAN ID is in the range of 1 to 4094. If you do not specify a VLAN, this command takes effect for all VLANs and VSIs.

Usage guidelines

The fast-leave processing feature enables the device to immediately remove a port from the forwarding entry for an IPv6 multicast group when the port receives a done message.

You can enable fast-leave processing globally for all ports in MLD-snooping view or for a port in interface view. For a port, the port-specific configuration takes priority over the global configuration.

Examples

Globally enable MLD snooping fast-leave processing for VLAN 2.

```
<Switch> system-view
[Switch] mld-snooping
[Switch-mld-snooping] fast-leave vlan 2
```

Related commands

mld-snooping fast-leave

7.1.15. group-policy (MLD-snooping view)

Use **group-policy** to globally configure an IPv6 multicast group policy to control the IPv6 multicast groups that hosts can join.

Use **undo group-policy** to globally delete IPv6 multicast group policies.

Syntax

group-policy *ipv6-acl-number* [**vlan** *vlan-list*]

undo group-policy [**vlan** *vlan-list*]

Default

No IPv6 multicast group policies exist. Hosts can join any IPv6 multicast groups.

Views

MLD-snooping view

Predefined user roles

network-admin

Parameters

ipv6-acl-number: Specifies an IPv6 basic or advanced ACL by its number in the range of 2000 to 3999. Hosts can join only IPv6 multicast groups that the ACL permits. If the ACL does not exist or does not have valid rules, hosts cannot join IPv6 multicast groups.

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The VLAN

ID is in the range of 1 to 4094. If you do not specify a VLAN, this command takes effect for all VLANs and VSIs.

Usage guidelines

An IPv6 multicast group policy filters MLD reports to control the IPv6 multicast groups that hosts can join.

This command does not take effect on static member ports, because static member ports do not send MLD reports.

You can configure an IPv6 multicast group policy globally for all ports in MLD-snooping view or for a port in interface view. For a port, the port-specific configuration takes priority over the global configuration.

When you configure a rule in the IPv6 ACL, follow these restrictions and guidelines:

- For the rule to take effect, do not specify the **vpn-instance** *vpn-instance* option.
- In a basic ACL, the **source** *source-address source-prefix* option specifies an IPv6 multicast group address.
- In an advanced ACL, the **source** *source-address source-prefix* option specifies an IPv6 multicast source address. The **destination** *dest-address dest-prefix* option specifies an IPv6 multicast group address.

  To match MLDv1 reports and MLDv2 IS_EX and MLDv2 TO_EX reports that do not carry IPv6 multicast source addresses, set the **source** *source-address source-prefix* option to 0::0.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

You can configure different ACLs for all ports in different VLANs. If you configure multiple ACLs for all ports in the same VLAN, the most recent configuration takes effect.

Examples

Configure an IPv6 multicast group policy for VLAN 2 so that hosts in VLAN 2 can join only IPv6 multicast group FF03::101.

```
<Switch> system-view
[Switch] acl ipv6 basic 2000
[Switch-acl-ipv6-basic-2000] rule permit source ff03::101 128
[Switch-acl-ipv6-basic-2000] quit
[Switch] mld-snooping
[Switch-mld-snooping] group-policy 2000 vlan 2
```

Related commands

mld-snooping group-policy

7.1.16. host-aging-time (MLD-snooping view)

Use **host-aging-time** to set the aging timer for dynamic member ports globally.

Use **undo host-aging-time** to restore the default.

Syntax

host-aging-time *seconds*

undo host-aging-time

Default

The aging timer for dynamic member ports is 260 seconds.

Views

MLD-snooping view

Predefined user roles

network-admin

Parameters

seconds: Specifies an aging timer for dynamic member ports, in the range of 1 to 8097894 seconds.

Usage guidelines

You can set the timer globally for all VLANs and VSIs in MLD-snooping view, for a VSI in VSI view, or for a VLAN in VLAN view. For a VSI, the VSI-specific configuration takes priority over the global configuration. For a VLAN, the VLAN-specific configuration takes priority over the global configuration.

To avoid mistakenly deleting IPv6 multicast group members, set the aging timer for dynamic member ports to be greater than the value calculated by using the following formula:

[MLD general query interval] + [maximum response time for MLD general queries]

As a best practice, set the aging timer of dynamic member ports to the value calculated by using the following formula:

[MLD general query interval] × 2 + [maximum response time for MLD general queries]

Examples

Set the global aging timer for dynamic member ports to 300 seconds.

```
<Switch> system-view
[Switch] mld-snooping
[Switch-mld-snooping] host-aging-time 300
```

Related commands

mld-snooping host-aging-time

7.1.17. last-listener-query-interval (MLD-snooping view)

Use **last-listener-query-interval** to set the MLD last listener query interval globally.

Use **undo last-listener-query-interval** to restore the default.

Syntax

last-listener-query-interval *interval*

undo last-listener-query-interval

Default

The MLD last listener query interval is 1 second.

Views

MLD-snooping view

Predefined user roles

network-admin

Parameters

interval: Specifies an MLD last listener query interval in the range of 1 to 25 seconds.

Usage guidelines

You can set the interval for a VLAN in VLAN view, for a VSI in VSI view, or globally for all VLANs and VSIs in MLD-snooping view. For a VLAN, the VLAN-specific configuration takes priority over the global configuration. For a VSI, the VSI-specific configuration takes priority over the global configuration.

Examples

Set the global MLD last listener query interval to 3 seconds.

```
<Switch> system-view
[Switch] mld-snooping
[Switch-mld-snooping] last-listener-query-interval 3
```

Related commands

mld-snooping last-listener-query-interval

7.1.18. max-response-time (MLD-snooping view)

Use **max-response-time** to set the maximum response time for MLD general queries globally.

Use **undo max-response-time** to restore the default.

Syntax

max-response-time *seconds*

undo max-response-time

Default

The maximum response time for MLD general queries is 10 seconds.

Views

MLD-snooping view

Predefined user roles

network-admin

Parameters

seconds: Specifies the maximum response time for MLD general queries, in the range of 1 to 3174 seconds.

Usage guidelines

You can set the time globally for all VLANs and VSIs in MLD-snooping view, for a VSI in VSI view, or for a VLAN in VLAN view. For a VSI, the VSI-specific configuration takes priority over the global configuration. For a VLAN, the VLAN-specific configuration takes priority over the global configuration.

To avoid mistakenly deleting IPv6 multicast group members, set the maximum response time for MLD general queries to be less than the MLD general query interval.

Examples

Set the global maximum response time for MLD general queries to 5 seconds.

```
<Switch> system-view
[Switch] mld-snooping
```

```
[Switch-mld-snooping] max-response-time 5
```

Related commands

mld-snooping max-response-time

mld-snooping query-interval

7.1.19. mld-snooping

Use **mld-snooping** to enable the MLD snooping feature and enter MLD-snooping view.

Use **undo mld-snooping** to disable the MLD snooping feature.

Syntax

mld-snooping

undo mld-snooping

Default

The MLD snooping feature is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

If you disable the MLD snooping feature, MLD snooping is disabled in all VLANs and VSIs.

Examples

Enable the MLD snooping feature and enter MLD-snooping view.

```
<Switch> system-view
[Switch] mld-snooping
[Switch-mld-snooping]
```

Related commands

enable (MLD-snooping view)

mld-snooping enable

7.1.20. mld-snooping done source-ip

Use **mld-snooping done source-ip** to configure the source IPv6 address for MLD done messages.

Use **undo mld-snooping done source-ip** to restore the default.

Syntax

mld-snooping done source-ip *ipv6-address*

undo mld-snooping done source-ip

Default

In a VLAN, the source IPv6 address of MLD done messages is the IPv6 link-local address of the current VLAN interface. If the current VLAN interface does not have an IPv6 link-local address, the source IPv6 address is FE80::02FF:FFFF:FE00:0001.

In a VSI, the source IPv6 address of MLD done messages is the IPv6 link-local address of the gateway interface for the VSI. If the gateway interface does not have an IPv6 link-local address, the source IPv6 address is FE80::02FF:FFFF:FE00:0001.

Views

VLAN view

VSI view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies the source IPv6 address for MLD done messages.

Usage guidelines

You must enable MLD snooping for a VLAN before you execute this command.

Examples

In VLAN 2, enable MLD snooping, and specify FE80:0:0:1::1 as the source IPv6 address of MLD done messages.

```
<Switch> system-view
[Switch] mld-snooping
[Switch-mld-snooping] quit
[Switch] vlan 2
[Switch-vlan2] mld-snooping enable
[Switch-vlan2] mld-snooping done source-ip fe80:0:0:1::1
```

In VSI **aaa**, enable MLD snooping, and specify FE80:0:0:1::1 as the source IPv6 address of MLD done messages.

```
<Switch> system-view
[Switch] mld-snooping
[Switch-mld-snooping] quit
[Switch] vsi aaa
[Switch-vsi-aaa] mld-snooping enable
[Switch-vsi-aaa] mld-snooping done source-ip fe80:0:0:1::1
```

Related commands

enable (MLD-snooping view)

mld-snooping enable

7.1.21. mld-snooping dot1p-priority

Use **mld-snooping dot1p-priority** to set the 802.1p priority for MLD messages in a VLAN.

Use **undo mld-snooping dot1p-priority** to restore the default.

Syntax

mld-snooping dot1p-priority *priority*

undo mld-snooping dot1p-priority

Default

The 802.1p priority for MLD messages is not configured. For MLD messages created by the device, the 802.1p priority is 0. For MLD messages to be forwarded, the device does not change the 802.1p priority.

Views

VLAN view

Predefined user roles

network-admin

Parameters

priority: Specifies an 802.1p priority for MLD messages, in the range of 0 to 7. The greater the value, the higher the priority.

Usage guidelines

You must enable MLD snooping for a VLAN before you execute this command.

You can set the 802.1p priority for a VLAN in VLAN view or globally for all VLANs in MLD-snooping view. For a VLAN, the VLAN-specific configuration takes priority over the global configuration.

Examples

In VLAN 2, enable MLD snooping, and set the 802.1p priority for MLD messages to 3.

```
<Switch> system-view
[Switch] mld-snooping
[Switch-mld-snooping] quit
[Switch] vlan 2
[Switch-vlan2] mld-snooping enable
[Switch-vlan2] mld-snooping dot1p-priority 3
```

Related commands

dot1p-priority (MLD-snooping view)

enable (MLD-snooping view)

mld-snooping enable

7.1.22. mld-snooping drop-unknown

Use **mld-snooping drop-unknown** to enable dropping unknown IPv6 multicast data packets for a VLAN or VSI.

Use **undo mld-snooping drop-unknown** to disable dropping unknown IPv6 multicast data packets for a VLAN or VSI.

Syntax

mld-snooping drop-unknown

undo mld-snooping drop-unknown

Default

Dropping unknown IPv6 multicast data packets is disabled. Unknown IPv6 multicast data packets are flooded.

Views

VLAN view

VSI view

Predefined user roles

network-admin

Usage guidelines

You must enable MLD snooping for a VLAN or VSI before you execute this command.

Examples

In VLAN 2, enable MLD snooping, and enable dropping unknown IPv6 multicast data packets.

```
<Switch> system-view
[Switch] mld-snooping
[Switch-mld-snooping] quit
[Switch] vlan 2
[Switch-vlan2] mld-snooping enable
[Switch-vlan2] mld-snooping drop-unknown
```

In VSI **aaa**, enable MLD snooping, and enable dropping unknown IPv6 multicast data packets.

```
<Switch> system-view
[Switch] mld-snooping
[Switch-mld-snooping] quit
[Switch] vsi aaa
[Switch-vsi-aaa] mld-snooping enable
[Switch-vsi-aaa] mld-snooping drop-unknown
```

Related commands

enable (MLD-snooping view)

mld-snooping enable

7.1.23. mld-snooping enable

Use **mld-snooping enable** to enable MLD snooping for a VLAN or VSI.

Use **undo mld-snooping** to disable MLD snooping status for a VLAN or VSI.

Syntax

mld-snooping enable

undo mld-snooping

Default

MLD snooping is disabled for a VLAN or VSI.

Views

VLAN view

VSI view

Predefined user roles

network-admin

Usage guidelines

You must enable the MLD snooping feature by using the **mld-snooping** command before you enable MLD snooping for a VLAN or VSI.

You can enable MLD snooping for a VLAN by using this command in VLAN view or for multiple VLANs by using the **enable** command. The configuration in VLAN view has the same priority as the configuration in MLD-snooping view, and the most recent configuration takes effect.

Examples

Enable the MLD snooping feature, and then enable MLD snooping for VLAN 2.

```
<Switch> system-view
[Switch] mld-snooping
[Switch-mld-snooping] quit
[Switch] vlan 2
[Switch-vlan2] mld-snooping enable
```

Enable the MLD snooping feature, and then enable MLD snooping for VSI **aaa**.

```
<Switch> system-view
[Switch] mld-snooping
[Switch-mld-snooping] quit
[Switch] vsi aaa
[Switch-vsi-aaa] mld-snooping enable
```

Related commands

enable (MLD-snooping view)

mld-snooping

7.1.24. mld-snooping fast-leave

Use **mld-snooping fast-leave** to enable fast-leave processing on a port.

Use **undo mld-snooping fast-leave** to disable fast-leave processing on a port.

Syntax

mld-snooping fast-leave [**vlan** *vlan-list*]

undo mld-snooping fast-leave [**vlan** *vlan-list*]

Default

Fast-leave processing is disabled on a port.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The VLAN ID is in the range of 1 to 4094. If you do not specify a VLAN, this command takes effect on all VLANs.

Usage guidelines

The fast-leave processing feature enables the device to immediately remove a port from the forwarding entry for an IPv6 multicast group when the port receives a done message.

You can enable fast-leave processing for a port in interface view or globally for all ports in MLD-snooping view. For a port, the port-specific configuration takes priority over the global configuration.

Examples

Enable fast-leave processing for VLAN 2 on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] mld-snooping fast-leave vlan 2
```

Related commands

fast-leave (MLD-snooping view)

7.1.25. mld-snooping general-query source-ip

Use **mld-snooping general-query source-ip** to configure the source IPv6 address for MLD general queries.

Use **undo mld-snooping general-query source-ip** to restore the default.

Syntax

mld-snooping general-query source-ip *ipv6-address*

undo mld-snooping general-query source-ip

Default

In a VLAN, the source IPv6 address for MLD general queries is the IPv6 link-local address of the current VLAN interface. If the current VLAN interface does not have an IPv6 link-local address, the source IPv6 address is FE80::02FF:FFFF:FE00:0001.

In a VSI, the source IPv6 address for MLD general queries is the IPv6 link-local address of the gateway interface for the VSI. If the gateway interface does not have an IPv6 link-local address, the source IPv6 address is FE80::02FF:FFFF:FE00:0001.

Views

VLAN view

VSI view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies the source IPv6 address for MLD general queries.

Usage guidelines

You must enable MLD snooping for a VLAN or VSI before you execute this command.

Examples

In VLAN 2, enable MLD snooping, and specify FE80:0:0:1::1 as the source IPv6 address for MLD general queries.

```
<Switch> system-view
[Switch] mld-snooping
[Switch-mld-snooping] quit
[Switch] vlan 2
[Switch-vlan2] mld-snooping enable
```

```
[Switch-vlan2] mld-snooping general-query source-ip fe80:0:0:1::1
```

In VSI **aaa**, enable MLD snooping, and specify FE80:0:0:1::1 as the source IPv6 address for MLD general queries.

```
<Switch> system-view
[Switch] mld-snooping
[Switch-mld-snooping] quit
[Switch] vsi aaa
[Switch-vsi-aaa] mld-snooping enable
[Switch-vsi-aaa] mld-snooping general-query source-ip fe80:0:0:1::1
```

Related commands

enable (MLD-snooping view)

mld-snooping enable

7.1.26. mld-snooping group-limit

Use **mld-snooping group-limit** to set the maximum number of IPv6 multicast groups that a port can join.

Use **undo mld-snooping group-limit** to remove the limit on the maximum number of IPv6 multicast groups that a port can join.

Syntax

mld-snooping group-limit *limit* [**vlan** *vlan-list*]

undo mld-snooping group-limit [**vlan** *vlan-list*]

Default

No limit is placed on the maximum number of IPv6 multicast groups that a port can join.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

limit: Specifies the maximum number of multicast groups that a port can join, in the range of 0 to 4294967295.

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The VLAN ID is in the range of 1 to 4094. If you do not specify a VLAN, this command takes effect for all VLANs.

Usage guidelines

This command takes effect only on the IPv6 multicast groups that a port joins dynamically.

Examples

On GigabitEthernet 1/0/1, set the maximum number to 10 for IPv6 multicast groups that the port can join in VLAN 2.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
```

```
[Switch-GigabitEthernet1/0/1] mld-snooping group-limit 10 vlan 2
```

7.1.27. mld-snooping group-policy

Use **mld-snooping group-policy** to configure an IPv6 multicast group policy on a port to control the IPv6 multicast groups that hosts attached to the port can join.

Use **undo mld-snooping group-policy** to delete IPv6 multicast group policies on a port.

Syntax

mld-snooping group-policy *ipv6-acl-number* [**vlan** *vlan-list*]

undo mld-snooping group-policy [**vlan** *vlan-list*]

Default

No IPv6 multicast group policies exist. Hosts attached to the port can join any IPv6 multicast groups.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

ipv6-acl-number: Specifies an IPv6 basic or advanced ACL number in the range of 2000 to 3999. Hosts can join only the IPv6 multicast groups that the ACL permits. If the ACL does not exist or does not have valid rules, hosts cannot join IPv6 multicast groups.

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The VLAN ID is in the range of 1 to 4094. If you do not specify a VLAN, this command takes effect on all VLANs.

Usage guidelines

An IPv6 multicast group policy filters MLD reports to control the IPv6 multicast groups that hosts can join.

This command does not take effect on static member ports, because static member ports do not send MLD reports.

You can configure an IPv6 multicast group policy for a port in interface view or globally for all ports in MLD-snooping view. For a port, the port-specific configuration takes priority over the global configuration.

When you configure a rule in the IPv6 ACL, follow these restrictions and guidelines:

- In a basic ACL, the **source** *source-address source-prefix* option specifies an IPv6 multicast group address.
- In an advanced ACL, the **source** *source-address source-prefix* option specifies an IPv6 multicast source address. The **destination** *dest-address dest-prefix* option specifies an IPv6 multicast group address.

  To match MLDv1 reports and MLD IS_EX and MLDv2 TO_EX reports that do not carry IPv6 multicast source addresses, set the **source** *source-address source-prefix* option to 0::0.
- For the rule to take effect, do not specify the **vpn-instance** *vpn-instance* option.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

You can configure different ACLs for different VLANs on a port. If you configure multiple ACLs for the same VLANs on a port, the most recent configuration takes effect.

Examples

On GigabitEthernet 1/0/1, configure an IPv6 multicast group policy for VLAN 2 so that hosts attached to the port in VLAN 2 can join only the group FF03::101.

```
<Switch> system-view
[Switch] acl ipv6 basic 2000
[Switch-acl-ipv6-basic-2000] rule permit source ff03::101 128
[Switch-acl-ipv6-basic-2000] quit
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] mld-snooping group-policy 2000 vlan 2
```

Related commands

group-policy (MLD-snooping view)

7.1.28. mld-snooping host-aging-time

Use **mld-snooping host-aging-time** to set the aging timer for dynamic member ports in a VLAN or VSI.

Use **undo mld-snooping host-aging-time** to restore the default.

Syntax

mld-snooping host-aging-time *seconds*

undo mld-snooping host-aging-time

Default

The aging timer for dynamic member ports is 260 seconds.

Views

VLAN view

VSI view

Predefined user roles

network-admin

Parameters

seconds: Specifies an aging timer for dynamic member ports, in the range of 1 to 8097894 seconds.

Usage guidelines

You must enable MLD snooping for a VLAN or VSI before you execute this command.

You can set the timer for a VLAN in VLAN view, for a VSI in VSI view, or globally for all VLANs and VSIs in MLD-snooping view. For a VLAN, the VLAN-specific configuration takes priority over the global configuration. For a VSI, the VSI-specific configuration takes priority over the global configuration.

To avoid mistakenly deleting IPv6 multicast group members, set the aging timer for dynamic member ports to be greater than the value calculated by using the following formula:

[MLD general query interval] + [maximum response time for MLD general queries]

As a best practice, set the aging timer of dynamic member ports to the value calculated by using the following formula:

[MLD general query interval] × 2 + [maximum response time for MLD general queries]

Examples

In VLAN 2, enable MLD snooping, and set the aging timer for dynamic member ports in the VLAN to 300 seconds.

```
<Switch> system-view
[Switch] mld-snooping
[Switch-mld-snooping] quit
[Switch] vlan 2
[Switch-vlan2] mld-snooping enable
[Switch-vlan2] mld-snooping host-aging-time 300
```

In VSI **aaa**, enable MLD snooping, and set the aging timer for dynamic member ports in the VSI to 300 seconds.

```
<Switch> system-view
[Switch] mld-snooping
[Switch-mld-snooping] quit
[Switch] vsi aaa
[Switch-vsi-aaa] mld-snooping enable
[Switch-vsi-aaa] mld-snooping host-aging-time 300
```

Related commands

enable (MLD-snooping view)

host-aging-time (MLD-snooping view)

mld-snooping enable

7.1.29. mld-snooping host-join

Use **mld-snooping host-join** to configure a port as a simulated member host for an IPv6 multicast group or an IPv6 multicast source and group.

Use **undo mld-snooping host-join** to remove the configuration of a simulated member host for an IPv6 multicast group.

Syntax

mld-snooping host-join *ipv6-group-address* [**source-ip** *ipv6-source-address*] **vlan** *vlan-id*

undo mld-snooping host-join { *ipv6-group-address* [**source-ip** *ipv6-source-address*] **vlan** *vlan-id* | **all** }

Default

A port is not a simulated member host of any IPv6 multicast groups or any IPv6 multicast sources and groups.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

ipv6-group-address: Specifies an IPv6 multicast group address. The value range for this argument is FFxy::/16 (excluding FFx1::/16 and FFx2::/16), where "x" and "y" represent any hexadecimal numbers in the range of 0 to F.

source-ip *ipv6-source-address*: Specifies an IPv6 multicast source by its IPv6 address. If you specify an IPv6 multicast source, this command configures the port as a simulated member host for an IPv6 multicast source and group. If you do not specify an IPv6 multicast source, this command configures the port as a simulated member host for an IPv6 multicast group. This option takes effect on MLDv2 snooping devices.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094.

all: Specifies all IPv6 multicast groups and all IPv6 multicast sources and groups.

Usage guidelines

The version of MLD running on a simulated member host is the same as the version of MLD snooping running on the port. The port ages out in the same way as a dynamic member port.

Examples

Configure GigabitEthernet 1/0/1 as a simulated member host for the IPv6 multicast group (*, FF3E::101) in VLAN 2.

```
<Switch> system-view
[Switch] mld-snooping
[Switch-mld-snooping] quit
[Switch] vlan 2
[Switch-vlan2] mld-snooping enable
[Switch-vlan2] quit
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] mld-snooping host-join ff3e::101 vlan 2
```

7.1.30. mld-snooping last-listener-query-interval

Use **mld-snooping last-listener-query-interval** to set the MLD last listener query interval for a VLAN or VSI.

Use **undo mld-snooping last-listener-query-interval** to restore the default.

Syntax

mld-snooping last-listener-query-interval *interval*

undo mld-snooping last-listener-query-interval

Default

The MLD last listener query interval is 1 second.

Views

VLAN view

VSI view

Predefined user roles

network-admin

Parameters

interval: Specifies an MLD last listener query interval in the range of 1 to 25 seconds.

Usage guidelines

You must enable MLD snooping for a VLAN or VSI before you execute this command.

You can set the interval for a VLAN in VLAN view, for a VSI in VSI view, or globally for all VLANs and VSIs in MLD-snooping view. For a VLAN, the VLAN-specific configuration takes priority over the global configuration. For a VSI, the VSI-specific configuration takes priority over the global configuration.

Examples

In VLAN 2, enable MLD snooping, and set the MLD last listener query interval to 3 seconds.

```
<Switch> system-view
[Switch] mld-snooping
[Switch-mld-snooping] quit
[Switch] vlan 2
[Switch-vlan2] mld-snooping enable
[Switch-vlan2] mld-snooping last-listener-query-interval 3
```

In VSI **aaa**, enable MLD snooping, and set the MLD last listener query interval to 3 seconds.

```
<Switch> system-view
[Switch] mld-snooping
[Switch-mld-snooping] quit
[Switch] vsi aaa
[Switch-vsi-aaa] mld-snooping enable
[Switch-vsi-aaa] mld-snooping last-listener-query-interval 3
```

Related commands

enable (MLD-snooping view)

last-listener-query-interval (MLD-snooping view)

mld-snooping enable

7.1.31. mld-snooping max-response-time

Use **mld-snooping max-response-time** to set the maximum response time for MLD general queries in a VLAN or VSI.

Use **undo mld-snooping max-response-time** to restore the default.

Syntax

mld-snooping max-response-time *seconds*

undo mld-snooping max-response-time

Default

The maximum response time for MLD general queries is 10 seconds.

Views

VLAN view

VSI view

Predefined user roles

network-admin

Parameters

seconds: Specifies the maximum response time for MLD general queries, in the range of 1 to 3174 seconds.

Usage guidelines

You must enable MLD snooping for a VLAN before you execute this command.

You can set the time for a VLAN in VLAN view, for a VSI in VSI view, or globally for all VLANs and VSIs in MLD-snooping view. For a VLAN, the VLAN-specific configuration takes priority over the global configuration. For a VSI, the VSI-specific configuration takes priority over the global configuration.

To avoid mistakenly deleting IPv6 multicast group members, set the maximum response time for MLD general queries to be less than the MLD general query interval.

Examples

In VLAN 2, enable MLD snooping, and set the maximum response time for MLD general queries to 5 seconds.

```
<Switch> system-view
[Switch] mld-snooping
[Switch-mld-snooping] quit
[Switch] vlan 2
[Switch-vlan2] mld-snooping enable
[Switch-vlan2] mld-snooping max-response-time 5
```

In VSI **aaa**, enable MLD snooping, and set the maximum response time for MLD general queries to 5 seconds.

```
<Switch> system-view
[Switch] mld-snooping
[Switch-mld-snooping] quit
[Switch] vsi aaa
[Switch-vsi-aaa] mld-snooping enable
[Switch-vsi-aaa] mld-snooping max-response-time 5
```

Related commands

enable (MLD-snooping view)

max-response-time (MLD-snooping view)

mld-snooping enable

mld-snooping query-interval

7.1.32. mld-snooping overflow-replace

Use **mld-snooping overflow-replace** to enable the IPv6 multicast group replacement feature on a port.

Use **undo mld-snooping overflow-replace** to disable the multicast group replacement feature on a port.

Syntax

mld-snooping overflow-replace [**vlan** *vlan-list*]

undo mld-snooping overflow-replace [**vlan** *vlan-list*]

Default

The IPv6 multicast group replacement feature is disabled.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The VLAN ID is in the range of 1 to 4094. If you do not specify a VLAN, this command takes effect on all VLANs.

Usage guidelines

This command takes effect only on the IPv6 multicast groups that a port joins dynamically.

You can enable the IPv6 multicast group replacement feature for a port in interface view or globally for all ports in MLD-snooping view. For a port, the port-specific configuration takes priority over the global configuration.

Examples

On GigabitEthernet 1/0/1, enable the IPv6 multicast group replacement feature for VLAN 2.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] mld-snooping overflow-replace vlan 2
```

Related commands

overflow-replace (MLD-snooping view)

7.1.33. mld-snooping querier

Use **mld-snooping querier** to enable the MLD snooping querier.

Use **undo mld-snooping querier** to disable the MLD snooping querier.

Syntax

mld-snooping querier

undo mld-snooping querier

Default

The MLD snooping querier is disabled.

Views

VLAN view

VSI view

Predefined user roles

network-admin

Usage guidelines

You must enable MLD snooping for a VLAN or VSI before you execute this command.

For a sub-VLAN of an IPv6 multicast VLAN, this command takes effect only after you remove the VLAN from the IPv6 multicast VLAN.

Examples

In VLAN 2, enable MLD snooping, and enable the MLD snooping querier.

```
<Switch> system-view
[Switch] mld-snooping
[Switch-mld-snooping] quit
[Switch] vlan 2
[Switch-vlan2] mld-snooping enable
[Switch-vlan2] mld-snooping querier
```

In VSI **aaa**, enable MLD snooping, and enable the MLD snooping querier.

```
<Switch> system-view
[Switch] mld-snooping
[Switch-mld-snooping] quit
[Switch] vsi aaa
[Switch-vsi-aaa] mld-snooping enable
[Switch-vsi-aaa] mld-snooping querier
```

Related commands

enable (MLD-snooping view)

mld-snooping enable

subvlan (IPv6 multicast-VLAN view)

7.1.34. mld-snooping query-interval

Use **mld-snooping query-interval** to set the MLD general query interval for a VLAN or VSI.

Use **undo mld-snooping query-interval** to restore the default.

Syntax

mld-snooping query-interval *interval*

undo mld-snooping query-interval

Default

The MLD general query interval is 125 seconds.

Views

VLAN view

VSI view

Predefined user roles

network-admin

Parameters

interval: Specifies an MLD general query interval, in the range of 2 to 31744 seconds.

Usage guidelines

You must enable MLD snooping for a VLAN or VSI before you execute this command for the VLAN.

To avoid mistakenly deleting IPv6 multicast group members, set the MLD general query interval to be greater than the maximum response time for MLD general queries.

Examples

In VLAN 2, enable MLD snooping, and set the MLD general query interval to 20 seconds.

```
<Switch> system-view
[Switch] mld-snooping
[Switch-mld-snooping] quit
[Switch] vlan 2
[Switch-vlan2] mld-snooping enable
[Switch-vlan2] mld-snooping query-interval 20
```

In VSI **aaa**, enable MLD snooping, and set the MLD general query interval to 20 seconds.

```
<Switch> system-view
[Switch] mld-snooping
[Switch-mld-snooping] quit
[Switch] vsi aaa
[Switch-vsi-aaa] mld-snooping enable
[Switch-vsi-aaa] mld-snooping query-interval 20
```

Related commands

enable (MLD-snooping view)

max-response-time

mld-snooping enable

mld-snooping max-response-time

mld-snooping querier

7.1.35. mld-snooping report source-ip

Use **mld-snooping report source-ip** to configure the source IPv6 address for MLD reports.

Use **undo mld-snooping report source-ip** to restore the default.

Syntax

mld-snooping report source-ip *ipv6-address*

undo mld-snooping report source-ip

Default

In a VLAN, the source IPv6 address for MLD reports is the IPv6 link-local address of the current VLAN interface. If the current VLAN interface does not have an IPv6 link-local address, the source IPv6 address is FE80::02FF:FFFF:FE00:0001.

In a VSI, the source IPv6 address for MLD reports is the IPv6 link-local address of the gateway interface for the VSI. If the gateway interface does not have an IPv6 link-local address, the source IPv6 address is FE80::02FF:FFFF:FE00:0001.

Views

VLAN view

VSI view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies the source IPv6 address for MLD reports.

Usage guidelines

You must enable MLD snooping for a VLAN before you execute this command.

Examples

In VLAN 2, enable MLD snooping, and specify FE80:0:0:1::1 as the source IPv6 address for MLD reports.

```
<Switch> system-view
[Switch] mld-snooping
[Switch-mld-snooping] quit
[Switch] vlan 2
[Switch-vlan2] mld-snooping enable
[Switch-vlan2] mld-snooping report source-ip fe80:0:0:1::1
```

In VSI **aaa**, enable MLD snooping, and specify FE80:0:0:1::1 as the source IPv6 address for MLD reports.

```
<Switch> system-view
[Switch] mld-snooping
[Switch-mld-snooping] quit
[Switch] vsi aaa
[Switch-vsi-aaa] mld-snooping enable
[Switch-vsi-aaa] mld-snooping report source-ip fe80:0:0:1::1
```

Related commands

enable (MLD-snooping view)

mld-snooping enable

7.1.36. mld-snooping router-aging-time

Use **mld-snooping router-aging-time** to set the aging timer for dynamic router ports in a VLAN or VSI.

Use **undo mld-snooping router-aging-time** to restore the default.

Syntax

mld-snooping router-aging-time *seconds*

undo mld-snooping router-aging-time

Default

The aging timer for dynamic router ports is 260 seconds.

Views

VLAN view

VSI view

Predefined user roles

network-admin

Parameters

seconds: Specifies an aging timer for dynamic router ports, in the range of 1 to 8097894 seconds.

Usage guidelines

You must enable MLD snooping for a VLAN or VSI before you execute this command.

You can set the timer for a VLAN in VLAN view, for a VSI in VSI view, or globally for all VLANs and VSIs in MLD-snooping view. For a VLAN, the VLAN-specific configuration takes priority over the global configuration. For a VSI, the VSI-specific configuration takes priority over the global configuration.

Examples

In VLAN 2, enable MLD snooping, and set the aging timer for dynamic router ports in the VLAN to 100 seconds.

```
<Switch> system-view
[Switch] mld-snooping
[Switch-mld-snooping] quit
[Switch] vlan 2
[Switch-vlan2] mld-snooping enable
[Switch-vlan2] mld-snooping router-aging-time 100
```

In VSI **aaa**, enable MLD snooping, and set the aging timer for dynamic router ports in the VSI to 100 seconds.

```
<Switch> system-view
[Switch] mld-snooping
[Switch-mld-snooping] quit
[Switch] vsi aaa
[Switch-vsi-aaa] mld-snooping enable
[Switch-vsi-aaa] mld-snooping router-aging-time 100
```

Related commands

enable (MLD-snooping view)

mld-snooping enable

router-aging-time (MLD-snooping view)

7.1.37. mld-snooping source-deny

Use **mld-snooping source-deny** to enable IPv6 multicast source port filtering on a port to discard all IPv6 multicast data packets.

Use **undo mld-snooping source-deny** to disable IPv6 multicast source port filtering on a port.

Syntax

mld-snooping source-deny

undo mld-snooping source-deny

Default

IPv6 multicast source port filtering is disabled.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

You can enable this feature for a port in interface view or for the specified ports in MLD-snooping view. For a port, the configuration in interface view has the same priority as the configuration in MLD-snooping view, and the most recent configuration takes effect.

Examples

Enable source port filtering for IPv6 multicast data on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] mld-snooping source-deny
```

Related commands

source-deny (MLD-snooping view)

7.1.38. mld-snooping special-query source-ip

Use **mld-snooping special-query source-ip** to configure the source IPv6 address for MLD multicast-address-specific queries.

Use **undo mld-snooping special-query source-ip** to restore the default.

Syntax

mld-snooping special-query source-ip *ipv6-address*

undo mld-snooping special-query source-ip

Default

In a VLAN, the source IPv6 address of MLD multicast-address-specific queries is one of the following:

- The source address of MLD general queries if the MLD snooping querier of the VLAN has received MLD general queries.
- The IPv6 link-local address of the current VLAN interface if the MLD snooping querier does not receive an MLD general query.
- FE80::02FF:FFFF:FE00:0001 if the MLD snooping querier does not receive an MLD general query and the current VLAN interface does not have an IPv6 link-local address.

In a VSI, the source IPv6 address of MLD multicast-address-specific queries is one of the following:

- The source address of MLD general queries if the MLD snooping querier of the VSI has received MLD general queries.
- The IPv6 link-local address of the gateway interface for the VSI if the MLD snooping querier does not receive an MLD general query.
- FE80::02FF:FFFF:FE00:0001 if the gateway interface does not have an IPv6 link-local address.

Views

VLAN view

VSI view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies the source IPv6 address for MLD multicast-address-specific queries.

Usage guidelines

You must enable MLD snooping for a VLAN or VSI before you execute this command.

Examples

In VLAN 2, enable MLD snooping, and specify FE80:0:0:1::1 as the source IPv6 address of MLD multicast-address-specific queries.

```
<Switch> system-view
[Switch] mld-snooping
[Switch-mld-snooping] quit
[Switch] vlan 2
[Switch-vlan2] mld-snooping enable
[Switch-vlan2] mld-snooping special-query source-ip fe80:0:0:1::1
```

In VSI **aaa**, enable MLD snooping, and specify FE80:0:0:1::1 as the source IPv6 address of MLD multicast-address-specific queries.

```
<Switch> system-view
[Switch] mld-snooping
[Switch-mld-snooping] quit
[Switch] vsi aaa
[Switch-vsi-aaa] mld-snooping enable
[Switch-vsi-aaa] mld-snooping special-query source-ip fe80:0:0:1::1
```

Related commands

enable (MLD-snooping view)

mld-snooping enable

7.1.39. mld-snooping static-group

Use **mld-snooping static-group** to configure a port as a static member port of an IPv6 multicast group or an IPv6 multicast source and group.

Use **undo mld-snooping static-group** to delete the configuration of static member ports.

Syntax

mld-snooping static-group *ipv6-group-address* [**source-ip** *ipv6-source-address*] **vlan** *vlan-id*

undo mld-snooping static-group { *ipv6-group-address* [**source-ip** *ipv6-source-address*] **vlan** *vlan-id* | **all** }

Default

A port is not a static member port of IPv6 multicast groups.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

ipv6-group-address: Specifies an IPv6 multicast group address. The value range for this argument is FFxy::/16 (excluding FFx1::/16 and FFx2::/16), where "x" and "y" represent any hexadecimal numbers in the range of 0 to F.

source-ip *ipv6-source-address*: Specifies an IPv6 multicast source by its IPv6 address. If you specify an IPv6 multicast source, this command configures the port as a static member port of an IPv6 multicast source and group. If you do not specify an IPv6 multicast source, this command configures the port as a static member port of an IPv6 multicast group. This option takes effect on MLDv2 snooping devices.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094.

all: Specifies all IPv6 multicast groups and all IPv6 multicast sources and groups.

Examples

Configure GigabitEthernet 1/0/1 as a static member port for the IPv6 multicast group (*, FF3E::101) in VLAN 2.

```
<Switch> system-view
[Switch] mld-snooping
[Switch-mld-snooping] quit
[Switch] vlan 2
[Switch-vlan2] mld-snooping enable
[Switch-vlan2] quit
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] mld-snooping static-group ff3e::101 vlan 2
```

7.1.40. mld-snooping static-router-port

Use **mld-snooping static-router-port** to configure a port as a static router port.

Use **undo mld-snooping static-router-port** to remove the configuration of static router ports.

Syntax

mld-snooping static-router-port vlan *vlan-id*

undo mld-snooping static-router-port { **all** | **vlan** *vlan-id* }

Default

A port is not a static router port.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

all: Specifies all VLANs.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094.

Examples

Configure GigabitEthernet 1/0/1 as a static router port in VLAN 2.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] mld-snooping static-router-port vlan 2
```

7.1.41. mld-snooping version

Use **mld-snooping version** to specify an MLD snooping version for a VLAN or VSI.

Use **undo mld-snooping version** to restore the default.

Syntax

mld-snooping version *version-number*

undo mld-snooping version

Default

The MLD snooping version in a VLAN or VSI is 1.

Views

VLAN view

VSI view

Predefined user roles

network-admin

Parameters

version-number: Specifies an MLD snooping version, 1 or 2.

Usage guidelines

You must enable MLD snooping for a VLAN or VSI before you configure this command.

You can specify the version for a VLAN in VLAN view or for the specified VLANs in MLD-snooping view. The VLAN-specific configuration has the same priority as the configuration in MLD-snooping view, and the most recent configuration takes effect.

Examples

In VLAN 2, enable MLD snooping, and specify MLD snooping version 2.

```
<Switch> system-view
[Switch] mld-snooping
[Switch-mld-snooping] quit
[Switch] vlan 2
[Switch-vlan2] mld-snooping enable
[Switch-vlan2] mld-snooping version 2
```

In VSI **aaa**, enable MLD snooping, and specify MLD snooping version 2.

```
<Switch> system-view
[Switch] mld-snooping
[Switch-mld-snooping] quit
[Switch] vsi aaa
[Switch-vsi-aaa] mld-snooping enable
[Switch-vsi-aaa] mld-snooping version 2
```

Related commands

enable (MLD-snooping view)

mld-snooping enable

version (MLD-snooping view)

7.1.42. overflow-replace (MLD-snooping view)

Use **overflow-replace** to enable the IPv6 multicast group replacement feature globally.

Use **undo overflow-replace** to disable the IPv6 multicast group replacement feature globally.

Syntax

overflow-replace [**vlan** *vlan-list*]

undo overflow-replace [**vlan** *vlan-list*]

Default

The IPv6 multicast group replacement feature is disabled.

Views

MLD-snooping view

Predefined user roles

network-admin

Parameters

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The VLAN ID is in the range of 1 to 4094. If you do not specify a VLAN, this command takes effect on all VLANs.

Usage guidelines

This command takes effect only on the IPv6 multicast groups that a port joins dynamically.

You can enable IPv6 multicast group replacement globally for all ports in MLD-snooping view or for a port in interface view. For a port, the port-specific configuration takes priority over the global configuration.

Examples

Globally enable the IPv6 multicast group replacement feature for VLAN 2.

```
<Switch> system-view
[Switch] mld-snooping
[Switch-mld-snooping] overflow-replace vlan 2
```

Related commands

mld-snooping overflow-replace

7.1.43. report-aggregation (MLD-snooping view)

Use **report-aggregation** to enable MLD report suppression.

Use **undo report-aggregation** to disable MLD report suppression.

Syntax

report-aggregation

undo report-aggregation

Default

MLD report suppression is enabled.

Views

MLD-snooping view

Predefined user roles

network-admin

Examples

Disable MLD report suppression.

```
<Switch> system-view
[Switch] mld-snooping
[Switch-mld-snooping] undo report-aggregation
```

7.1.44. reset mld-snooping group

Use **reset mld-snooping group** to clear information about dynamic MLD snooping group entries.

Syntax

reset mld-snooping group { *ipv6-group-address* [*ipv6-source-address*] | **all** } [**vlan** *vlan-id* | **vsi** *vsi-name*]

Views

User view

Predefined user roles

network-admin

Parameters

ipv6-group-address: Specifies an IPv6 multicast group address. The value range for this argument is FFxy::/16 (excluding FFx1::/16 and FFx2::/16), where "x" and "y" represent any hexadecimal numbers in the range of 0 to F.

ipv6-source-address: Specifies an IPv6 multicast source address. If you do not specify an IPv6 multicast source, this command clears information about dynamic MLD snooping group entries for all IPv6 multicast sources.

all: Specifies all IPv6 multicast groups.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command clears information about dynamic MLD snooping group entries for all VLANs.

vsi *vsi-name*: Specifies a VSI by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VSI, this command clears information about dynamic MLD snooping group entries for all VSIs.

Examples

Clear information about all dynamic MLD snooping group entries.

```
<Switch> reset mld-snooping group all
```

Related commands

display mld-snooping group

7.1.45. reset mld-snooping router-port

Use **reset mld-snooping router-port** to clear dynamic router port information.

Syntax

reset mld-snooping router-port { **all** | **vlan** *vlan-id* | **vsi** *vsi-name* }

Views

User view

Predefined user roles

network-admin

Parameters

all: Specifies all dynamic router ports.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command clears dynamic router port information for all VLANs.

vsi *vsi-name*: Specifies a VSI by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VSI, this command clears dynamic router port information for all VSIs.

Examples

Clear information about all dynamic router ports.

```
<Switch> reset mld-snooping router-port all
```

Related commands

display mld-snooping router-port

7.1.46. reset mld-snooping statistics

Use **reset mld-snooping statistics** to clear statistics for MLD messages and IPv6 PIM hello messages learned through MLD snooping.

Syntax

reset mld-snooping statistics

Views

User view

Predefined user roles

network-admin

Examples

Clear statistics for all MLD messages and IPv6 PIM hello messages learned through MLD snooping.

```
<Switch> reset mld-snooping statistics
```

Related commands

display mld-snooping statistics

7.1.47. router-aging-time (MLD-snooping view)

Use **router-aging-time** to set the aging timer for dynamic router ports globally.

Use **undo router-aging-time** to restore the default.

Syntax

router-aging-time *seconds*

undo router-aging-time

Default

The aging timer for dynamic router ports is 260 seconds.

Views

MLD-snooping view

Predefined user roles

network-admin

Parameters

seconds: Specifies an aging timer for dynamic router ports, in the range of 1 to 8097894 seconds.

Usage guidelines

You can set the timer globally for all VLANs and VSIs in MLD-snooping view, for a VSI in VSI view, or for a VLAN in VLAN view. For a VSI, the VSI-specific configuration takes priority over the global configuration. For a VLAN, the VLAN-specific configuration takes priority over the global configuration.

Examples

Set the global aging timer for dynamic router ports to 100 seconds.

```
<Switch> system-view
[Switch] mld-snooping
[Switch-mld-snooping] router-aging-time 100
```

Related commands

mld-snooping router-aging-time

7.1.48. source-deny (MLD-snooping view)

Use **source-deny** to enable IPv6 multicast source port filtering on ports to discard all IPv6 multicast data packets.

Use **undo source-deny** to disable IPv6 multicast source port filtering on ports.

Syntax

source-deny port *interface-list*

undo source-deny port *interface-list*

Default

IPv6 multicast source port filtering is disabled.

Views

MLD-snooping view

Predefined user roles

network-admin

Parameters

port *interface-list*: Specifies a space-separated list of port items. Each item specifies a port by its port type and number or a range of ports in the form of *start-interface-type interface-number* **to** *end-interface-type interface-number*.

Usage guidelines

You can enable this feature for the specified ports in MLD-snooping view or for a port in interface view. For a port, the configuration in MLD-snooping view has the same priority as the configuration in interface view, and the most recent configuration takes effect.

Examples

Enable source port filtering for IPv6 multicast data on ports GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4.

```
<Switch> system-view
[Switch] mld-snooping
[Switch-mld-snooping] source-deny port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
```

Related commands

mld-snooping source-deny

7.1.49. version (MLD-snooping view)

Use **version** to specify an MLD snooping version for VLANs.

Use **undo version** to restore the default.

Syntax

version *version-number* **vlan** *vlan-list*

undo version vlan *vlan-list*

Default

The MLD snooping version in a VLAN is 1.

Views

MLD-snooping view

Predefined user roles

network-admin

Parameters

version-number: Specifies an MLD snooping version, 1 or 2.

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The VLAN ID is in the range of 1 to 4094.

Usage guidelines

You must enable MLD snooping for the specified VLANs before you execute this command.

You can specify the version for the specified VLANs in MLD-snooping view or for a VLAN in VLAN view. The VLAN-specific configuration has the same priority as the configuration in MLD-snooping view, and the most recent configuration takes effect.

Examples

Enable MLD snooping for VLAN 2 through VLAN 10, and specify MLD snooping version 2 for these VLANs.

```
<Switch> system-view
[Switch] mld-snooping
[Switch-mld-snooping] enable vlan 2 to 10
[Switch-mld-snooping] version 2 vlan 2 to 10
```

Related commands

enable (MLD-snooping view)

mld-snooping enable

mld-snooping version

Contents

A page of this section is **6-x-x**

8. IPv6 multicast VLAN commands 8-1
8.1. IPv6 multicast VLAN commands 8-1
8.1.1. display ipv6 multicast-vlan 8-1
8.1.2. display ipv6 multicast-vlan forwarding-table 8-2
8.1.3. display ipv6 multicast-vlan group 8-3
8.1.4. ipv6 multicast-vlan 8-5
8.1.5. ipv6 multicast-vlan entry-limit 8-6
8.1.6. ipv6 port multicast-vlan 8-7
8.1.7. port (IPv6 multicast VLAN view) 8-7
8.1.8. reset ipv6 multicast-vlan group 8-8
8.1.9. subvlan (IPv6 multicast VLAN view) 8-9

8. IPv6 multicast VLAN commands

8.1. IPv6 multicast VLAN commands

8.1.1. display ipv6 multicast-vlan

Use **display ipv6 multicast-vlan** to display information about IPv6 multicast VLANs.

Syntax

display ipv6 multicast-vlan [*vlan-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vlan-id: Specifies an IPv6 multicast VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify an IPv6 multicast VLAN, this command displays information about all IPv6 multicast VLANs.

Examples

Display information about all IPv6 multicast VLANs.

```
<Switch> display ipv6 multicast-vlan
Total 2 IPv6 multicast VLANs.

IPv6 multicast VLAN 100:
  Sub-VLAN list(3 in total):
    2-3, 6
  Port list(3 in total):
    GE1/0/1
    GE1/0/2
    GE1/0/3

IPv6 multicast VLAN 200:
  Sub-VLAN list(0 in total):
  Port list(0 in total):
```

Table 8-1 Command output

Field	Description
Total 2 IPv6 multicast VLANs	Total number of IPv6 multicast VLANs.
Sub-VLAN list(3 in total)	Sub-VLAN list of the IPv6 multicast VLAN, and the total number of the sub-VLANs.
Port list(3 in total)	Port list of the IPv6 multicast VLAN, and the total number of the ports.

8.1.2. display ipv6 multicast-vlan forwarding-table

Use **display ipv6 multicast-vlan forwarding-table** to display IPv6 multicast VLAN forwarding entries.

Syntax

display ipv6 multicast-vlan forwarding-table [*ipv6-source-address* [*prefix-length*] | *ipv6-group-address* [*prefix-length*] | **slot** *slot-number* | **subvlan** *vlan-id* | **vlan** *vlan-id*] *

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ipv6-source-address: Specifies an IPv6 multicast source by its IPv6 address. If you do not specify an IPv6 multicast source, this command displays IPv6 multicast VLAN forwarding entries for all IPv6 multicast sources.

prefix-length: Specifies a prefix length of the IPv6 multicast source address. The value range is 0 to 128 and the default value is 128.

ipv6-group-address: Specifies an IPv6 multicast group address. The value range for this argument is FFxy::/16, where "x" and "y" represent any hexadecimal numbers in the range of 0 to F. If you do not specify an IPv6 multicast group, this command displays IPv6 multicast VLAN forwarding entries for all IPv6 multicast groups.

prefix-length: Specifies a prefix length of the IPv6 multicast group address. The value range is 8 to 128 and the default value is 128.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays IPv6 multicast VLAN forwarding entries for the master device.

subvlan *vlan-id*: Specifies a sub-VLAN by its VLAN ID. If you do not specify a sub-VLAN, this command displays IPv6 multicast VLAN forwarding entries for all sub-VLANs.

vlan *vlan-id*: Specifies an IPv6 multicast VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify an IPv6 multicast VLAN, this command displays IPv6 multicast VLAN forwarding entries for all VLANs.

Examples

Display all IPv6 multicast VLAN forwarding entries.

```
<Switch> display ipv6 multicast-vlan forwarding-table
IPv6 multicast VLAN 100 Forwarding Table
Total 1 entries, 1 matched

00001. (1::1, FF0E::1)
     Flags: 0x10000
     IPv6 multicast VLAN: 100
     List of sub-VLANs (3 in total):
       1: VLAN 10
       2: VLAN 20
```

```
3: VLAN 30
```

Table 8-2 Command output

Field	Description
IPv6 multicast VLAN 100 Forwarding Table	The multicast forwarding table for IPv6 multicast VLAN 100.
Total 1 entries, 1 matched	Total number of (S, G) entries, and the number of matching entries.
00001	Sequence number of the (S, G) entry.
(1::1, FF0E::1)	(S, G) entry, where a double colon (::) in the S position means all IPv6 multicast sources.
Flags	Entry flag. This field displays one flag or the sum of multiple flags. In this example, the value 0x10000 means that the entry has only one flag 0x10000. The following flags are available for an entry: • **0x1**—The entry is in inactive state. • **0x4**—The entry fails to update. • **0x8**—The sub-VLAN information fails to update for the entry. • **0x200**—The entry is in GR state. • **0x10000**—The entry is an IPv6 multicast VLAN forwarding entry.
List of sub-VLANs (3 in total)	Sub-VLAN list of the IPv6 multicast VLAN, and the total number of the sub-VLANs.

8.1.3. display ipv6 multicast-vlan group

Use **display ipv6 multicast-vlan group** to display information about IPv6 multicast groups in IPv6 multicast VLANs.

Syntax

display ipv6 multicast-vlan group [*ipv6-source-address* | *ipv6-group-address* | **slot** *slot-number* | **verbose** | **vlan** *vlan-id*] *

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ipv6-source-address: Specifies an IPv6 multicast source by its IPv6 address. If you do not specify an IPv6 multicast source, this command displays information about IPv6 multicast groups for all IPv6 multicast sources in IPv6 multicast VLANs.

ipv6-group-address: Specifies an IPv6 multicast group address. The value range for this argument is FFxy::/16 (excluding FFx1::/16 and FFx2::/16), where "x" and "y" represent any hexadecimal numbers in the range of 0 to F. If you do not specify an IPv6 multicast group, this command displays information about all IPv6 multicast groups in IPv6 multicast VLANs.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information about IPv6 multicast groups in IPv6 multicast VLANs for the master device.

verbose: Displays detailed information. If you do not specify the keyword, this command displays brief information.

vlan *vlan-id*: Specifies an IPv6 multicast VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify an IPv6 multicast VLAN, this command displays information about IPv6 multicast groups for all IPv6 multicast VLANs.

Examples

Display detailed information about all IPv6 multicast groups in IPv6 multicast VLANs.

```
<Switch> display ipv6 multicast-vlan group verbose
Total 6 entries.

IPv6 multicast VLAN 10: Total 3 entries.
  (2::2, FF0E::2)
    Flags: 0x70000020
    Sub-VLANs (1 in total):
      VLAN 40
  (22::22, FF0E::4)
    Flags: 0x70000030
    Sub-VLANs (1 in total):
      VLAN 40
  (::, FF0E::10)
    Flags: 0x10000030
    Sub-VLANs (1 in total):
      VLAN 40

IPv6 multicast VLAN 20: Total 3 entries.
  (2::2, FF0E::2)
    Flags: 0x70000010
    Sub-VLANs (0 in total):
  (22::22, FF0E::4)
    Flags: 0x70000010
    Sub-VLANs (0 in total):
  (::, FF0E::10)
    Flags: 0x50000010
    Sub-VLANs (0 in total):
```

Table 8-3 Command output

Field	Description
Total 6 entries	Total number of (S, G) entries.
IPv6 multicast VLAN 10: Total 3 entries	Total number of (S, G) entries in IPv6 multicast VLAN 10.
(::, FF0E::10)	(S, G) entry, where a double colon (::) in the S position means all IPv6 multicast sources.
Flags	Entry flag. This field displays one flag or the sum of multiple flags.

Field	Description

	For example, the value 0x70000020 means that the entry has flags 0x20, 0x10000000, 0x20000000, and 0x40000000.
	The following flags are available for an entry:
	• **0x10**—The entry is created by the IPv6 multicast VLAN.
	• **0x20**—The entry is created by the sub-VLAN of the IPv6 multicast VLAN.
	• **0x40**—The entry is to be deleted.
	• **0x10000000**—This value represents one of the following situations:
	  ○ The entry is newly created.
	  ○ The device receives an MLD query within an MLD general query interval.
	• **0x20000000**—The device does not receive MLDv1 or MLDv2 reports that match the entry within an MLD general query interval.
	• **0x40000000**—The device does not receive MLDv2 IS_EX (NULL) reports that match the entry within an MLD general query interval.

Sub-VLANs (1 in total)	Sub-VLAN list of the IPv6 multicast VLAN, and the total number of the sub-VLANs.

Related commands

reset ipv6 multicast-vlan group

8.1.4. ipv6 multicast-vlan

Use **ipv6 multicast-vlan** to configure an IPv6 multicast VLAN and enter its view, or enter the view of an existing IPv6 multicast VLAN.

Use **undo ipv6 multicast-vlan** to remove the configuration of IPv6 multicast VLANs.

Syntax

ipv6 multicast-vlan *vlan-id*

undo ipv6 multicast-vlan { **all** | *vlan-id* }

Default

No IPv6 multicast VLANs exist.

Views

System view

Predefined user roles

network-admin

Parameters

vlan-id: Specifies an existing VLAN ID in the range of 1 to 4094.

all: Specifies all IPv6 multicast VLANs.

Usage guidelines

The total number of IPv6 multicast VLANs on a device cannot exceed the system upper limit.

You must enable MLD snooping for the VLAN to be configured as an IPv6 multicast VLAN.

As a best practice, do not configure an IPv6 multicast VLAN on a device that is enabled with IPv6 multicast routing.

Examples

Enable MLD snooping for VLAN 100. Configure VLAN 100 as an IPv6 multicast VLAN and enter its view.

```
<Switch> system-view
[Switch] mld-snooping
[Switch-mld-snooping] quit
[Switch] vlan 100
[Switch-vlan100] mld-snooping enable
[Switch-vlan100] quit
[Switch] ipv6 multicast-vlan 100
[Switch-ipv6-mvlan-100]
```

Related commands

ipv6 multicast routing

mld-snooping enable

8.1.5. ipv6 multicast-vlan entry-limit

Use **ipv6 multicast-vlan entry-limit** to set the maximum number of IPv6 multicast VLAN forwarding entries.

Use **undo ipv6 multicast-vlan entry-limit** to restore the default.

Syntax

ipv6 multicast-vlan entry-limit *limit*

undo ipv6 multicast-vlan entry-limit

Default

The maximum number of IPv6 multicast VLAN forwarding entries is 4000.

Views

System view

Predefined user roles

network-admin

Parameters

limit: Specifies the maximum number of IPv6 multicast VLAN forwarding entries. The value range for this argument is 0 to 4000.

Examples

Set the maximum number of IPv6 multicast VLAN forwarding entries to 120.

```
<Switch> system-view
[Switch] ipv6 multicast-vlan entry-limit 120
```

Related commands

entry-limit (MLD-snooping view)

8.1.6. ipv6 port multicast-vlan

Use **ipv6 port multicast-vlan** to assign a user port to an IPv6 multicast VLAN.

Use **undo ipv6 port multicast-vlan** to restore the default.

Syntax

ipv6 port multicast-vlan *vlan-id*

undo ipv6 port multicast-vlan

Default

A port does not belong to an IPv6 multicast VLAN.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

vlan-id: Specifies an IPv6 multicast VLAN by its VLAN ID in the range of 1 to 4094.

Usage guidelines

You can assign a port to only one IPv6 multicast VLAN.

For the port to be assigned to an IPv6 multicast VLAN, you must enable MLD snooping for the VLAN to which the port belongs.

Examples

Assign GigabitEthernet 1/0/1 to IPv6 multicast VLAN 100.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] ipv6 port multicast-vlan 100
```

8.1.7. port (IPv6 multicast VLAN view)

Use **port** to assign user ports to an IPv6 multicast VLAN.

Use **undo port** to delete user ports from an IPv6 multicast VLAN.

Syntax

port *interface-list*

undo port { **all** | *interface-list* }

Default

An IPv6 multicast VLAN does not have user ports.

Views

IPv6 multicast VLAN view

Predefined user roles

network-admin

Parameters

interface-list: Specifies a port in the form of *interface-type interface-number*, or a port range in the form of *interface-type interface-number* to *interface-type interface-number*.

all: Specifies all user ports in the current IPv6 multicast VLAN.

Usage guidelines

You can assign only Layer 2 Ethernet interfaces or Layer 2 aggregate interfaces as user ports to an IPv6 multicast VLAN. Additionally, you can assign a port to only one IPv6 multicast VLAN.

For ports to be assigned to an IPv6 multicast VLAN, you must enable MLD snooping for the VLANs to which the ports belong.

Examples

Assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/5 as user ports to IPv6 multicast VLAN 100.

```
<Switch> system-view
[Switch] ipv6 multicast-vlan 100
[Switch-ipv6-mvlan-100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/5
```

8.1.8. reset ipv6 multicast-vlan group

Use **reset ipv6 multicast-vlan group** to clear IPv6 multicast group entries in IPv6 multicast VLANs.

Syntax

reset ipv6 multicast-vlan group [*ipv6-group-address* [*prefix-length*] | *ipv6-source-address* [*prefix-length*] | **vlan** *vlan-id*] *

Views

User view

Predefined user roles

network-admin

Parameters

ipv6-group-address: Specifies an IPv6 multicast group address. The value range for this argument is FFxy::/16 (excluding FFx1::/16 and FFx2::/16), where "x" and "y" represent any hexadecimal numbers in the range of 0 to F. If you do not specify an IPv6 multicast group, this command clears all IPv6 multicast group entries in IPv6 multicast VLANs.

prefix-length: Specifies a prefix length of the IPv6 multicast group address. The value range is 8 to 128 and the default value is 128.

ipv6-source-address: Specifies an IPv6 multicast source by its IPv6 address. If you do not specify an IPv6 multicast source, this command clears IPv6 multicast group entries for all IPv6 multicast sources in IPv6 multicast VLANs.

prefix-length: Specifies a prefix length of the IPv6 multicast source address. The value range is 0 to 128 and the default value is 128.

vlan *vlan-id*: Specifies an IPv6 multicast VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify an IPv6 multicast VLAN, this command clears IPv6 multicast group entries for all IPv6 multicast VLANs.

Examples

Clear all IPv6 multicast group entries for all IPv6 multicast VLANs.

```
<Switch> reset ipv6 multicast-vlan group
```

Related commands

display ipv6 multicast-vlan group

8.1.9. subvlan (IPv6 multicast VLAN view)

Use **subvlan** to assign VLANs as sub-VLANs to an IPv6 multicast VLAN.

Use **undo subvlan** to delete sub-VLANs from an IPv6 multicast VLAN.

Syntax

subvlan *vlan-list*

undo subvlan { **all** | *vlan-list* }

Default

An IPv6 multicast VLAN does not have sub-VLANs.

Views

IPv6 multicast VLAN view

Predefined user roles

network-admin

Parameters

vlan-list: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The value range for the VLAN ID is 1 to 4094. The specified VLANs must exist and cannot be multicast VLANs or sub-VLANs of other IPv6 multicast VLANs.

all: Specifies all sub-VLANs of the current IPv6 multicast VLAN.

Usage guidelines

You must enable MLD snooping for VLANs to be configured as sub-VLANs of an IPv6 multicast VLAN.

Examples

Assign VLAN 10 through VLAN 15 as sub-VLANs to multicast VLAN 100.

```
<Switch> system-view
[Switch] ipv6 multicast-vlan 100
[Switch-ipv6-mvlan-100] subvlan 10 to 15
```

Contents

A page of this section is **6-x-x**

9. IPv6 multicast routing and forwarding commands 9-1
9.1. IPv6 multicast routing and forwarding commands 9-1
9.1.1. display ipv6 multicast boundary 9-1
9.1.2. display ipv6 multicast forwarding-table 9-2
9.1.3. display ipv6 multicast routing-table 9-4
9.1.4. display ipv6 multicast rpf-info 9-6
9.1.5. ipv6 multicast boundary 9-7
9.1.6. ipv6 multicast routing 9-8
9.1.7. load-splitting (IPv6 MRIB view) 9-9
9.1.8. longest-match (IPv6 MRIB view) 9-10
9.1.9. reset ipv6 multicast forwarding-table 9-10
9.1.10. reset ipv6 multicast routing-table 9-11

9. IPv6 multicast routing and forwarding commands

MEMO:

The **vpn-instance** *vpn-instance-name* option for each command is supported by V7.2.18 and later software.

9.1. IPv6 multicast routing and forwarding commands

9.1.1. display ipv6 multicast boundary

Use **display ipv6 multicast boundary** to display IPv6 multicast boundary information.

Syntax

display ipv6 multicast [**vpn-instance** *vpn-instance-name*] **boundary** { **group** [*ipv6-group-address* [*prefix-length*]] | **scope** [*scope-id*] } [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command deletes all static multicast routes on the public network.**group**: Displays the IPv6 multicast boundary information for the specified groups.

ipv6-group-address: Specifies an IPv6 multicast group address in the range of FFxy::/16, where "x" and "y" represent any hexadecimal numbers in the range of 0 to F. If you do not specify an IPv6 multicast group, this command displays IPv6 multicast boundary information for all IPv6 multicast groups.

prefix-length: Specifies an address prefix length in the range of 8 to 128. The default is 128.

scope: Displays the IPv6 multicast group boundary information in the admin-scoped zone.

scope-id: Specifies an admin-scope zone by its ID in the range of 3 to 15, which is identified by the scope field in the IPv6 multicast group address. If you do not specify an admin-scoped zone, this command displays IPv6 multicast boundary information for all IPv6 admin-scoped zones.

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays IPv6 multicast boundary information for all interfaces.

Examples

Display IPv6 multicast boundary information of all IPv6 multicast groups for all interfaces.

```
<Switch> display ipv6 multicast boundary group
 Boundary                                                Interface
 FF1E::/64                                               Vlan1
```

Display IPv6 multicast boundary information in all IPv6 admin-scope zones for all interfaces.

```
<Switch> display ipv6 multicast boundary scope
 Boundary            Interface
        3            Vlan-interface1
```

Table 9-1 Command output

Field	Description
Boundary	IPv6 multicast group or IPv6 admin-scoped zone associated with the IPv6 multicast boundary.
Interface	Boundary interface associated with the IPv6 multicast boundary.

Related commands

ipv6 multicast boundary

9.1.2. display ipv6 multicast forwarding-table

Use **display ipv6 multicast forwarding-table** to display IPv6 multicast forwarding entries.

Syntax

display ipv6 multicast [**vpn-instance** *vpn-instance-name*] **forwarding-table** [*ipv6-source-address* [*prefix-length*] | *ipv6-group-address* [*prefix-length*] | **incoming-interface** *interface-type interface-number* | **outgoing-interface** { **exclude** | **include** | **match** } *interface-type interface-number* | **slot** *slot-number* | **statistics**] *

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command deletes all static multicast routes on the public network.*ipv6-source-address*: Specifies an IPv6 multicast source address.

ipv6-group-address: Specifies an IPv6 multicast group address in the range of FFxy::/16, where "x" and "y" represent any hexadecimal numbers in the range of 0 to F.

prefix-length: Specifies an address prefix length. The default value is 128. For an IPv6 multicast group address, the value range for this argument is 8 to 128. For an IPv6 multicast source address, the value range for this argument is 0 to 128.

incoming-interface: Specifies the IPv6 forwarding entries that contain the specified incoming interface.

interface-type interface-number: Specifies an interface by its type and number.

outgoing-interface: Specifies the IPv6 forwarding entries that contain the specified outgoing interface.

exclude: Specifies the IPv6 forwarding entries that do not contain the specified interface in the outgoing interface list.

include: Specifies the IPv6 forwarding entries that contain the specified interface in the outgoing interface list.

match: Specifies the IPv6 forwarding entries that contain only the specified interface in the outgoing interface list.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays IPv6 multicast forwarding entries for the master device.

statistics: Displays statistics for the IPv6 multicast forwarding table.

Examples

Display IPv6 multicast forwarding entries.

```
<Switch> display ipv6 multicast forwarding-table
Total 1 entries, 1 matched

00001. (1::1, ff0e::1)
     Flags: 0x0
     Uptime: 00:08:32, Timeout in: 00:03:26
     Incoming interface: Vlan-interface10
          Incoming sub-VLAN: VLAN 11
          Outgoing sub-VLAN: VLAN 12
                             VLAN 13
     List of 1 outgoing interface:
       1: Vlan-interface20
          Sub-VLAN: VLAN 21
                    VLAN 22
     Matched 19648 packets(20512512 bytes), Wrong If 0 packet
     Forwarded 19648 packets(20512512 bytes)
```

Table 9-2 Command output

Field	Description
Total 1 entries, 1 matched	Total number of (S, G) entries, and the total number of matching (S, G) entries.
00001	Sequence number of the (S, G) entry.
(1::1, ff0e::1)	(S, G) entry.
Flags	Entry flag. This field displays one flag or the sum of multiple flags. In this example, the value 0x0 means that the entry has

Field	Description
	only one flag 0x0. The following flags are available for an entry: • **0x0**—The entry is in correct state. • **0x1**—The entry is in inactive state. • **0x2**—The entry is null. • **0x4**—The entry fails to update. • **0x8**—The outgoing interface information fails to update for the entry. • **0x20**—A register outgoing interface is available. • **0x40**—The entry is to be deleted. • **0x80**—The entry is in registration suppression state. • **0x100**—The entry is being deleted. • **0x200**—The entry is in GR state. • **0x400**—The entry has the VLAN interface of the super VLAN. • **0x800**—The entry has the associated ND entry for the IPv6 multicast source address. • **0x4000000**—The entry is created by the MLD proxy.
Uptime	Length of time for which the (S, G) entry has been up.
Timeout in	Length of time in which the (S, G) entry will time out.
Incoming interface	Incoming interface of the (S, G) entry.
Incoming sub-VLAN	Incoming sub-VLAN of the super VLAN when the incoming interface of the (S, G) entry is the VLAN interface of this super VLAN.
Outgoing sub-VLAN	Outgoing sub-VLAN of the super VLAN when the incoming interface of the (S, G) entry is the VLAN interface of this super VLAN.
List of 1 outgoing interfaces	Outgoing interface list of the (S, G) entry.
Sub-VLAN	Outgoing sub-VLAN of the super VLAN when the outgoing interface of the (S, G) entry is the VLAN interface of this super VLAN.
Matched 19648 packets (20512512 bytes), Wrong If 0 packet	Number of packets (bytes) that match the (S, G) entry, and number of packets with incoming interface errors. The numbers are displayed as 0 if an outgoing interface of the (S, G) entry is on the specified slot.
Forwarded 19648 packets (20512512 bytes)	Number of packets (bytes) that have been forwarded. The numbers are displayed as 0 if an outgoing interface of the (S, G) entry is on the specified slot.

Related commands

`reset ipv6 multicast forwarding-table`

9.1.3. display ipv6 multicast routing-table

Use **`display ipv6 multicast routing-table`** to display IPv6 multicast routing entries.

Syntax

display ipv6 multicast [**vpn-instance** *vpn-instance-name*] **routing-table** [*ipv6-source-address* [*prefix-length*] | *ipv6-group-address* [*prefix-length*] | **incoming-interface** *interface-type interface-number* | **outgoing-interface** { **exclude** | **include** | **match** } *interface-type interface-number*] *

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command deletes all static multicast routes on the public network.*ipv6-source-address*: Specifies an IPv6 multicast source address.

ipv6-group-address: Specifies an IPv6 multicast group address in the range of FFxy::/16, where "x" and "y" represent any hexadecimal numbers in the range of 0 to F.

prefix-length: Specifies an address prefix length. The default is 128. For an IPv6 multicast group address, the value range for this argument is 8 to 128. For an IPv6 multicast source address, the value range for this argument is 0 to 128.

incoming-interface: Displays the IPv6 routing entries that contain the specified incoming interface.

interface-type interface-number: Specifies an interface by its type and number.

outgoing-interface: Displays the IPv6 routing entries that contain the specified outgoing interface.

exclude: Displays the IPv6 routing entries that do not contain the specified interface in the outgoing interface list.

include: Displays the IPv6 routing entries that contain the specified interface in the outgoing interface list.

match: Displays the IPv6 routing entries that contain only the specified interface in the outgoing interface list.

Usage guidelines

IPv6 multicast routing entries are the basis of IPv6 multicast forwarding. You can use this command to view the establishment state of (S, G) entries.

Examples

Display IPv6 multicast routing entries.

```
<Switch> display ipv6 multicast routing-table
 Total 1 entries

 00001. (2001::2, FFE3::101)
       Uptime: 00:00:14
       Upstream Interface: Vlan-interface1
       List of 2 downstream interfaces
```

```
1:  Vlan-interface2
2:  Vlan-interface3
```

Table 9-3 Command output

Field	Description
Total 1 entries	Total number of (S, G) entries.
00001	Sequence number of the (S, G) entry.
(2001::2, FFE3::101)	(S, G) entry.
Uptime	Length of time for which the (S, G) entry has been up.
Upstream Interface	Upstream interface at which the (S, G) packets should arrive.
List of 2 downstream interfaces	List of downstream interfaces that forward (S, G) packets.

Related commands

reset ipv6 multicast routing-table

9.1.4. display ipv6 multicast rpf-info

Use **display ipv6 multicast rpf-info** to display RPF information for an IPv6 multicast source.

Syntax

display ipv6 multicast [**vpn-instance** *vpn-instance-name*] **rpf-info** *ipv6-source-address* [*ipv6-group-address*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command deletes all static multicast routes on the public network.*ipv6-source-address*: Specifies an IPv6 multicast source address.

ipv6-group-address: Specifies an IPv6 multicast group address in the range of FFxy::/16 (excluding FFx1::/16 and FFx2::/16), where "x" and "y" represent any hexadecimal numbers in the range of 0 to F.

Examples

Display RPF information for IPv6 multicast source 2001::101.

```
<Switch> display ipv6 multicast rpf-info 2001::101
 RPF information about source 2001::101:
     RPF interface: Vlan-interface1, RPF neighbor: FE80::A01:101:1
     Referenced prefix/prefix length: 2001::/64
     Referenced route type: igp
     Route selection rule: preference-preferred
```

```
Load splitting rule: disable
```

Table 9-4 Command output

Field	Description
RPF information about source 2001::101	RPF information of the IPv6 multicast source 2001::101.
RPF interface	Type and number of the RPF interface.
RPF neighbor	IPv6 address (link-local address) of the RPF neighbor.
Referenced prefix/prefix length	Referenced route and its prefix length.
Referenced route type	Type of the referenced route: • **igp**—IPv6 IGP unicast route. • **egp**—IPv6 EGP unicast route. • **unicast (direct)** —IPv6 directly connected unicast route. • **unicast**—Other IPv6 unicast route, such as IPv6 unicast static route. • **mbgp**—IPv6 MBGP route.
Route selection rule	RPF route selection rule: • Route preference. • Longest prefix match.
Load splitting rule	Whether load splitting is enabled.

Related commands

display ipv6 multicast forwarding-table

display ipv6 multicast routing-table

9.1.5. ipv6 multicast boundary

Use **ipv6 multicast boundary** to configure an IPv6 multicast forwarding boundary.

Use **undo ipv6 multicast boundary** to delete an IPv6 multicast forwarding boundary.

Syntax

ipv6 multicast boundary { *ipv6-group-address prefix-length* | **scope** { *scope-id* | **admin-local** | **global** | **organization-local** | **site-local** } }

undo ipv6 multicast boundary { *ipv6-group-address prefix-length*| **all** | **scope** { *scope-id* | **admin-local** | **global** | **organization-local** | **site-local** } }

Default

An interface is not an IPv6 multicast forwarding boundary.

Views

Interface view

Predefined user roles

network-admin

Parameters

ipv6-group-address: Specifies an IPv6 multicast group address in the range of FFxy::/16, where "x" and "y" represent any hexadecimal numbers in the range of 0 to F.

prefix-length: Specifies the address prefix length in the range of 8 to 128.

all: Specifies all IPv6 multicast boundaries configured on the interface.

scope-id: Specifies the ID of an admin-scoped zone, in the range of 3 to 15, which is identified by the scope field in the IPv6 multicast group address.

admin-local: Specifies the scoped zone as admin-local, which has a scope ID of 4.

global: Specifies the scoped zone as global, which has a scope ID of 14.

organization-local: Specifies the scoped zone as organization-local, which has a scope ID of 8.

site-local: Specifies the scoped zone as site-local, which has a scope ID of 5.

Usage guidelines

A multicast forwarding boundary sets the boundary condition for the IPv6 multicast groups in the specified address range. If the destination address of an IPv6 multicast packet matches the set boundary condition, the packet is not forwarded.

An interface can act as a forwarding boundary for multiple IPv6 multicast groups in different address ranges. You can implement this by using this command on the interface for each multicast address range. These multicast groups must be in the same scope. The latest configuration of a scope overwrites the previous one.

You do not need to enable IPv6 multicast routing before you execute this command.

Assume that Set A and Set B are both IPv6 multicast forwarding boundary sets with different address ranges, and that B is a subset of A. A takes effect on the interface no matter whether A is configured earlier or later than B.

Examples

Configure VLAN-interface 100 as the forwarding boundary of IPv6 multicast groups in the range of FF03::/16.

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ipv6 multicast boundary ff03:: 16
```

Configure VLAN-interface 100 as the forwarding boundary of IPv6 multicast groups in the admin-local scope.

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ipv6 multicast boundary scope 4
```

Related commands

display ipv6 multicast boundary

9.1.6. ipv6 multicast routing

Use **ipv6 multicast routing** to enable IPv6 multicast routing and enter IPv6 MRIB view.

Use **undo ipv6 multicast routing** to disable IPv6 multicast routing.

Syntax

ipv6 multicast routing [**vpn-instance** *vpn-instance-name*]

undo ipv6 multicast routing [**vpn-instance** *vpn-instance-name*]

Default

IPv6 multicast routing is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command deletes all static multicast routes on the public network.

Usage guidelines

Other Layer 3 IPv6 multicast commands take effect only when IPv6 multicast routing is enabled.

The device does not forward any IPv6 multicast packets before IPv6 multicast routing is enabled.

Examples

Enable IPv6 multicast routing and enter IPv6 MRIB view.

```
<Switch> system-view
[Switch] ipv6 multicast routing
[Switch-mrib6]
```

9.1.7. load-splitting (IPv6 MRIB view)

Use **load-splitting** to enable IPv6 multicast load splitting.

Use **multicast load-splitting** to restore the default.

Syntax

load-splitting { **source** | **source-group** }

undo load-splitting

Default

IPv6 multicast load splitting is disabled.

Views

IPv6 MRIB view

Predefined user roles

network-admin

Parameters

source: Enables IPv6 multicast load splitting based on IPv6 multicast source.

source-group: Enables IPv6 multicast load splitting based on IPv6 multicast source and group.

Examples

Enable IPv6 multicast load splitting based on IPv6 multicast source.

```
<Switch> system-view
[Switch] ipv6 multicast routing
[Switch-mrib6] load-splitting source
```

9.1.8. longest-match (IPv6 MRIB view)

Use **longest-match** to specify the longest prefix match principle for RPF route selection.

Use **undo longest-match** to restore the default.

Syntax

longest-match

undo longest-match

Default

Route preference is used for RPF route selection. The route with the highest route preference is used as the RPF route.

Views

IPv6 MRIB view

Predefined user roles

network-admin

Usage guidelines

This command enables the device to use the matching route with the longest prefix as the RPF route.

Examples

Specify the longest prefix match principle for RPF route selection.

```
<Switch> system-view
[Switch] ipv6 multicast routing
[Switch-mrib6] longest-match
```

9.1.9. reset ipv6 multicast forwarding-table

Use **reset ipv6 multicast forwarding-table** to clear IPv6 multicast forwarding entries.

Syntax

reset ipv6 multicast [**vpn-instance** *vpn-instance-name*] **forwarding-table** { { *ipv6-source-address* [*prefix-length*] | *ipv6-group-address* [*prefix-length*] | **incoming-interface** { *interface-type interface-number* } } * | **all** }

Views

User view

Predefined user roles

network-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command deletes all static multicast routes on the public network.*ipv6-source-address*: Specifies an IPv6 multicast source address.

ipv6-group-address: Specifies an IPv6 multicast group address in the range of FFxy::/16, where "x" and "y" represent any hexadecimal numbers in the range of 0 to F.

prefix-length: Specifies the address prefix length. The default value is 128. For an IPv6 multicast group address, the value range for this argument is 8 to 128. For an IPv6 multicast source address, the value range for this argument is 0 to 128.

incoming-interface: Specifies the IPv6 multicast forwarding entries that contain the specified incoming interface.

interface-type interface-number: Specifies an interface by its type and number.

all: Specifies all IPv6 multicast forwarding entries.

Usage guidelines

When you clear an IPv6 multicast forwarding entry, the associated IPv6 multicast routing entry is also cleared.

Examples

Clear IPv6 multicast forwarding entries for IPv6 multicast group FF0E::1.

```
<Switch> reset ipv6 multicast forwarding-table ff0e::1
```

Related commands

display ipv6 multicast forwarding-table

9.1.10. reset ipv6 multicast routing-table

Use **reset ipv6 multicast routing-table** to clear IPv6 multicast routing entries.

Syntax

reset ipv6 multicast [**vpn-instance** *vpn-instance-name*] **routing-table** { { *ipv6-source-address* [*prefix-length*] | *ipv6-group-address* [*prefix-length*] | **incoming-interface** *interface-type interface-number* } * | **all** }

Views

User view

Predefined user roles

network-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command deletes all static multicast routes on the public network.*ipv6-source-address*: Specifies an IPv6 multicast source address.

ipv6-group-address: Specifies an IPv6 multicast group address in the range of FFxy::/16, where "x" and "y" represent any hexadecimal numbers in the range of 0 to F.

prefix-length: Specifies an address prefix length. The default is 128. For an IPv6 multicast group address, the value range for this argument is 8 to 128. For an IPv6 multicast source address, the value range for this argument is 0 to 128.

incoming-interface: Specifies the IPv6 multicast routing entries that contain the specified incoming interface.

interface-type interface-number: Specifies an interface by its type and number.

all: Specifies all IPv6 multicast routing entries.

Usage guidelines

When you clear an IPv6 multicast routing entry, the associated IPv6 multicast forwarding entry is also cleared.

Examples

Clear IPv6 multicast routing entries for IPv6 multicast group FF03::101.

```
<Switch> reset ipv6 multicast routing-table ff03::101
```

Related commands

display ipv6 multicast routing-table

Contents

A page of this section is **6-x-x**

10. MLD commands 10-1
10.1. MLD commands 10-1
10.1.1. display mld group 10-1
10.1.2. display mld interface 10-5
10.1.3. display mld ssm-mapping 10-7
10.1.4. last-listener-query-interval (MLD view) 10-8
10.1.5. max-response-time (MLD view) 10-8
10.1.6. mld 10-9
10.1.7. mld enable 10-9
10.1.8. mld group-policy 10-10
10.1.9. mld last-listener-query-interval 10-11
10.1.10. mld max-response-time 10-12
10.1.11. mld other-querier-present-timeout 10-13
10.1.12. mld query-interval 10-13
10.1.13. mld robust-count 10-14
10.1.14. mld startup-query-count 10-15
10.1.15. mld startup-query-interval 10-15
10.1.16. mld static-group 10-16
10.1.17. mld version 10-17
10.1.18. other-querier-present-timeout (MLD view) 10-18
10.1.19. query-interval (MLD view) 10-18
10.1.20. reset mld group 10-19
10.1.21. robust-count (MLD view) 10-20
10.1.22. ssm-mapping (MLD view) 10-21
10.1.23. startup-query-count (MLD view) 10-21
10.1.24. startup-query-interval (MLD view) 10-22

10. MLD commands

MEMO:

The **vpn-instance** *vpn-instance-name* option for each command is supported by V7.2.18 and later software.

10.1. MLD commands

10.1.1. display mld group

Use **display mld group** to display information about MLD multicast groups (IPv6 multicast groups that hosts have joined through MLD).

Syntax

display mld [**vpn-instance** *vpn-instance-name*] **group** [*ipv6-group-address* | **interface** *interface-type interface-number*] [**static** | **verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command deletes all static multicast routes on the public network.

ipv6-group-address: Specifies an IPv6 multicast group address. The value range for this argument is FFxy::/16 (excluding FFx1::/16 and FFx2::/16), where "x" and "y" represent any hexadecimal numbers in the range of 0 to F. If you do not specify an IPv6 multicast group, this command displays information about all MLD multicast groups.

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays information about MLD multicast groups for all interfaces.

static: Specifies MLD multicast groups that hosts have joined statically. If you do not specify this keyword, the command displays information about MLD multicast groups that hosts have joined dynamically.

verbose: Displays detailed information about MLD multicast groups.

Examples

Display information about MLD multicast groups that hosts have dynamically joined.

```
<Switch> display mld group
MLD groups in total: 1
 Vlan-interface1(FE80::101):
```

```
MLD groups reported in total: 1
 Group address: FF03::101
  Last reporter: FE80::10
  Uptime: 00:02:04
  Expires: 00:01:15
```

Table 10-1 Command output

Field	Description
MLD groups in total	Total number of MLD multicast groups.
MLD groups reported in total	Total number of MLD multicast groups that the hosts attached to the interface have joined dynamically.
Group address	IPv6 multicast group address.
Last reporter	IPv6 address of the receiver host that last reported membership for the group.
Uptime	Length of time since the IPv6 multicast group was joined.
Expires	Remaining lifetime for the IPv6 multicast group. This field displays **Off** if the timer is disabled.

Display detailed information about MLD multicast group FF3E::101 that hosts have statically joined. In this example, the switch is configured with MLD SSM mappings.

```
<Switch> display mld group ff3e::101 verbose
 Vlan-interface1(FE80::101):
  MLD groups reported in total: 1
   Group: FF3E::101
     Uptime: 00:01:46
     Exclude expires: 00:04:16
     Mapping expires: 00:02:16
     Last reporter: FE80::10
     Last-listener-query-counter: 0
     Last-listener-query-timer-expiry: Off
     Mapping last-listener-query-counter: 0
     Mapping last-listener-query-timer-expiry: Off
     Group mode: Exclude
     Version1-host-present-timer-expiry: Off
     Source list (sources in total: 1):
       Source: 10::10
          Uptime: 00:00:09
          V2 expires: 00:04:11
          Mapping expires: 00:02:16
          Last-listener-query-counter: 0
          Last-listener-query-timer-expiry: Off
```

Table 10-2 Command output

Field	Description
MLD groups reported in total	Total number of MLD multicast groups that the hosts attached to the interface have joined dynamically.

Field	Description
Group	IPv6 multicast group address.
Uptime	Length of time since the IPv6 multicast group was reported.
Exclude expires	Remaining time for the IPv6 multicast group in Exclude mode. This field displays **Off** if the timer is disabled.
Mapping expires	Remaining time for the IPv6 multicast group specified in MLD SSM mappings. This field is displayed only when the device is configured with MLD SSM mappings.
Last reporter	IPv6 address of the receiver host that last reported membership for this group.
Last-listener-query-counter	Number of MLD multicast-address-specific queries or MLD multicast-address-and-source-specific queries sent for the group.
Last-listener-query-timer-expiry	Remaining time for the MLD last listener query timer for the multicast group. This field displays **Off** if the timer is disabled.
Mapping last-listener-query-counter	Number of MLD multicast-address-specific queries or MLD multicast-address-and-source-specific queries sent for the IPv6 multicast group specified in MLD SSM mappings. This field is displayed only when the device is configured with MLD SSM mappings.
Mapping last-listener-query-timer-expiry	Remaining time for the last listener query timer of the IPv6 multicast group specified in MLD SSM mappings. This field displays **Off** if the timer is disabled. This field is displayed only when the device is configured with MLD SSM mappings.
Group mode	IPv6 multicast source filtering mode: • **Include**—Include mode. • **Exclude**—Exclude mode. For a device that runs MLDv1: • If MLD SSM mappings are not configured, this field displays **Exclude**. • If MLD SSM mappings are configured, this field displays **Include** or **Exclude** depending on the SSM mappings and the IPv6 multicast groups that the host joins.
Version1-host-present-timer-expiry	Remaining time for the MLDv1 host present timer. This field displays **Off** if the timer is disabled. This field is displayed only when the device runs MLDv2.
Source list (sources in total 1)	List of IPv6 multicast sources and total number of IPv6 multicast sources. This field is displayed only when the device runs MLDv2 or is configured with MLD SSM mappings.
Source	IPv6 multicast source address. This field is displayed only when the device runs MLDv2 or the device is configured with MLD SSM mappings.

Field	Description
Uptime	Length of time since the IPv6 multicast source was reported. This field is displayed only when the device runs MLDv2 or is configured with MLD SSM mappings.
V2 expires	Remaining time for the IPv6 multicast source when the device runs MLDv2. This field displays **Off** if the timer is disabled. This field displays three hyphens (---) if the IPv6 multicast source is specified in MLD SSM mappings. This field is displayed only when the device runs MLDv2 or is configured with MLD SSM mappings.
Mapping expires	Remaining time for the IPv6 multicast sources specified in MLD SSM mappings.
Last-listener-query-counter	Number of MLD multicast-address-specific queries or MLD multicast-address-and-source-specific queries sent for the IPv6 multicast source and group. This field is displayed only when the device runs MLDv2 or is configured with MLD SSM mappings.
Last-listener-query-timer-expiry	Remaining time for the last listener query timer for the IPv6 multicast source and group. This field displays **Off** if the timer is disabled. This field is displayed only when the device runs MLDv2 or is configured with MLD SSM mappings.

Display information about the MLD multicast groups that hosts have statically joined.

```
<Switch> display mld group static
 Entries in total: 2
  (*, FF03::101)
   Interface: Vlan1
   Expires: Never

  (2001::101, FF3E::202)
   Interface: Vlan1
   Expires: Never
```

Table 10-3 Command output

Field	Description
Entries in total	Total number of the IPv6 multicast groups that hosts have joined statically.
(*, FF03::101)	(*, G) entry.
(2001::101, FF3E::202)	(S, G) entry.
Expires	Remaining lifetime for the IPv6 multicast group. This field always displays **Never**, which means that the IPv6 multicast group never expires.

Related commands

reset mld group

10.1.2. display mld interface

Use **display mld interface** to display MLD information for interfaces.

Syntax

display mld [**vpn-instance** *vpn-instance-name*] **interface** [*interface-type interface-number*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command deletes all static multicast routes on the public network.

interface-type interface-number: Specifies an interface by its type and number. If you do not specify an interface, this command displays MLD information for all interfaces.

verbose: Displays detailed MLD information.

Examples

Display detailed MLD information for VLAN-interface 1 (non-proxy interface).

```
<Switch> display mld interface vlan-interface 1 verbose
 Vlan-interface1(FE80::200:AFF:FE01:101):
   MLD is enabled.
   MLD version: 1
   Query interval for MLD: 125s
   Other querier present time for MLD: 255s
   Maximum query response time for MLD: 10s
   Last listener query interval: 1s
   Last listener query count: 2
   Startup query interval: 31s
   Startup query count: 2
   General query timer expiry (hh:mm:ss): 00:00:23
   Querier for MLD: FE80::200:AFF:FE01:101 (This router)
   MLD activity: 1 join(s), 0 done(s)
   IPv6 multicast routing on this interface: Enabled
   Robustness: 2
   Require-router-alert: Disabled
   Fast-leave: Disabled
   Startup-query: Off
   Other-querier-present-timer-expiry (hh:mm:ss): Off
   MLD groups reported in total: 1
```

Table 10-4 Command output

Field	Description
Vlan-interface1(FE80::200:AFF:FE01:101)	Interface and its IPv6 link-local address.
MLD is enabled	MLD is enabled on the interface.
MLD version	Version of MLD that the interface runs.
Query interval for MLD	MLD query interval, in seconds.
Other querier present time for MLD	MLD other querier present interval, in seconds.
Maximum query response time for MLD	Maximum response time for MLD general query messages, in seconds.
Last listener query interval	Interval for sending MLD multicast-address-specific queries or MLD multicast-address-and-source-specific queries, in seconds.
Last listener query count	Number of MLD multicast-address-specific queries or MLD multicast-address-and-source-specific queries sent for the group.
Startup query interval	MLD startup query interval, in seconds.
Startup query count	Number of MLD general queries sent on startup.
General query timer expiry	Remaining time for the MLD general query timer. This field displays **Off** if the timer is disabled.
Querier for MLD	IPv6 link-local address of the MLD querier.
MLD activity: 1 join(s), 0 done(s)	MLD activity statistics: • **join(s)**—Total number of IPv6 multicast groups that the interface has joined. • **done(s)**—Total number of IPv6 multicast groups that the interface has left.
IPv6 multicast routing on this interface	Whether IPv6 multicast routing is enabled: Enabled or Disabled.
Robustness	Robustness variable of the MLD querier.
Require-router-alert	Whether the feature of dropping MLD messages without Router-Alert is enabled: Enabled or Disabled.
Fast-leave	Whether fast-leave processing is enabled: Enabled or Disabled.
Startup-query	Whether the MLD querier sends MLD general queries at the startup query interval on startup: • **On**—The MLD querier performs the above action. • **Off**—The MLD querier does not perform the above action.
Other-querier-present-timer-expiry	Remaining time for MLD other querier present timer. This field displays **Off** if the timer is disabled.

Field	Description
MLD groups reported in total	Total number of IPv6 multicast groups that the interface has joined dynamically. This field is not displayed if the interface does not join IPv6 multicast groups.
MLD proxy is enabled	MLD proxying is enabled.
Version1-querier-present-timer-expiry	Remaining time for the MLDv1 querier present timer. This field displays **Off** if the timer is disabled.

10.1.3. display mld ssm-mapping

Use **display mld ssm-mapping** to display MLD SSM mappings.

Syntax

display mld [**vpn-instance** *vpn-instance-name*] **ssm-mapping** *ipv6-group-address*

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command deletes all static multicast routes on the public network.

ipv6-group-address: Specifies an IPv6 multicast group by its IPv6 address. The value range for this argument is FFxy::/16 (excluding FFx1::/16 and FFx2::/16), where "x" and "y" represent any hexadecimal numbers in the range of 0 to F.

Examples

Display MLD SSM mappings for IPv6 multicast group FF3E::101.

```
<Switch> display mld ssm-mapping ff3e::101
 Group: FF3E::101
 Source list:
        1::1
        1::2
        10::1
        100::10
```

Table 10-5 Command output

Field	Description
Group	IPv6 multicast group address.
Source list	List of IPv6 multicast source addresses.

10.1.4. last-listener-query-interval (MLD view)

Use **last-listener-query-interval** to set the MLD last listener query interval globally.

Use **undo last-listener-query-interval** to restore the default.

Syntax

last-listener-query-interval *interval*

undo last-listener-query-interval

Default

The MLD last listener query interval is 1 second.

Views

MLD view

Predefined user roles

network-admin

Parameters

interval: Specifies an MLD last listener query interval in the range of 1 to 25 seconds.

Usage guidelines

You can set the MLD last listener query interval globally for all interfaces in MLD view or for an interface in interface view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the global MLD last listener query interval to 6 seconds.

```
<Switch> system-view
[Switch] mld
[Switch-mld] last-listener-query-interval 6
```

Related commands

mld last-listener-query-interval

10.1.5. max-response-time (MLD view)

Use **max-response-time** to set the maximum response time for MLD general queries globally.

Use **undo max-response-time** to restore the default.

Syntax

max-response-time *time*

undo max-response-time

Default

The maximum response time for MLD general queries is 10 seconds.

Views

MLD view

Predefined user roles

network-admin

Parameters

time: Specifies the maximum response time for MLD general queries in the range of 1 to 3174 seconds.

Usage guidelines

You can set the maximum response time globally for all interfaces in MLD view or for an interface in interface view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the global maximum response time for MLD general queries to 25 seconds.

```
<Switch> system-view
[Switch] mld
[Switch-mld] max-response-time 25
```

Related commands

mld max-response-time

10.1.6. mld

Use **mld** to enter MLD view.

Use **undo mld** to delete the configurations in MLD view.

Syntax

mld [**vpn-instance** *vpn-instance-name*]

undo mld [**vpn-instance** *vpn-instance-name*]

Views

System view

Predefined user roles

network-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays multicast boundary information on the public network.

Examples

Enter MLD view.

```
<Switch> system-view
[Switch] mld
[Switch-mld]
```

10.1.7. mld enable

Use **mld enable** to enable MLD on an interface.

Use **undo mld enable** to disable MLD on an interface.

Syntax

mld enable

undo mld enable

Default

MLD is disabled on an interface.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

This command takes effect only when IPv6 multicast routing is enabled.

Other MLD configurations on the interface take effect only when MLD is enabled on the interface.

Examples

Enable IPv6 multicast routing, and enable MLD for VLAN-interface 100.

```
<Switch> system-view
[Switch] ipv6 multicast routing
[Switch-mrib6] quit
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] mld enable
```

Related commands

ipv6 multicast routing

10.1.8. mld group-policy

Use **mld group-policy** to configure an IPv6 multicast group policy on an interface to control the IPv6 multicast groups that hosts attached to the interface can join.

Use **undo mld group-policy** to delete the IPv6 multicast group policy on an interface.

Syntax

mld group-policy *ipv6-acl-number* [*version-number*]

undo mld group-policy

Default

No IPv6 multicast group policy exists. Hosts attached to the interface can join any IPv6 multicast groups.

Views

Interface view

Predefined user roles

network-admin

Parameters

ipv6-acl-number: Specifies an IPv6 basic or advanced ACL by its number in the range of 2000 to 3999. Receiver hosts can join only the IPv6 multicast groups that the ACL permits. If the ACL does not exist or have valid rules, receiver hosts cannot join IPv6 multicast groups.

version-number: Specifies an MLD version number, 1 or 2. By default, this command takes effect on both MLDv1 reports and MLDv2 reports.

Usage guidelines

An IPv6 multicast group policy filters MLD reports to control the IPv6 multicast groups that hosts can join.

This command does not take effect on static member interfaces because static member interfaces do not send MLD reports.

When you configure a rule in the IPv6 ACL, follow these restrictions and guidelines:

- For the rule to take effect, do not specify the **vpn-instance** *vpn-instance* option.
- In a basic ACL, the **source** *source-address source-prefix* option specifies an IPv6 multicast group address.
- In an advanced ACL, the **source** *source-address source-prefix* option specifies an IPv6 multicast source address. The **destination** *dest-address dest-prefix* option specifies an IPv6 multicast group address.

  To match the following MLD reports, set the **source** *source-address source-prefix* option to 0::0:
  - MLDv1 reports.
  - MLDv2 IS_EX and MLDv2 TO_EX reports that do not carry multicast source addresses.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure an IPv6 multicast group policy on VLAN-interface 100 so that hosts attached to the interface can join only IPv6 multicast group FF03::101.

```
<Switch> system-view
[Switch] acl ipv6 basic 2005
[Switch-acl-ipv6-basic-2005] rule permit source ff03::101 128
[Switch-acl-ipv6-basic-2005] quit
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] mld group-policy 2005
```

10.1.9. mld last-listener-query-interval

Use **mld last-listener-query-interval** to set the MLD last listener query interval on an interface.

Use **undo mld last-listener-query-interval** to restore the default.

Syntax

mld last-listener-query-interval *interval*

undo mld last-listener-query-interval

Default

The MLD last listener query interval is 1 second.

Views

Interface view

Predefined user roles

network-admin

Parameters

interval: Specifies an MLD last listener query interval in the range of 1 to 25 seconds.

Usage guidelines

You can set the MLD last listener query interval for an interface in interface view or globally for all interfaces in MLD view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the MLD last listener query interval to 6 seconds on VLAN-interface 100.

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] mld last-listener-query-interval 6
```

Related commands

last-listener-query-interval (MLD view)

10.1.10. mld max-response-time

Use **mld max-response-time** to set the maximum response time for MLD general queries on an interface.

Use **undo mld max-response-time** to restore the default.

Syntax

mld max-response-time *time*

undo mld max-response-time

Default

The maximum response time for MLD general queries is 10 seconds.

Views

Interface view

Predefined user roles

network-admin

Parameters

time: Specifies the maximum response time for MLD general queries, in the range of 1 to 3174 seconds.

Usage guidelines

You can set the maximum response time for an interface in interface view or globally for all interfaces in MLD view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the maximum response time for MLD general queries to 25 seconds on VLAN-interface 100.

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] mld max-response-time 25
```

Related commands

max-response-time (MLD view)

10.1.11. mld other-querier-present-timeout

Use **mld other-querier-present-timeout** to set the MLD other querier present timer on an interface.

Use **undo mld other-querier-present-timeout** to restore the default.

Syntax

mld other-querier-present-timeout *time*

undo mld other-querier-present-timeout

Default

The MLD other querier present timer is calculated by using the following formula:

[MLD general query interval] × [MLD querier's robustness variable] + [maximum response time for MLD general queries] / 2.

Views

Interface view

Predefined user roles

network-admin

Parameters

time: Specifies an MLD other querier present timer in the range of 1 to 31744 seconds.

Usage guidelines

You can set the MLD other querier present timer for an interface in interface view or globally for all interfaces in MLD view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the MLD other querier present timer to 125 seconds on VLAN-interface 100.

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] mld other-querier-present-timeout 125
```

Related commands

other-querier-present-timeout (MLD view)

10.1.12. mld query-interval

Use **mld query-interval** to set the MLD general query interval on an interface.

Use **undo mld query-interval** to restore the default.

Syntax

mld query-interval *interval*

undo mld query-interval

Default

The MLD general query interval is 125 seconds.

Views

Interface view

Predefined user roles

network-admin

Parameters

interval: Specifies an MLD general interval in the range of 1 to 31744 seconds.

Usage guidelines

You can set the MLD general interval for an interface in interface view or globally for all interfaces in MLD view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the MLD general query interval to 60 seconds on VLAN-interface 100.

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] mld query-interval 60
```

Related commands

query-interval (MLD view)

10.1.13. mld robust-count

Use **mld robust-count** to set the MLD querier's robustness variable on an interface.

Use **undo mld robust-count** to restore the default.

Syntax

mld robust-count *count*

undo mld robust-count

Default

The MLD querier's robustness variable is 2.

Views

Interface view

Predefined user roles

network-admin

Parameters

count: Specifies an MLD querier's robustness variable in the range of 1 to 255.

Usage guidelines

The MLD querier's robustness variable defines the number of times to retransmit MLD queries if packet loss occurs. A higher robustness variable makes the MLD querier more robust, but it increases the timeout time for IPv6 multicast groups.

You can set the MLD querier's robustness variable for an interface in interface view or globally for all interfaces in MLD view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the MLD querier's robustness variable to 5 on VLAN-interface 100.

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] mld robust-count 5
```

Related commands

robust-count (MLD view)

10.1.14. mld startup-query-count

Use **mld startup-query-count** to set the MLD startup query count on an interface.

Use **undo mld startup-query-count** to restore the default.

Syntax

mld startup-query-count *count*

undo mld startup-query-count

Default

The MLD startup query count equals the MLD querier's robustness variable.

Views

Interface view

Predefined user roles

network-admin

Parameters

count: Specifies an MLD startup query count in the range of 1 to 255.

Usage guidelines

You can set the MLD startup query count for an interface in interface view or globally for all interfaces in MLD view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the MLD startup query count to 5 on VLAN-interface 100.

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] mld startup-query-count 5
```

Related commands

startup-query-count (MLD view)

10.1.15. mld startup-query-interval

Use **mld startup-query-interval** to set the MLD startup query interval on an interface.

Use **undo mld startup-query-interval** to restore the default.

Syntax

mld startup-query-interval *interval*

undo mld startup-query-interval

Default

The MLD startup query interval equals one quarter of the MLD general query interval.

Views

Interface view

Predefined user roles

network-admin

Parameters

interval: Specifies an MLD startup query interval in the range of 1 to 31744 seconds.

Usage guidelines

You can set the MLD startup query interval for an interface in interface view or globally for all interfaces in MLD view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the MLD startup query interval to 100 seconds on VLAN-interface 100.

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] mld startup-query-interval 100
```

Related commands

startup-query-interval (MLD view)

10.1.16. mld static-group

Use **mld static-group** to configure an interface as a static group member of an IPv6 multicast group.

Use **undo mld static-group** to restore the default.

Syntax

mld static-group *ipv6-group-address* [**source** *ipv6-source-address*]

undo mld static-group { **all** | *ipv6-group-address* [**source** *ipv6-source-address*] }

Default

An interface is not a static member of IPv6 multicast groups.

Views

Interface view

Predefined user roles

network-admin

Parameters

ipv6-group-address: Specifies an IPv6 multicast group by its IPv6 address. The value range for this argument is FFxy::/16 (excluding FFx1::/16 and FFx2::/16), where "x" and "y" represent any hexadecimal numbers in the range of 0 to F.

ipv6-source-address: Specifies an IPv6 multicast source by its IPv6 address. If you do not specify an IPv6 multicast source, this command configures an interface as a static group member of the multicast groups with all IPv6 multicast source addresses.

all: Specifies all IPv6 multicast groups that the interface has statically joined.

Usage guidelines

For IPv6 multicast routing entries to be created, specify an IPv6 multicast source address if the specified IPv6 multicast group address is in the SSM group range.

Examples

Configure VLAN-interface 100 as a static group member of IPv6 multicast group FF03::101.

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] mld static-group ff03::101
```

Configure VLAN-interface 100 as a static group member of IPv6 multicast source and group (2001::101, FF3E::202).

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] mld static-group ff3e::202 source 2001::101
```

10.1.17. mld version

Use **mld version** to specify an MLD version for an interface.

Use **undo mld version** to restore the default.

Syntax

mld version *version-number*

undo mld version

Default

The MLD version is 1.

Views

Interface view

Predefined user roles

network-admin

Parameters

version-number: Specifies an MLD version, 1 or 2.

Examples

Specify MLD version 2 for VLAN-interface 100.

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] mld version 2
```

10.1.18. other-querier-present-timeout (MLD view)

Use **other-querier-present-timeout** to set the MLD other querier present timer globally.

Use **undo other-querier-present-timeout** to restore the default.

Syntax

other-querier-present-timeout *time*

undo other-querier-present-timeout

Default

The MLD other querier present timer is calculated by using the following formula:

[MLD general query interval] × [MLD querier's robustness variable] + [maximum response time for MLD general queries] / 2.

Views

MLD view

Predefined user roles

network-admin

Parameters

time: Specifies an MLD other querier present timer in the range of 1 to 31744 seconds.

Usage guidelines

You can set the MLD other querier present timer globally for all interfaces in MLD view or for an interface in interface view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the global MLD other querier present timer to 125 seconds.

```
<Switch> system-view
[Switch] mld
[Switch-mld] other-querier-present-timeout 125
```

Related commands

mld other-querier-present-timeout

10.1.19. query-interval (MLD view)

Use **query-interval** to set the MLD general query interval globally.

Use **undo query-interval** to restore the default.

Syntax

query-interval *interval*

undo query-interval

Default

The MLD general query interval is 125 seconds.

Views

MLD view

Predefined user roles

network-admin

Parameters

interval: Specifies an MLD general query interval in the range of 1 to 31744 seconds.

Usage guidelines

You can set the MLD general query interval globally for all interfaces in MLD view or for an interface in interface view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the global MLD general query interval to 60 seconds.

```
<Switch> system-view
[Switch] mld
[Switch-mld] query-interval 60
```

Related commands

mld query-interval

10.1.20. reset mld group

Use **reset mld group** to clear dynamic MLD multicast group entries.

Syntax

reset mld [**vpn-instance** *vpn-instance-name*] **group** { **all** | **interface** *interface-type interface-number* { **all** | *ipv6-group-address* [*prefix-length*] [*ipv6-source-address* [*prefix-length*]] } }

Views

User view

Predefined user roles

network-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays multicast boundary information on the public network.

all: The first **all** specifies all interfaces, and the second **all** specifies all MLD multicast groups.

interface-type interface-number: Specifies an interface by its type and number.

ipv6-group-address: Specifies an IPv6 multicast group by its IPv6 address. The value range for this argument is FFxy::/16 (excluding FFx1::/16 and FFx2::/16), where "x" and "y" represent any hexadecimal numbers in the range of 0 to F.

ipv6-source-address: Specifies an IPv6 multicast source by its IPv6 address. If you do not specify an IPv6 multicast source, this command clears dynamic MLD multicast group entries for all IPv6 multicast sources.

prefix-length: Specifies an address prefix length. The default is 128. For a multicast source address, the value range for this argument is 0 to 128. For a multicast group address, the value range for this argument is 8 to 128.

Usage guidelines

This command might interrupt the IPv6 multicast information transmission.

Examples

Clear dynamic MLD multicast group entries for all interfaces.

```
<Switch> reset mld group all
```

Clear all dynamic MLD multicast group entries for VLAN-interface 100.

```
<Switch> reset mld group interface vlan-interface 100 all
```

Clear the dynamic entry of MLD multicast group FF03::101:10 for VLAN-interface 100.

```
<Switch> reset mld group interface vlan-interface 100 ff03::101:10
```

Related commands

display mld group

10.1.21. robust-count (MLD view)

Use **robust-count** to set the MLD querier's robustness variable globally.

Use **undo robust-count** to restore the default.

Syntax

robust-count *count*

undo robust-count

Default

The MLD querier's robustness variable is 2.

Views

MLD view

Predefined user roles

network-admin

Parameters

count: Specifies an MLD querier's robustness variable in the range of 1 to 255.

Usage guidelines

The MLD querier's robustness variable defines the number of times to retransmit MLD queries if packet loss occurs. A higher robustness variable makes the MLD querier more robust, but it increases the timeout time for IPv6 multicast groups.

You can set the MLD querier's robustness variable globally for all interfaces in MLD view or for an interface in interface view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the global MLD querier's robustness variable to 5.

```
<Switch> system-view
[Switch] mld
[Switch-mld] robust-count 5
```

Related commands

mld robust-count

10.1.22. ssm-mapping (MLD view)

Use **ssm-mapping** to configure an MLD SSM mapping.

Use **undo ssm-mapping** to delete MLD SSM mappings.

Syntax

ssm-mapping *ipv6-source-address ipv6-acl-number*

undo ssm-mapping { *ipv6-source-address* | **all** }

Default

No MLD SSM mappings exist.

Views

MLD view

Predefined user roles

network-admin

Parameters

ipv6-source-address: Specifies an IPv6 multicast source by its IPv6 address.

ipv6-acl-number: Specifies an IPv6 basic ACL number in the range of 2000 to 2999. IPv6 multicast groups in MLD reports permitted by the ACL are associated with the IPv6 multicast source. If the ACL does not exist or does not have valid rules, no IPv6 multicast groups are associated with the IPv6 multicast source.

all: Specifies all MLD SSM mappings.

Usage guidelines

When you configure a rule in the IPv6 basic ACL, follow these restrictions and guidelines:

- For the rule to take effect, do not specify the **vpn-instance** *vpn-instance* option.
- The **source** *source-address source-prefix* **option specifies an** IPv6 multicast group address.
- Among the other optional parameters, only the **fragment keyword and the time-range** *time-range-name* option take effect.

Examples

Configure an MLD SSM mapping with IPv6 multicast source 1::1 and IPv6 multicast group range FF3E::/64.

```
<Switch> system-view
[Switch] acl ipv6 basic 2001
[Switch-acl-ipv6-basic-2001] rule permit source ff3e:: 64
[Switch-acl-ipv6-basic-2001] quit
[Switch] mld
[Switch-mld] ssm-mapping 1::1 2001
```

Related commands

display mld ssm-mapping

10.1.23. startup-query-count (MLD view)

Use **startup-query-count** to set the MLD startup query count globally.

Use **undo startup-query-count** to restore the default.

Syntax

startup-query-count *count*

undo startup-query-count

Default

The MLD startup query count equals the MLD querier's robustness variable.

Views

MLD view

Predefined user roles

network-admin

Parameters

count: Specifies an MLD startup query count in the range of 1 to 255.

Usage guidelines

You can set the MLD startup query count globally for all interfaces in MLD view or for an interface in interface view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the global MLD startup query count to 5.

```
<Switch> system-view
[Switch] mld
[Switch-mld] startup-query-count 5
```

Related commands

mld startup-query-count

10.1.24. startup-query-interval (MLD view)

Use **startup-query-interval** to set the MLD startup query interval globally.

Use **undo startup-query-interval** to restore the default.

Syntax

startup-query-interval *interval*

undo startup-query-interval

Default

The MLD startup query interval equals one quarter of the MLD general query interval.

Views

MLD view

Predefined user roles

network-admin

Parameters

interval: Specifies an MLD startup query interval in the range of 1 to 31744 seconds.

Usage guidelines

You can set the MLD startup query interval globally for all interfaces in MLD view or for an interface in interface view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the global MLD startup query interval to 100 seconds.

```
<Switch> system-view
[Switch] mld
[Switch-mld] startup-query-interval 100
```

Related commands

mld startup-query-interval

Contents

A page of this section is **6-x-x**

11. IPv6 PIM commands 11-1
11.1. IPv6 PIM commands 11-1
11.1.1. bsm-reflection enable (IPv6 PIM view) 11-1
11.1.2. bsr-policy (IPv6 PIM view) 11-1
11.1.3. c-bsr (IPv6 PIM view) 11-2
11.1.4. c-rp (IPv6 PIM view) 11-3
11.1.5. crp-policy (IPv6 PIM view) 11-4
11.1.6. display ipv6 pim bsr-info 11-5
11.1.7. display ipv6 pim claimed-route 11-7
11.1.8. display ipv6 pim c-rp 11-8
11.1.9. display ipv6 pim interface 11-9
11.1.10. display ipv6 pim neighbor 11-12
11.1.11. display ipv6 pim routing-table 11-13
11.1.12. display ipv6 pim rp-info 11-17
11.1.13. hello-option dr-priority (IPv6 PIM view) 11-19
11.1.14. hello-option holdtime (IPv6 PIM view) 11-20
11.1.15. hello-option lan-delay (IPv6 PIM view) 11-20
11.1.16. hello-option neighbor-tracking (IPv6 PIM view) 11-21
11.1.17. hello-option override-interval (IPv6 PIM view) 11-22
11.1.18. holdtime join-prune (IPv6 PIM view) 11-22
11.1.19. ipv6 pim 11-23
11.1.20. ipv6 pim bsr-boundary 11-24
11.1.21. ipv6 pim hello-option dr-priority 11-24
11.1.22. ipv6 pim hello-option holdtime 11-25
11.1.23. ipv6 pim hello-option lan-delay 11-26
11.1.24. ipv6 pim hello-option neighbor-tracking 11-26
11.1.25. ipv6 pim hello-option override-interval 11-27
11.1.26. ipv6 pim holdtime join-prune 11-28
11.1.27. ipv6 pim neighbor-policy 11-29
11.1.28. ipv6 pim require-genid 11-30
11.1.29. ipv6 pim sm 11-30
11.1.30. ipv6 pim state-refresh-capable 11-31
11.1.31. ipv6 pim timer hello 11-31
11.1.32. ipv6 pim timer join-prune 11-32
11.1.33. ipv6 pim triggered-hello-delay 11-33
11.1.34. jp-pkt-size (IPv6 PIM view) 11-33
11.1.35. register-policy (IPv6 PIM view) 11-34
11.1.36. register-whole-checksum (IPv6 PIM view) 11-35
11.1.37. snmp-agent trap enable pim6 11-35
11.1.38. source-lifetime (IPv6 PIM view) 11-36
11.1.39. source-policy (IPv6 PIM view) 11-37
11.1.40. spt-switch-threshold (IPv6 PIM view) 11-38
11.1.41. ssm-policy (IPv6 PIM view) 11-39
11.1.42. state-refresh-hoplimit (IPv6 PIM view) 11-40
11.1.43. state-refresh-interval (IPv6 PIM view) 11-40
11.1.44. state-refresh-rate-limit (IPv6 PIM view) 11-41
11.1.45. static-rp (IPv6 PIM view) 11-42
11.1.46. timer hello (IPv6 PIM view) 11-43
11.1.47. timer join-prune (IPv6 PIM view) 11-43

11. IPv6 PIM commands

MEMO:

The **vpn-instance** *vpn-instance-name* option for each command is supported by V7.2.18 and later software.

11.1. IPv6 PIM commands

11.1.1. bsm-reflection enable (IPv6 PIM view)

Use **bsm-reflection enable** to enable the device to forward BSMs out of their incoming interfaces.

Use **undo bsm-reflection enable** to disable the device from forwarding BSMs out of their incoming interfaces.

Syntax

bsm-reflection enable

undo bsm-reflection enable

Default

The device forwards BSMs out of their incoming interfaces.

Views

IPv6 PIM view

Predefined user roles

network-admin

Usage guidelines

Disable this feature if all the routers in the IPv6 PIM-SM domain have consistent routing information.

Examples

Disable the device from forwarding BSMs out of their incoming interfaces.

```
<Switch> system-view
[Switch] ipv6 pim
[Switch-pim6] undo bsm-reflection enable
```

11.1.2. bsr-policy (IPv6 PIM view)

Use **bsr-policy** to configure a BSR policy.

Use **undo bsr-policy** to restore the default.

Syntax

bsr-policy *ipv6-acl-number*

undo bsr-policy

Default

No BSR policy exists, and all bootstrap messages are regarded as legal.

Views

IPv6 PIM view

Predefined user roles

network-admin

Parameters

ipv6-acl-number: Specifies an IPv6 basic ACL by its number in the range of 2000 to 2999.

Usage guidelines

A BSR policy filters bootstrap messages to guard against BSR spoofing.

When you configure a rule in the IPv6 basic ACL, follow these restrictions and guidelines:

- For the rule to take effect, do not specify the **vpn-instance** *vpn-instance* option.
- The **source** *source-address source-prefix* option specifies a BSR address.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure a BSR policy so that only the devices on subnet 2001::2/64 can act as the BSR.

```
<Switch> system-view
[Switch] acl ipv6 basic 2000
[Switch-acl-ipv6-basic-2000] rule permit source 2001::2 64
[Switch-acl-ipv6-basic-2000] quit
[Switch] ipv6 pim
[Switch-pim6] bsr-policy 2000
```

Related commands

c-bsr (IPv6 PIM view)

11.1.3. c-bsr (IPv6 PIM view)

Use **c-bsr** to configure a candidate-BSR (C-BSR).

Use **undo c-bsr** to remove the configuration of a C-BSR.

Syntax

c-bsr *ipv6-address* [**scope** *scope-id*] [**hash-length** *hash-length* | **priority** *priority*] *

undo c-bsr *ipv6-address* [**scope** *scope-id*]

Default

No C-BSRs exist.

Views

IPv6 PIM view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies the IPv6 address of a C-BSR. You must specify the IPv6 address of a local IPv6 PIM interface.

scope *scope-id*: Specifies an IPv6 admin-scoped zone by its ID in the range of 3 to 15. If you do not specify an IPv6 admin-scoped zone, this command designates the C-BSR to the global-scoped zone.

hash-length *hash-length*: Specifies a hash mask length in the range of 0 to 128. The default is 126.

priority *priority*: Specifies a C-BSR priority in the range of 0 to 255. The default is 64. The greater the value, the higher the priority.

Usage guidelines

If you execute this command for a zone multiple times, the most recent configuration takes effect.

You can configure the same C-BSR for different zones.

Examples

Configure the interface with IPv6 address 1101::1 as a C-BSR for the global-scoped zone.

```
<Switch> system-view
[Switch] ipv6 pim
[Switch-pim6] c-bsr 1101::1
```

11.1.4. c-rp (IPv6 PIM view)

Use **c-rp** to configure a candidate-RP (C-RP).

Use **undo c-rp** to remove the configuration of a C-RP.

Syntax

c-rp *ipv6-address* [**advertisement-interval** *adv-interval* | { **group-policy** *ipv6-acl-number* | **scope** *scope-id* } | **holdtime** *hold-time* | **priority** *priority*] *

undo c-rp *ipv6-address*

Default

No C-RPs exist.

Views

IPv6 PIM view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies the IPv6 address of a C-RP. You must specify the IPv6 address of a local IPv6 PIM interface.

advertisement-interval *adv-interval*: Specifies a C-RP advertisement message interval in the range of 1 to 65535 seconds. The default is 60 seconds.

group-policy *ipv6-acl-number*: Specifies an IPv6 basic ACL number by its number in the range of 2000 to 2999. If you specify an ACL, this command designates the C-RP to IPv6 multicast groups in C-RP advertisement messages that the ACL permits. The C-RP is designated to all IPv6 multicast groups when one of the following conditions exists:

- You do not specify an ACL.
- The specified ACL does not exist.
- The specified ACL does not have valid rules.

scope *scope-id:* Specifies an IPv6 admin-scoped zone by its ID in the range of 3 to 15.

holdtime *hold-time*: Specifies a C-RP lifetime in the range of 1 to 65535 seconds. The default is 150 seconds.

priority *priority*: Specifies a C-RP priority in the range of 0 to 255. The default is 192. The greater the value, the lower the priority.

Usage guidelines

To designate a C-RP to multiple IPv6 multicast group ranges, create multiple rules that specify different IPv6 multicast group ranges in the ACL.

When you configure a rule in the IPv6 basic ACL, follow these restrictions and guidelines:

- For the rule to take effect, do not specify the **vpn-instance** *vpn-instance* option.
- The **source** *source-address source-prefix* option specifies an IPv6 multicast group range.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

If you execute this command by using the same IPv6 address of a C-RP multiple times, the most recent configuration takes effect.

Examples

Configure the interface with IPv6 address 2001::1 as the C-RP for IPv6 multicast group range FF0E:0:1391::/96, and set its priority to 10.

```
<Switch> system-view
[Switch] acl ipv6 basic 2000
[Switch-acl-ipv6-basic-2000] rule permit source ff0e:0:1391:: 96
[Switch-acl-ipv6-basic-2000] quit
[Switch] ipv6 pim
[Switch-pim6] c-rp 2001::1 group-policy 2000 priority 10
```

11.1.5. crp-policy (IPv6 PIM view)

Use **crp-policy** to configure a C-RP policy.

Use **undo crp-policy** to restore the default.

Syntax

crp-policy *ipv6-acl-number*

undo crp-policy

Default

No C-RP policy exists, and all C-RP messages are regarded as legal.

Views

IPv6 PIM view

Predefined user roles

network-admin

Parameters

ipv6-acl-number: Specifies an IPv6 advanced ACL number in the range of 3000 to 3999.

Usage guidelines

A C-RP policy filters C-RP advertisement messages to guard against C-RP spoofing.

The device uses only the prefixes of the multicast group ranges in advertisement messages to match the destination field in ACL rules. For example, the IPv6 multicast group range in a C-RP advertisement message is FF0E:0:1::/96. If the prefix FF0E:0:1:: is in the range specified by the destination field of an ACL rule, the specified C-RPs are designated to this IPv6 multicast group range.

When you configure a rule in the IPv6 ACL, follow these restrictions and guidelines:

- For the rule to take effect, do not specify the **vpn-instance** *vpn-instance* option.
- The **source** *source-address source-prefix* option specifies an RP address.
- The **destination** *dest-address dest-prefix* option specifies an IPv6 multicast group address.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure a C-RP policy so that only devices in the address range of 2001::2/64 can be C-RPs for the groups in the range of FF03::101/64.

```
<Switch> system-view
[Switch] acl ipv6 advanced 3000
[Switch-acl-ipv6-adv-3000] rule permit ipv6 source 2001::2 64 destination ff03::101 64
[Switch-acl-ipv6-adv-3000] quit
[Switch] ipv6 pim
[Switch-pim6] crp-policy 3000
```

Related commands

c-rp (IPv6 PIM view)

11.1.6. display ipv6 pim bsr-info

Use **display ipv6 pim bsr-info** to display IPv6 PIM BSR information.

Syntax

display ipv6 pim [**vpn-instance** *vpn-instance-name*] **bsr-info**

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command deletes all static multicast routes on the public network.

Examples

Display IPv6 PIM BSR information.

```
<Switch> display ipv6 pim bsr-info
 Scope: non-scoped
     State: Accept Preferred
     Bootstrap timer: 00:01:44
     Elected BSR address: 12:12::1
       Priority: 64
       Hash mask length: 126
       Uptime: 00:21:56

 Scope: 5
     State: Accept Any
     Scope-zone expiry timer: 00:21:12

 Scope: 6
     State: Elected
     Bootstrap timer: 00:00:26
     Elected BSR address: 17:11::1
       Priority: 64
       Hash mask length: 126
       Uptime: 02:53:37
     Candidate BSR address: 17:11::1
       Priority: 64
       Hash mask length: 126

 Scope: 7
     State: Candidate
     Bootstrap timer: 00:01:56
     Elected BSR address: 61:37::1
       Priority: 64
       Hash mask length: 126
       Uptime: 02:53:32
     Candidate BSR address: 17:12::1
       Priority: 64
       Hash mask length: 126

 Scope: 8
     State: Pending
     Bootstrap timer: 00:00:07
     Candidate BSR address: 17:13::1
       Priority: 64
```

```
Hash mask length: 126
```

Table 11-1 Command output

Field	Description
Bootstrap timer	Aging timer for the BSR.
Scope-zone expiry timer	Aging timer for the scoped zone.
Elected BSR address	Address of the elected BSR.
Candidate BSR address	Address of the C-BSR.
Priority	BSR priority.
Uptime	Length of time the BSR has been up.

11.1.7. display ipv6 pim claimed-route

Use **display ipv6 pim claimed-route** to display information about all routes that IPv6 PIM uses.

Syntax

display ipv6 pim [**vpn-instance** *vpn-instance-name*] **claimed-route** [*ipv6-source-address*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command deletes all static multicast routes on the public network.

ipv6-source-address: Specifies an IPv6 multicast source by its IPv6 address. If you do not specify an IPv6 multicast source, this command displays information about all routes that IPv6 PIM uses.

Examples

Display information about all routes that IPv6 PIM uses.

```
<Switch> display ipv6 pim claimed-route
 RPF-route selecting rule: longest-match

 Route/mask: 7:11::/64 (unicast (direct))
     RPF interface: Vlan-interface2, RPF neighbor: 8::2
     Total number of (S,G) or (*,G) dependent on this route entry: 4
     (7:11::10, ff1e::1)
     (7:11::10, ff1e::2)
     (7:11::10, ff1e::3)
     (*, ff1e::4)
 Route/mask: 7:12::/64 (unicast)
```

```
RPF interface: Vlan-interface2, RPF neighbor: 8::3,
Total number of (S,G) or (*,G) dependent on this route entry: 2
(7:12::10, ff1e::1)
(7:12::10, ff1e::2)
```

Table 11-2 Command output

Field	Description
Route/mask	Route entry. Route types in parentheses include: • **igp**—IGP unicast route. • **egp**—EGP unicast route. • **unicast (direct)**—Directly connected unicast route. • **unicast**—Other unicast route, such as static unicast route. • **mbgp**—IPv6 MBGP route.
RPF interface	Name of the RPF interface.
RPF neighbor	IPv6 address of the RPF neighbor.
Total number of (S,G) or (*,G) dependent on this route entry	Total number (S, G) or (*, G) entries associated with the RPF route and the entry list.

11.1.8. display ipv6 pim c-rp

Use **display ipv6 pim c-rp** to display C-RP information.

Syntax

display ipv6 pim [**vpn-instance** *vpn-instance-name*] **c-rp** [**local**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command deletes all static multicast routes on the public network.

local: Specifies local C-RPs. If you do not specify this keyword, the command displays information about all C-RPs.

Usage guidelines

You can display information about learned C-RPs only on the BSR. On other devices, you can display information about the locally configured C-RPs.

Examples

Display information about learned C-RPs.

```
<Switch> display ipv6 pim c-rp
 Scope: non-scoped
     Group/MaskLen: FF00::/8 [B]
```

```
  C-RP address             Priority  HoldTime  Uptime    Expires
  8:12::2 (local)          192       150       00:27:48  00:01:43
Group/MaskLen: FF23::/92 Expires: 00:02:07
```

Display information about the locally configured C-RPs.

```
<Switch> display ipv6 pim c-rp local
 Candidate RP: 8:12::2(Loop1)
     Priority: 192
     HoldTime: 150
     Advertisement interval: 60
     Next advertisement scheduled at: 00:00:46
```

Table 11-3 Command output

Field	Description
Group/MaskLen	IPv6 multicast group to which the C-RP is designated.
[B]	This field is not supported in the current software version. The C-RP is an IPv6 BIDIR-PIM RP. This field is not displayed if the C-RP is an IPv6 PIM-SM RP.
C-RP address	IPv6 address of the C-RP. If the C-RP resides on the device where the command is executed, this field displays **(local)** after the IPv6 address.
Priority	C-RP priority.
HoldTime	C-RP lifetime.
Uptime	Length of time the C-RP has been up: • **w**—Weeks. • **d**—Days. • **h**—Hours.
Expires	Remaining lifetime for the C-RP and the IPv6 multicast group.
Candidate RP	IPv6 address of the locally configured C-RP.
Advertisement interval	Interval between two advertisement messages sent by the locally configured C-RP.
Next advertisement scheduled at	Remaining time for the locally configured C-RP to send the next advertisement message.

11.1.9. display ipv6 pim interface

Use **display ipv6 pim** [**vpn-instance** *vpn-instance-name*] **interface** to display IPv6 PIM information for interfaces.

Syntax

display ipv6 pim interface [*interface-type interface-number*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command deletes all static multicast routes on the public network.

interface-type interface-number: Specifies an interface by its type and number. If you do not specify an interface, this command displays IPv6 PIM information for all interfaces.

verbose: Displays detailed IPv6 PIM information. If you do not specify this keyword, the command displays brief IPv6 PIM information.

Examples

Display brief IPv6 PIM information for all interfaces.

```
<Switch> display ipv6 pim interface
 Interface          NbrCnt  HelloInt  DR-Pri     DR-Address
 Vlan1              1       30        1          FE80::200:5EFF:FE04:8700
```

Table 11-4 Command output

Field	Description
Interface	Name of the interface.
NbrCnt	Number of IPv6 PIM neighbors.
HelloInt	Interval for sending hello messages.
DR-Pri	DR priority.
DR-Address	IPv6 address (link-local address) of the DR.

Display detailed IPv6 PIM information on VLAN-interface 1.

```
<Switch> display ipv6 pim interface vlan-interface 1 verbose
 Interface: Vlan-interface1, FE80::200:5EFF:FE04:8700
     PIM version: 2
     PIM mode: Sparse
     PIM DR: FE80::200:AFF:FE01:101
     PIM DR Priority (configured): 1
     PIM neighbors count: 1
     PIM hello interval: 30 s
     PIM LAN delay (negotiated): 500 ms
     PIM LAN delay (configured): 500 ms
     PIM override interval (negotiated): 2500 ms
     PIM override interval (configured): 2500 ms
     PIM neighbor tracking (negotiated): disabled
     PIM neighbor tracking (configured): disabled
     PIM generation ID: 0xF5712241
     PIM require generation ID: disabled
     PIM hello hold interval: 105 s
     PIM assert hold interval: 180 s
     PIM triggered hello delay: 5 s
     PIM J/P interval: 60 s
     PIM J/P hold interval: 210 s
     PIM BSR domain border: disabled
     PIM BFD: disabled
```

```
PIM passive: disabled
Number of routers on network not using DR priority: 0
Number of routers on network not using LAN delay: 0
Number of routers on network not using neighbor tracking: 2
```

Table 11-5 Command output

Field	Description
Interface	Interface name and IPv6 address (link-local address).
PIM version	Version of the IPv6 PIM protocol
PIM mode	IPv6 PIM mode: dense or sparse.
PIM DR	IPv6 address (link-local address) of the DR.
PIM DR Priority (configured)	Configured DR priority.
PIM neighbor count	Total number of IPv6 PIM neighbors.
PIM hello interval	Interval for sending hello messages.
PIM LAN delay (negotiated)	Negotiated IPv6 message propagation delay.
PIM LAN delay (configured)	Configured IPv6 message propagation delay.
PIM override interval (negotiated)	Negotiated interval for overriding prune messages.
PIM override interval (configured)	Configured interval for overriding prune messages.
PIM neighbor tracking (negotiated)	Negotiated neighbor tracking status: enabled or disabled.
PIM neighbor tracking (configured)	Configured neighbor tracking status: enabled or disabled.
PIM require generation ID	Whether the feature of dropping hello messages without Generation_ID is enabled.
PIM hello hold interval	IPv6 PIM neighbor lifetime.
PIM assert hold interval	Assert holdtime timer.
PIM triggered hello delay	Maximum delay for sending hello messages.
PIM J/P interval	Interval for sending join/prune messages.
PIM J/P hold interval	Joined/pruned state holdtime timer.
PIM BSR domain border	Whether an IPv6 PIM domain border is configured.
PIM BFD	Whether IPv6 PIM is enabled to work with BFD.
PIM passive	Whether IPv6 PIM passive mode is enabled on the interface.
Number of routers on network not using DR priority	Number of routers that do not use the DR priority field on the subnet where the interface resides.
Number of routers on network not using LAN delay	Number of routers that do not use the LAN delay field on the subnet where the interface resides.
Number of routers on network not using neighbor tracking	Number of routers that are not enabled with neighbor tracking on the subnet where the interface resides.

11.1.10. display ipv6 pim neighbor

Use **display ipv6 pim neighbor** to display IPv6 PIM neighbor information.

Syntax

display ipv6 pim [**vpn-instance** *vpn-instance-name*] **neighbor** [*ipv6-neighbor-address* | **interface** *interface-type interface-number* | **verbose**] *

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command deletes all static multicast routes on the public network.

ipv6-neighbor-address: Specifies an IPv6 PIM neighbor by its IPv6 address. If you do not specify an IPv6 PIM neighbor, this command displays information about all IPv6 PIM neighbors.

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays information about IPv6 PIM neighbors on all interfaces.

verbose: Displays detailed IPv6 PIM neighbor information. If you do not specify this keyword, the command displays brief IPv6 PIM neighbor information.

Examples

Display brief information about all IPv6 PIM neighbors.

```
<Switch> display ipv6 pim neighbor
 Total Number of Neighbors = 2

 Neighbor        Interface           Uptime   Expires  DR-Priority Mode
 FE80::A01:101:1  Vlan1              02:50:49 00:01:31 1           B
 FE80::A01:102:1  Vlan2              02:49:39 00:01:42 1
```

Display detailed information about the IPv6 PIM neighbor with IPv6 address FE80::A01:101:1.

```
<Switch> display ipv6 pim neighbor fe80::a01:101:1 verbose
 Neighbor: FE80::A01:101:1
     Interface: Vlan-interface3
     Uptime: 00:00:10
     Expiry time: 00:00:30
     DR Priority: 1
     Generation ID: 0x2ACEFE15
     Holdtime: 105 s
     LAN delay: 500 ms
     Override interval: 2500 ms
     State refresh interval: 60 s
     Neighbor tracking: Disabled
```

```
Bidirectional PIM: Disabled
Secondary address(es):
1::1
```

Table 11-6 Command output

Field	Description
Total Number of Neighbors	Total number of IPv6 PIM neighbors.
Neighbor	Primary IPv6 address (link-local address) of the IPv6 PIM neighbor.
Interface	Interface that connects to the IPv6 PIM neighbor.
Uptime	Length of time the IPv6 PIM neighbor has been up.
Expires/Expiry time	Remaining lifetime for the IPv6 PIM neighbor. If the IPv6 PIM neighbor is always up and reachable, this field displays **never**.
DR-Priority/DR Priority	DR priority of the IPv6 PIM neighbor.
Mode	IPv6 PIM mode. This field displays **B** if the IPv6 PIM mode is BIDIR-PIM.IPv6 BIDIR-PIM is not supported in the current software version. This field is empty if an IPv6 PIM mode other than IPv6 BIDIR-PIM is used.
Generation ID	Generation ID of the IPv6 PIM neighbor. (A random value represents a status change of the IPv6 PIM neighbor.)
Holdtime	Lifetime of the IPv6 PIM neighbor. If the IPv6 PIM neighbor is always up and reachable, this field displays **forever**.
LAN delay	IPv6 PIM message propagation delay on the shared-media LAN.
Override interval	Interval for overriding prune messages.
State refresh interval	Interval for refreshing state. This field is displayed only when the state refresh feature is enabled.
Neighbor tracking	Neighbor tracking status: enabled or disabled.
Bidirectional PIM	This field is not supported in the current software version. Whether IPv6 BIDIR-PIM is enabled.
RPF proxy vector	Whether the RPF proxy vector feature is enabled.
Secondary address(es)	Secondary IPv6 address (non-link-local address) of the IPv6 PIM neighbor.

11.1.11. display ipv6 pim routing-table

Use **display ipv6 pim routing-table** to display IPv6 PIM routing entries.

Syntax

display ipv6 pim [**vpn-instance** *vpn-instance-name*] **routing-table** [*ipv6-group-address* [*prefix-length*] | *ipv6-source-address* [*prefix-length*] | **flags** *flag-value* | **fsm** | **incoming-interface**

interface-type interface-number | **mode** *mode-type* | **outgoing-interface** { **exclude** | **include** | **match** } *interface-type interface-number*] *

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ipv6-group-address: Specifies an IPv6 multicast group address. The value range for this argument is FFxy::/16, where "x" and "y" represent any hexadecimal numbers in the range of 0 to F. If you do not specify an IPv6 multicast group, this command displays IPv6 PIM routing entries for all IPv6 multicast groups.

ipv6-source-address: Specifies an IPv6 multicast source by its IPv6 address.

prefix-length: Specifies a prefix length of the IPv6 multicast group or IPv6 multicast source address. The default is 128. For an IPv6 multicast group address, the value range for this argument is 8 to 128. For an IPv6 multicast source address, the value range for this argument is 0 to 128.

flags *flag-value*: Specifies a flag. If you do not specify a flag, this command displays IPv6 PIM routing entries that contain all flags.

The following lists the values for the *flag-value* argument and their meanings:

- **act**: Specifies IPv6 PIM routing entries that have been used for routing data.
- **del**: Specifies IPv6 PIM routing entries to be deleted.
- **exprune**: Specifies IPv6 PIM routing entries that contain outgoing interfaces pruned by other IPv6 multicast routing protocols.
- **ext**: Specifies IPv6 PIM routing entries that contain outgoing interfaces provided by other multicast routing protocols.
- **loc**: Specifies IPv6 PIM routing entries on the devices that reside on the same subnet as the IPv6 multicast source.
- **niif**: Specifies IPv6 PIM routing entries that contain unknown incoming interfaces.
- **nonbr**: Specifies IPv6 PIM routing entries with IPv6 PIM neighbor lookup failure.
- **rpt**: Specifies IPv6 PIM routing entries on the RPT branches where (S, G) prunes have been sent to the RP.
- **rq**: Specifies IPv6 PIM routing entries on the receiving side of the RPT-to-SPT switchover.
- **spt**: Specifies IPv6 PIM routing entries on the SPT.
- **sq**: Specifies IPv6 PIM routing entries on the originating side of the RPT-to-SPT switchover.
- **swt**: Specifies IPv6 PIM routing entries in the process of RPT-to-SPT switchover.
- **wc**: Specifies IPv6 PIM routing entries with wildcards.

fsm: Displays detailed information about the finite state machine.

incoming-interface *interface-type interface-number*: Specifies an incoming interface. If you do not specify an incoming interface, this command displays IPv6 PIM routing entries that contain all incoming interfaces.

interface-type interface-number: Specifies an interface by its type and number.

mode *mode-type*: Specifies an IPv6 PIM mode. If you do not specify an IPv6 PIM mode, this command displays IPv6 PIM routing entries in all modes. The available IPv6 PIM modes include:

- **sm**: Specifies IPv6 PIM-SM.
- **ssm**: Specifies IPv6 PIM-SSM.

outgoing-interface { **exclude** | **include** | **match** } *interface-type interface-number*: Specifies an outgoing interface. If you do not specify an outgoing interface, this command displays IPv6 PIM routing entries that contain all outgoing interfaces. Whether the specified outgoing interface is contained in the IPv6 PIM routing table depends on the following conditions:

- If you specify an excluded interface, this command displays IPv6 PIM routing entries that do not contain the specified outgoing interface.
- If you specify an included interface, this command displays IPv6 PIM routing entries that contain the specified outgoing interface.
- If you specify a matching interface, this command displays IPv6 PIM routing entries that contain only the specified outgoing interface.

Examples

Display IPv6 PIM routing entries.

```
<Switch> display ipv6 pim routing-table
 Total 0 (*, G) entry; 1 (S, G) entry

 (2001::2, FFE3::101)
     RP: FE80::A01:100:1
     Protocol: pim-sm, Flag: SPT LOC ACT
     UpTime: 02:54:43
     Upstream interface: Vlan-interface1
         Upstream neighbor: NULL
         RPF prime neighbor: NULL
     Downstream interface information:
     Total number of downstream interfaces: 1
         1: Vlan-interface2
             Protocol: pim-sm, UpTime: 02:54:43, Expires: 00:02:47
```

Display state machine information for the IPv6 PIM routing table.

```
<Switch> display ipv6 pim routing-table fsm
 Total 0 (*, G) entries; 1 (S, G) entries

 Abbreviations for FSM states:
     NI - no info, J - joined, NJ - not joined, P - pruned,
     NP - not pruned, PP - prune pending, W - winner, L - loser,
     F - forwarding, AP - ack pending, DR - designated router,
     NDR - non-designated router, RCV - downstream receivers

 (2001::2, FFE3::101)
     RP: FE80::A01:100:1
     Protocol: pim-sm, Flag: SPT LOC ACT
     UpTime: 02:54:43
     Upstream interface: Vlan-interface1
         Upstream neighbor: NULL
```

```
    RPF prime neighbor: NULL
    Join/Prune FSM: [SPT: J] [RPT: NP]
Downstream interface information:
Total number of downstream interfaces: 1
    1: Vlan-interface2
        Protocol: pim-sm, UpTime: 02:54:43, Expires: 00:02:47
        DR state: [DR]
        Join/Prune FSM: [NI]
        Assert FSM: [NI]

FSM information for non-downstream interfaces: None
```

Table 11-7 Command output

Field	Description
Total 0 (*, G) entries; 1 (S, G) entries	Total number of (*, G) entries, and the total number of (S, G) entries.
(2001::2, FFE3::101)	(S, G) entry.
RP	IPv6 address of the RP.
Protocol	IPv6 PIM mode: IPv6 PIM-SM.
Flag	Flag of the (S, G) entry or (*, G) entry: • **ACT**—The entry has been used for routing data. • **DEL**—The entry will be removed. • **EXPRUNE**—Some outgoing interfaces are pruned by other IPv6 multicast routing protocols. • **EXT**—The entry contains outgoing interfaces provided by other multicast routing protocols. • **LOC**—The entry is on a router directly connected to the same subnet with the IPv6 multicast source. • **NIIF**—The entry contains unknown incoming interfaces. • **NONBR**—The entry has an IPv6 PIM neighbor lookup failure. • **RPT**—The entry is on an RPT branch where (S, G) prunes have been sent to the RP. • **RQ**—The entry is on the receiving side of the RPT-to-SPT switchover. • **SPT**—The entry is on the SPT. • **SQ**—The entry is on the originating side of the RPT-to-SPT switchover. • **SWT**—The entry is in the process of RPT-to-SPT switchover. • **WC**—The entry contains a wildcard.
Uptime	Length of time since the (S, G) entry or (*, G) entry was installed.
Upstream interface	Upstream (incoming) interface of the (S, G) entry or (*, G) entry.
Upstream neighbor	Upstream neighbor of the (S, G) entry or (*, G) entry.
RPF prime neighbor	RPF neighbor of the (S, G) or (*, G) entry: • For a (*, G) entry, if the RPF neighbor is the RP, the field displays **NULL**.

Field	Description
	• For an (S, G) entry, if the RPF neighbor is a router that directly connects to the IPv6 multicast source, this field displays **NULL**.
Downstream interface information	Information about the downstream interfaces: • Total number of downstream interfaces. • Names of the downstream interfaces. • Protocol type on the downstream interfaces. • Uptime of the downstream interfaces. • Expiration time of the downstream interfaces.

11.1.12. display ipv6 pim rp-info

Use **display ipv6 pim rp-info** to display RP information.

Syntax

display ipv6 pim [**vpn-instance** *vpn-instance-name*] **rp-info** [*ipv6-group-address*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command deletes all static multicast routes on the public network.

ipv6-group-address: Specifies an IPv6 multicast group address. The value range for this argument is FFxy::/16 (excluding FFx1::/16 and FFx2::/16), where "x" and "y" represent any hexadecimal numbers in the range of 0 to F. If you do not specify an IPv6 multicast group, this command displays RP information for all IPv6 multicast groups.

Examples

Display information about the RP for IPv6 multicast group FF0E::101.

```
<Switch> display ipv6 pim rp-info ff0e::101
 BSR RP address is: 7:12::1
     Priority: 192
     HoldTime: 180
     Uptime: 03:01:10
     Expires: 00:02:30

 Static RP address is: 7:12::1
     Preferred: No
     Configured ACL: 2003

 RP mapping for this group is: 7:12::1 (local host)

 Anycast-RP 7:12::1 members:
```

```
    Member address          State
    1:1::1                  Active
    1:1::2                  Local
    1:2::1                  Remote
```

Display information about all RPs for all IPv6 multicast groups.

```
<Switch> display ipv6 pim rp-info
 BSR RP information:
   Scope: non-scoped
     Group/MaskLen: FF00::/8
       RP address               Priority  HoldTime  Uptime    Expires
       8:12::2 (local)          192       180       03:01:36  00:02:29
     Group/MaskLen: FF23::/92 [B]
       RP address               Priority  HoldTime  Uptime    Expires
       7:12::1 (local)          192       180       00:00:39  00:02:57

 Static RP information:
       RP address               ACL   Mode    Preferred
       3:3::1                   2000  pim-sm  No
       3:3::2                   2001  bidir   Yes
       3:3::3                   2002  pim-sm  No
       3:3::4                         pim-sm  No
       3:3::5                   2002  pim-sm  Yes

 Anycast-RP information:
       RP address               Member address          State
       3:3::1                   1:1::1                  Active
       3:3::1                   1:1::2                  Local
       3:3::1                   1:2::1                  Remote
```

Table 11-8 Command output

Field	Description
BSR RP address is	IPv6 address of the RP.
BSR RP information	Information about the RP.
Group/MaskLen	IPv6 multicast group to which the RP is designated.
[B]	This field is not supported in the current software version. The RP is an IPv6 BIDIR-PIM RP. This field is not displayed if the RP is an IPv6 PIM-SM RP.
RP address	IPv6 address of the RP. If the RP resides on the device where the command is executed, this field displays **(local)** after the IPv6 address.
Priority	Priority of the RP.
HoldTime	RP lifetime.
Uptime	Length of time the RP has been up.
Expires	Remaining time for the RP lifetime.
Static RP address	IPv6 address of the static RP.

Field	Description
is/RP address	
Preferred	Whether the static RP is preferred.
Configured ACL/ACL	ACL defining the IPv6 multicast groups to which the static RP is designated.
Mode	RP service mode: IPv6 PIM-SM or IPv6 BIDIR-PIM. IPv6 BIDIR-PIM is not supported in the current software version.
RP mapping for this group	IPv6 address of the RP that provides services for the IPv6 multicast group.
Anycast-RP 7:12::1 members	Members of Anycast RP 7:12::1.
Member address	IPv6 address of the Anycast RP member.
State	State of the interface from which the member address originates: • **Active**—Activated local interface. • **Local**—Inactivated local interface. • **Remote**—Remote interface.

11.1.13. hello-option dr-priority (IPv6 PIM view)

Use **hello-option dr-priority** to set the DR priority globally.

Use **undo hello-option dr-priority** to restore the default.

Syntax

hello-option dr-priority *priority*

undo hello-option dr-priority

Default

The DR priority is 1.

Views

IPv6 PIM view

Predefined user roles

network-admin

Parameters

priority: Specifies a DR priority in the range of 0 to 4294967295. The greater the value, the higher the priority.

Usage guidelines

You can set the DR priority globally for all interfaces in IPv6 PIM view or for an interface in interface view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the global DR priority to 3.

```
<Switch> system-view
[Switch] ipv6 pim
[Switch-pim6] hello-option dr-priority 3
```

Related commands

ipv6 pim hello-option dr-priority

11.1.14. hello-option holdtime (IPv6 PIM view)

Use **hello-option holdtime** to set the IPv6 PIM neighbor lifetime globally.

Use **undo hello-option holdtime** to restore the default.

Syntax

hello-option holdtime *time*

undo hello-option holdtime

Default

The IPv6 PIM neighbor lifetime is 105 seconds.

Views

IPv6 PIM view

Predefined user roles

network-admin

Parameters

time: Specifies an IPv6 PIM neighbor lifetime in the range of 1 to 65535 seconds. If you set the value to 65535 seconds, the IPv6 PIM neighbors are always reachable.

Usage guidelines

You can set the IPv6 PIM neighbor lifetime globally for all interfaces in IPv6 PIM view or for an interface in interface view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the global IPv6 PIM neighbor lifetime to 120 seconds.

```
<Switch> system-view
[Switch] ipv6 pim
[Switch-pim6] hello-option holdtime 120
```

Related commands

ipv6 pim hello-option holdtime

11.1.15. hello-option lan-delay (IPv6 PIM view)

Use **hello-option lan-delay** to set the IPv6 PIM message propagation delay on a shared-media LAN globally.

Use **undo hello-option lan-delay** to restore the default.

Syntax

hello-option lan-delay *delay*

undo hello-option lan-delay

Default

The IPv6 PIM message propagation delay on a shared-media LAN is 500 milliseconds.

Views

IPv6 PIM view

Predefined user roles

network-admin

Parameters

delay: Specifies an IPv6 PIM message propagation delay on a shared-media LAN in the range of 1 to 32767 milliseconds.

Usage guidelines

You can set the IPv6 PIM message propagation delay globally for all interfaces in IPv6 PIM view or for an interface in interface view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the global IPv6 PIM message propagation delay on a shared-media LAN to 200 milliseconds.

```
<Switch> system-view
[Switch] ipv6 pim
[Switch-pim6] hello-option lan-delay 200
```

Related commands

hello-option override-interval (IPv6 PIM view)

ipv6 pim hello-option lan-delay

ipv6 pim hello-option override-interval

11.1.16. hello-option neighbor-tracking (IPv6 PIM view)

Use **hello-option neighbor-tracking** to enable neighbor tracking globally.

Use **undo hello-option neighbor-tracking** to disable neighbor tracking globally.

Syntax

hello-option neighbor-tracking

undo hello-option neighbor-tracking

Default

Neighbor tracking is disabled.

Views

IPv6 PIM view

Predefined user roles

network-admin

Usage guidelines

You can enable neighbor tracking globally for all interfaces in IPv6 PIM view or for an interface in interface view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Enable neighbor tracking globally.

```
<Switch> system-view
```

```
[Switch] ipv6 pim
[Switch-pim6] hello-option neighbor-tracking
```

Related commands

ipv6 pim hello-option neighbor-tracking

11.1.17. hello-option override-interval (IPv6 PIM view)

Use **hello-option override-interval** to set the override interval globally.

Use **undo hello-option override-interval** to restore the default.

Syntax

hello-option override-interval *interval*

undo hello-option override-interval

Default

The override interval is 2500 milliseconds.

Views

IPv6 PIM view

Predefined user roles

network-admin

Parameters

interval: Specifies an override interval in the range of 1 to 65535 milliseconds.

Usage guidelines

You can set the override interval globally for all interfaces in IPv6 PIM view or for an interface in interface view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the global override interval to 2000 milliseconds.

```
<Switch> system-view
[Switch] ipv6 pim
[Switch-pim6] hello-option override-interval 2000
```

Related commands

hello-option lan-delay (IPv6 PIM view)

ipv6 pim hello-option lan-delay

ipv6 pim hello-option override-interval

11.1.18. holdtime join-prune (IPv6 PIM view)

Use **holdtime join-prune** to set the joined/pruned state holdtime globally.

Use **undo holdtime join-prune** to restore the default.

Syntax

holdtime join-prune *time*

undo holdtime join-prune

Default

The joined/pruned state holdtime is 210 seconds.

Views

IPv6 PIM view

Predefined user roles

network-admin

Parameters

time: Specifies a joined/pruned state holdtime in the range of 1 to 65535 seconds.

Usage guidelines

You can set the joined/pruned state holdtime globally for all interfaces in IPv6 PIM view or for an interface in interface view. For an interface, the interface-specific configuration takes priority over the global configuration.

To prevent the upstream neighbors from aging out, you must set the join/prune interval to be less than the joined/pruned state holdtime timer.

Examples

Set the global joined/pruned state holdtime to 280 seconds.

```
<Switch> system-view
[Switch] ipv6 pim
[Switch-pim6] holdtime join-prune 280
```

Related commands

ipv6 pim holdtime join-prune

timer join-prune (IPv6 PIM view)

11.1.19. ipv6 pim

Use **ipv6 pim** to enter IPv6 PIM view.

Use **undo ipv6 pim** to remove all configurations in IPv6 PIM view.

Syntax

ipv6 pim [**vpn-instance** *vpn-instance-name*]

undo ipv6 pim [**vpn-instance** *vpn-instance-name*]

Views

System view

Predefined user roles

network-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command deletes all static multicast routes on the public network.

Examples

Enable IPv6 multicast routing and enter the IPv6 PIM view.

```
<Switch> system-view
[Switch] ipv6 multicast routing
[Switch-mrib6] quit
[Switch] ipv6 pim
[Switch-pim6]
```

11.1.20. ipv6 pim bsr-boundary

Use **ipv6 pim bsr-boundary** to configure an IPv6 PIM-SM domain border (a bootstrap message boundary).

Use **ipv6 pim bsr-boundary** to restore the default.

Syntax

ipv6 pim bsr-boundary

undo ipv6 pim bsr-boundary

Default

An interface is not an IPv6 PIM-SM domain border.

Views

Interface view

Predefined user roles

network-admin

Examples

Configure VLAN-interface 100 as an IPv6 PIM-SM domain border.

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ipv6 pim bsr-boundary
```

Related commands

c-bsr (IPv6 PIM view)

ipv6 multicast boundary

11.1.21. ipv6 pim hello-option dr-priority

Use **ipv6 pim hello-option dr-priority** to set the DR priority on an interface.

Use **undo ipv6 pim hello-option dr-priority** to restore the default.

Syntax

ipv6 pim hello-option dr-priority *priority*

undo ipv6 pim hello-option dr-priority

Default

The DR priority is 1.

Views

Interface view

Predefined user roles

network-admin

Parameters

priority: Specifies a DR priority in the range of 0 to 4294967295. The greater the value, the higher the priority.

Usage guidelines

You can set the DR priority for an interface in interface view or globally for all interfaces in IPv6 PIM view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the DR priority to 3 on VLAN-interface 100.

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ipv6 pim hello-option dr-priority 3
```

Related commands

hello-option dr-priority (IPv6 PIM view)

11.1.22. ipv6 pim hello-option holdtime

Use **ipv6 pim hello-option holdtime** to set the IPv6 PIM neighbor lifetime on an interface.

Use **undo ipv6 pim hello-option holdtime** to restore the default.

Syntax

ipv6 pim hello-option holdtime *time*

undo ipv6 pim hello-option holdtime

Default

The IPv6 PIM neighbor lifetime is 105 seconds.

Views

Interface view

Predefined user roles

network-admin

Parameters

time: Specifies an IPv6 PIM neighbor lifetime in the range of 1 to 65535 seconds. If you set the value to 65535 seconds, the IPv6 PIM neighbor is always reachable.

Usage guidelines

You can set the IPv6 PIM neighbor lifetime for an interface in interface view or globally for all interfaces in IPv6 PIM view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the IPv6 PIM neighbor lifetime to 120 seconds on VLAN-interface 100.

```
<Switch> system-view
```

```
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ipv6 pim hello-option holdtime 120
```

Related commands

hello-option holdtime (IPv6 PIM view)

11.1.23. ipv6 pim hello-option lan-delay

Use **ipv6 pim hello-option lan-delay** to set the IPv6 PIM message propagation delay on a shared-media LAN for an interface.

Use **undo ipv6 pim hello-option lan-delay** to restore the default.

Syntax

ipv6 pim hello-option lan-delay *delay*

undo ipv6 pim hello-option lan-delay

Default

The IPv6 PIM message propagation delay on a shared-media LAN is 500 milliseconds.

Views

Interface view

Predefined user roles

network-admin

Parameters

delay: Specifies an IPv6 PIM message propagation delay on a shared-media LAN in the range of 1 to 32767 milliseconds.

Usage guidelines

You can set the IPv6 PIM message propagation delay for an interface in interface view or globally for all interfaces in IPv6 PIM view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the IPv6 PIM message propagation delay on a shared-media LAN to 200 milliseconds on VLAN-interface 100.

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ipv6 pim hello-option lan-delay 200
```

Related commands

hello-option lan-delay (IPv6 PIM view)

hello-option override-interval (IPv6 PIM view)

ipv6 pim hello-option override-interval

11.1.24. ipv6 pim hello-option neighbor-tracking

Use **ipv6 pim hello-option neighbor-tracking** to enable neighbor tracking on an interface.

Use **ipv6 pim hello-option neighbor-tracking disable** to disable neighbor tracking on an interface when join message suppression is disabled globally.

Use **undo ipv6 pim hello-option neighbor-tracking** to restore neighbor tracking setting on an interface to be consistent with the global setting.

Syntax

ipv6 pim hello-option neighbor-tracking

ipv6 pim hello-option neighbor-tracking disable

undo ipv6 pim hello-option neighbor-tracking

Default

Neighbor tracking is disabled on an interface.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

You can enable neighbor tracking for an interface in interface view or globally for all interfaces in IPv6 PIM view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Enable neighbor tracking on VLAN-interface 100.

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ipv6 pim hello-option neighbor-tracking
```

Disable neighbor tracking on VLAN-interface 100 when neighbor tracking is enabled globally.

```
<Switch> system-view
[Switch] ipv6 pim
[Switch-pim6] hello-option neighbor-tracking
[Switch-pim6] quit
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ipv6 pim hello-option neighbor-tracking disable
```

Related commands

hello-option neighbor-tracking (IPv6 PIM view)

11.1.25. ipv6 pim hello-option override-interval

Use **ipv6 pim hello-option override-interval** to set the override interval on an interface.

Use **undo ipv6 pim hello-option override-interval** to restore the default.

Syntax

ipv6 pim hello-option override-interval *interval*

undo ipv6 pim hello-option override-interval

Default

The override interval is 2500 milliseconds.

Views

Interface view

Predefined user roles

network-admin

Parameters

interval: Specifies an override interval in the range of 1 to 65535 milliseconds.

Usage guidelines

You can set the override interval for an interface in interface view or globally for all interfaces in IPv6 PIM view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the override interval to 2000 milliseconds on VLAN-interface 100.

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ipv6 pim hello-option override-interval 2000
```

Related commands

hello-option lan-delay (IPv6 PIM view)

hello-option override-interval (IPv6 PIM view)

ipv6 pim hello-option lan-delay

11.1.26. ipv6 pim holdtime join-prune

Use **ipv6 pim holdtime join-prune** to set the joined/pruned state holdtime on an interface.

Use **undo ipv6 pim holdtime join-prune** to restore the default.

Syntax

ipv6 pim holdtime join-prune *time*

undo ipv6 pim holdtime join-prune

Default

The joined/pruned state holdtime is 210 seconds.

Views

Interface view

Predefined user roles

network-admin

Parameters

time: Specifies a joined/pruned state holdtime in the range of 1 to 65535 seconds.

Usage guidelines

You can set the joined/pruned state holdtime for an interface in interface view or globally for all interfaces in IPv6 PIM view. For an interface, the interface-specific configuration takes priority over the global configuration.

To prevent the upstream neighbors from aging out, you must configure the join/prune interval to be less than the joined/pruned state holdtime timer.

Examples

Set the joined/pruned state holdtime to 280 seconds on VLAN-interface 100.

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ipv6 pim holdtime join-prune 280
```

Related commands

holdtime join-prune (IPv6 PIM view)

ipv6 pim timer join-prune

11.1.27. ipv6 pim neighbor-policy

Use **ipv6 pim neighbor-policy** to configure an IPv6 PIM hello policy.

Use **undo ipv6 pim neighbor-policy** to restore the default.

Syntax

ipv6 pim neighbor-policy *ipv6-acl-number*

undo ipv6 pim neighbor-policy

Default

No IPv6 PIM hello policy exists on an interface, and all IPv6 PIM hello messages are regarded as legal.

Views

Interface view

Predefined user roles

network-admin

Parameters

ipv6-acl-number: Specifies an IPv6 basic ACL number in the range of 2000 to 2999.

Usage guidelines

An IPv6 PIM hello policy filters IPv6 PIM hello messages to guard against hello message spoofing.

When you configure a rule in the IPv6 basic ACL, follow these restrictions and guidelines:

- For the rule to take effect, do not specify the **vpn-instance** *vpn-instance* option.
- The **source** *source-address source-prefix* option specifies a source IPv6 address.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure an IPv6 PIM hello policy on VLAN-interface 100, so that only the devices on subnet FE80:101::101/64 can become PIM neighbors of this switch.

```
<Switch> system-view
[Switch] acl ipv6 basic 2000
[Switch-acl-ipv6-basic-2000] rule permit source fe80:101::101 64
[Switch-acl-ipv6-basic-2000] quit
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ipv6 pim neighbor-policy 2000
```

11.1.28. ipv6 pim require-genid

Use **ipv6 pim require-genid** to drop hello messages without the generation ID options.

Use **undo ipv6 pim require-genid** to restore the default.

Syntax

ipv6 pim require-genid

undo ipv6 pim require-genid

Default

Hello messages without the generation ID options are accepted.

Views

Interface view

Predefined user roles

network-admin

Examples

Enable VLAN-interface 100 to drop hello messages without the generation ID options.

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ipv6 pim require-genid
```

11.1.29. ipv6 pim sm

Use **ipv6 pim sm** to enable IPv6 PIM-SM.

Use **undo ipv6 pim sm** to disable IPv6 PIM-SM.

Syntax

ipv6 pim sm

undo ipv6 pim sm

Default

IPv6 PIM-SM is disabled.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

This command takes effect only when IPv6 multicast routing is enabled.

Examples

Enable IPv6 multicast routing, and enable IPv6 PIM-SM on VLAN-interface 100.

```
<Switch> system-view
[Switch] ipv6 multicast routing
[Switch-mrib6] quit
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ipv6 pim sm
```

Related commands

ipv6 multicast routing

11.1.30. ipv6 pim state-refresh-capable

Use **ipv6 pim state-refresh-capable** to enable the state refresh feature on an interface.

Use **undo ipv6 pim state-refresh-capable** to disable the state refresh feature.

Syntax

ipv6 pim state-refresh-capable

undo ipv6 pim state-refresh-capable

Default

The state refresh feature is enabled.

Views

Interface view

Predefined user roles

network-admin

Examples

Disable the state refresh feature on VLAN-interface 100.

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] undo ipv6 pim state-refresh-capable
```

Related commands

state-refresh-hoplimit (IPv6 PIM view)

state-refresh-interval (IPv6 PIM view)

state-refresh-rate-limit (IPv6 PIM view)

11.1.31. ipv6 pim timer hello

Use **ipv6 pim timer hello** to set the hello interval on an interface.

Use **undo ipv6 pim timer hello** to restore the default.

Syntax

ipv6 pim timer hello *interval*

undo ipv6 pim timer hello

Default

The hello interval is 30 seconds.

Views

Interface view

Predefined user roles

network-admin

Parameters

interval: Specifies a hello interval in the range of 0 to 18000 seconds. If you set the value to 0 seconds, the interface does not send hello messages.

Usage guidelines

You can set the hello interval for an interface in interface view or globally for all interfaces in IPv6 PIM view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the hello interval to 40 seconds on VLAN-interface 100.

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ipv6 pim timer hello 40
```

Related commands

timer hello (IPv6 PIM view)

11.1.32. ipv6 pim timer join-prune

Use **ipv6 pim timer join-prune** to set the join/prune interval on an interface.

Use **undo ipv6 pim timer join-prune** to restore the default.

Syntax

ipv6 pim timer join-prune *interval*

undo ipv6 pim timer join-prune

Default

The join/prune interval is 60 seconds.

Views

Interface view

Predefined user roles

network-admin

Parameters

interval: Specifies a join/prune interval in the range of 0 to 18000 seconds. If you set the value to 0 seconds, the interface does not send join or prune messages.

Usage guidelines

You can set the join/prune interval for an interface in interface view or globally for all interfaces in IPv6 PIM view. For an interface, the interface-specific configuration takes priority over the global configuration.

The configuration takes effect after the current interval ends.

To prevent the upstream neighbors from aging out, you must set the interval for sending join/prune messages to be less than the joined/pruned state holdtime timer.

Examples

Set the join/prune interval to 80 seconds on VLAN-interface 100.

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ipv6 pim timer join-prune 80
```

Related commands

ipv6 pim holdtime join-prune

timer join-prune (IPv6 PIM view)

11.1.33. ipv6 pim triggered-hello-delay

Use **ipv6 pim triggered-hello-delay** to set the triggered hello delay (maximum delay for sending a hello message).

Use **undo ipv6 pim triggered-hello-delay** to restore the default.

Syntax

ipv6 pim triggered-hello-delay *delay*

undo ipv6 pim triggered-hello-delay

Default

The triggered hello delay is 5 seconds.

Views

Interface view

Predefined user roles

network-admin

Parameters

delay: Specifies a triggered hello delay in the range of 1 to 60 seconds.

Examples

Set the triggered hello delay to 3 seconds on VLAN-interface 100.

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ipv6 pim triggered-hello-delay 3
```

11.1.34. jp-pkt-size (IPv6 PIM view)

Use **jp-pkt-size** to set the maximum size of a join/prune message.

Use **undo jp-pkt-size** to restore the default.

Syntax

jp-pkt-size *size*

undo jp-pkt-size

Default

The maximum size of a join/prune message is 8100 bytes.

Views

IPv6 PIM view

Predefined user roles

network-admin

Parameters

size: Specifies the maximum size of a join/prune message, in the range of 100 to 64000 bytes.

Examples

Set the maximum size of a join/prune message to 1500 bytes.

```
<Switch> system-view
[Switch] ipv6 pim
[Switch-pim6] jp-pkt-size 1500
```

11.1.35. register-policy (IPv6 PIM view)

Use **register-policy** to configure an IPv6 PIM register policy.

Use **undo register-policy** to restore the default.

Syntax

register-policy *ipv6-acl-number*

undo register-policy

Default

No IPv6 PIM register policy exists, and all IPv6 PIM register messages are regarded as legal.

Views

IPv6 PIM view

Predefined user roles

network-admin

Parameters

ipv6-acl-number: Specifies an IPv6 advanced ACL number in the range of 3000 to 3999.

Usage guidelines

An IPv6 PIM register policy enables an RP to filter IPv6 PIM register messages so that the RP is designated only to IPv6 multicast groups permitted by the ACL.

When you configure a rule in the IPv6 advanced ACL, follow these restrictions and guidelines:

- For the rule to take effect, do not specify the **vpn-instance** *vpn-instance* option.
- The **source** *source-address source-prefix* option specifies an IPv6 multicast source address.

- The **destination** *dest-address dest-prefix* option specifies an IPv6 multicast group range.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure an IPv6 PIM register policy to accept register messages from sources on subnet 3:1::/64 to groups on the subnet FF0E:13::/64.

```
<Switch> system-view
[Switch] acl ipv6 advanced 3000
[Switch-acl-ipv6-adv-3000] rule permit ipv6 source 3:1:: 64 destination ff0e:13:: 64
[Switch-acl-ipv6-adv-3000] quit
[Switch] ipv6 pim
[Switch-pim6] register-policy 3000
```

11.1.36. register-whole-checksum (IPv6 PIM view)

Use **register-whole-checksum** to configure the device to calculate the checksum based on an entire register message.

Use **undo register-whole-checksum** to restore the default.

Syntax

register-whole-checksum

undo register-whole-checksum

Default

The device calculates the checksum based on the register message header.

Views

IPv6 PIM view

Predefined user roles

network-admin

Examples

Configure the device to calculate the checksum based on an entire register message.

```
<Switch> system-view
[Switch] ipv6 pim
[Switch-pim6] register-whole-checksum
```

11.1.37. snmp-agent trap enable pim6

Use **snmp-agent trap enable pim6** to enable SNMP notifications for IPv6 PIM.

Use **undo snmp-agent trap enable pim6** to disable SNMP notifications for IPv6 PIM.

Syntax

snmp-agent trap enable pim6 [**candidate-bsr-win-election** | **elected-bsr-lost-election** | **neighbor-loss**] *

undo snmp-agent trap enable pim6 [**candidate-bsr-win-election** | **elected-bsr-lost-election** | **neighbor-loss**] *

Default

SNMP notifications for IPv6 PIM are enabled.

Views

System view

Predefined user roles

network-admin

Parameters

candidate-bsr-win-election: Specifies notifications about winning the BSR election.

elected-bsr-lost-election: Specifies notifications about losing the BSR election.

neighbor-loss: Specifies notifications about losing neighbors.

Usage guidelines

If you do not specify an optional keyword, this command enables or disables IPv6 PIM to generate SNMP notifications.

To report critical IPv6 PIM events to an NMS, enable SNMP notifications for IPv6 PIM. For IPv6 PIM event notifications to be sent correctly, you must also configure SNMP as described in *Network Management and Monitoring Configuration Guide*.

Examples

Disable SNMP notifications for IPv6 PIM.

```
<Switch> system-view
[Switch] undo snmp-agent trap enable pim6
```

11.1.38. source-lifetime (IPv6 PIM view)

Use **source-lifetime** to set the IPv6 multicast source lifetime.

Use **undo source-lifetime** to restore the default.

Syntax

source-lifetime *time*

undo source-lifetime

Default

The IPv6 multicast source lifetime is 210 seconds.

Views

IPv6 PIM view

Predefined user roles

network-admin

Parameters

time: Specifies an IPv6 multicast source lifetime in the range of 0 to 31536000 seconds. If you set the value to 0 seconds, IPv6 multicast sources are never aged out.

Examples

Set the IPv6 multicast source lifetime to 200 seconds.

```
<Switch> system-view
[Switch] ipv6 pim
[Switch-pim6] source-lifetime 200
```

11.1.39. source-policy (IPv6 PIM view)

Use **source-policy** to configure an IPv6 multicast source policy.

Use **undo source-policy** to restore the default.

Syntax

source-policy *ipv6-acl-number*

undo source-policy

Default

No IPv6 multicast source policy exists, The device does not filter IPv6 multicast data packets.

Views

IPv6 PIM view

Predefined user roles

network-admin

Parameters

ipv6-acl-number: Specifies an IPv6 basic or advanced ACL number in the range of 2000 to 3999.

Usage guidelines

An IPv6 multicast source policy filters IPv6 multicast data packets to control information available to downstream receivers.

When you configure a rule in the IPv6 ACL, follow these restrictions and guidelines:

- For the rule to take effect, do not specify the **vpn-instance** *vpn-instance* option.
- In a basic ACL, the **source** *source-address source-prefix* option specifies a source IPv6 address.
- In an advanced ACL, the **source** *source-address source-prefix* option specifies a source IPv6 address. The **destination** *dest-address dest-prefix* option specifies an IPv6 multicast group address.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure an IPv6 multicast source policy to accept IPv6 multicast data from source 3121::1 and to deny the data from source 3121::2.

```
<Switch> system-view
[Switch] acl ipv6 basic 2000
[Switch-acl-ipv6-basic-2000] rule permit source 3121::1 128
[Switch-acl-ipv6-basic-2000] rule deny source 3121::2 128
```

```
[Switch-acl-ipv6-basic-2000] quit
[Switch] ipv6 pim
[Switch-pim6] source-policy 2000
[Switch-pim6] quit
```

11.1.40. spt-switch-threshold (IPv6 PIM view)

Use **spt-switch-threshold** to configure a criterion for an RPT-to-SPT switchover.

Use **undo spt-switch-threshold** to remove criteria for RPT-to-SPT switchovers.

Syntax

spt-switch-threshold { **immediacy** | **infinity** } [**group-policy** *ipv6-acl-number*]

undo spt-switch-threshold [**immediacy** | **infinity**] [**group-policy** *ipv6-acl-number*]

Default

The first IPv6 multicast data packet triggers an RPT-to-SPT switchover.

Views

IPv6 PIM view

Predefined user roles

network-admin

Parameters

immediacy: Triggers an RPT-to-SPT switchover immediately.

infinity: Disables RPT-to-SPT switchover.

group-policy *ipv6-acl-number*: Specifies an IPv6 basic ACL by its number in the range of 2000 to 2999. If you specify an ACL, the configuration applies to the IPv6 multicast groups that the ACL permits. The configuration applies to all IPv6 multicast groups when one of the following conditions exists:

- You do not specify an ACL.
- The specified ACL does not exist.
- The specified ACL does not have valid rules.

Usage guidelines

CAUTION:
If the device is an RP, disabling RPT-to-SPT switchover might cause multicast traffic forwarding failures on the source-side DR. When disabling RPT-to-SPT switchover, make sure you fully understand its impact on your network.

When you configure a rule in the IPv6 basic ACL, follow these restrictions and guidelines:

- For the rule to take effect, do not specify the **vpn-instance** *vpn-instance* option.
- The **source** *source-address source-prefix* option specifies an IPv6 multicast group address.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

Examples

Disable RPT-to-SPT switchover on receiver-side DR.

```
<Switch> system-view
[Switch] ipv6 pim
[Switch-pim6] spt-switch-threshold infinity
```

11.1.41. ssm-policy (IPv6 PIM view)

Use **ssm-policy** to configure the IPv6 SSM group range.

Use **undo ssm-policy** to restore the default.

Syntax

ssm-policy *ipv6-acl-number*

undo ssm-policy

Default

The IPv6 SSM group range is FF3x::/32, where x can be any valid scope.

Views

IPv6 PIM view

Predefined user roles

network-admin

Parameters

ipv6-acl-number: Specifies an IPv6 basic ACL number in the range of 2000 to 2999.

Usage guidelines

This command defines an IPv6 multicast group range that is used by IPv6 PIM-SSM. The IPv6 PIM-SSM mode applies to IPv6 multicast packets that are permitted by the ACL. The IPv6 PIM-SM mode applies to IPv6 multicast packets that are not permitted by the ACL.

When you configure a rule in the IPv6 basic ACL, follow these restrictions and guidelines:

- For the rule to take effect, do not specify the **vpn-instance** *vpn-instance* option.
- The **source** *source-address source-prefix* option specifies an IPv6 multicast group range.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure the IPv6 SSM group range as FF3E:0:8192::/96.

```
<Switch> system-view
[Switch] acl ipv6 basic 2000
[Switch-acl-ipv6-basic-2000] rule permit source ff3e:0:8192:: 96
[Switch-acl-ipv6-basic-2000] quit
[Switch] ipv6 pim
[Switch-pim6] ssm-policy 2000
```

11.1.42. state-refresh-hoplimit (IPv6 PIM view)

Use **state-refresh-hoplimit** to set the hop limit for state refresh messages.

Use **undo state-refresh-hoplimit** to restore the default.

Syntax

state-refresh-hoplimit *hoplimit-value*

undo state-refresh-hoplimit

Default

The hop limit for state refresh messages is 255.

Views

IPv6 PIM view

Predefined user roles

network-admin

Parameters

hoplimit-value: Specifies the hop limit for state refresh messages, in the range of 1 to 255.

Examples

Set the hop limit for state refresh messages to 45.

```
<Switch> system-view
[Switch] ipv6 pim
[Switch-pim6] state-refresh-hoplimit 45
```

Related commands

ipv6 pim state-refresh-capable

state-refresh-interval (IPv6 PIM view)

state-refresh-rate-limit (IPv6 PIM view)

11.1.43. state-refresh-interval (IPv6 PIM view)

Use **state-refresh-interval** to set the state refresh interval.

Use **undo state-refresh-interval** to restore the default.

Syntax

state-refresh-interval *interval*

undo state-refresh-interval

Default

The state refresh interval is 60 seconds.

Views

IPv6 PIM view

Predefined user roles

network-admin

Parameters

interval: Specifies a state refresh interval in the range of 1 to 255 seconds.

Examples

Set the state refresh interval to 70 seconds.

```
<Switch> system-view
[Switch] ipv6 pim
[Switch-pim6] state-refresh-interval 70
```

Related commands

ipv6 pim state-refresh-capable

state-refresh-hoplimit (IPv6 PIM view)

state-refresh-rate-limit (IPv6 PIM view)

11.1.44. state-refresh-rate-limit (IPv6 PIM view)

Use **state-refresh-rate-limit** to set the waiting time to accept a new state refresh message.

Use **undo state-refresh-rate-limit** to restore the default.

Syntax

state-refresh-rate-limit *time*

undo state-refresh-rate-limit

Default

The device waits 30 seconds before it accepts a new state refresh message.

Views

IPv6 PIM view

Predefined user roles

network-admin

Parameters

time: Specifies the waiting time to accept a new refresh message, in the range of 1 to 65535 seconds.

Examples

Set the waiting time to 45 seconds to accept a new state refresh message.

```
<Switch> system-view
[Switch] ipv6 pim
[Switch-pim6] state-refresh-rate-limit 45
```

Related commands

ipv6 pim state-refresh-capable

state-refresh-hoplimit (IPv6 PIM view)

state-refresh-interval (IPv6 PIM view)

11.1.45. static-rp (IPv6 PIM view)

Use **static-rp** to configure a static RP.

Use **undo static-rp** to delete a static RP.

Syntax

static-rp *ipv6-rp-address* [*ipv6-acl-number* | **preferred**] *

undo static-rp *ipv6-rp-address*

Default

No static RPs exist.

Views

IPv6 PIM view

Predefined user roles

network-admin

Parameters

ipv6-rp-address: Specifies the IPv6 address of the static RP. This address must be a valid IPv6 global unicast address.

ipv6-acl-number: Specifies an IPv6 basic ACL number in the range of 2000 to 2999. If you specify an ACL, the static RP is designated only to IPv6 multicast groups that the ACL permits. The static RP is designated to all IPv6 multicast groups when one of the following conditions exists:

- You do not specify an ACL.
- The specified ACL does not exist.
- The specified ACL does not have valid rules.

preferred: Gives priority to the static RP if the static RP and the dynamic RP exist at the same time on the network. The dynamic RP takes effect only when no static RP exists on the network. If you do not specify this keyword, the dynamic RP has priority. The static RP takes effect only when the dynamic RP fails.

Usage guidelines

You do not need to enable IPv6 PIM on an interface that acts as a static RP.

When you configure a rule in the IPv6 basic ACL, follow these restrictions and guidelines:

- For the rule to take effect, do not specify the **vpn-instance** *vpn-instance* option.
- The **source** *source-address source-prefix* option specifies an IPv6 multicast group address.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

When rules in the ACL used by a static RP change, new RPs are dynamically elected for all IPv6 multicast groups.

You can configure multiple static RPs by using this command multiple times. However, if you specify the same static RP address or use the same ACL in the commands, the most recent configuration takes effect. If you configure multiple static RPs for the same IPv6 multicast group, the static RP with the highest IPv6 address is used.

Examples

Configure the interface with IPv6 address 2001::2 as a static RP for IPv6 multicast group range FF03::101/64 and give priority to this static RP.

```
<Switch> system-view
[Switch] acl ipv6 basic 2001
[Switch-acl-ipv6-basic-2001] rule permit source ff03::101 64
[Switch-acl-ipv6-basic-2001] quit
[Switch] ipv6 pim
[Switch-pim6] static-rp 2001::2 2001 preferred
```

Related commands

display ipv6 pim rp-info

11.1.46. timer hello (IPv6 PIM view)

Use **timer hello** to set the hello interval globally.

Use **undo timer hello** to restore the default.

Syntax

timer hello *interval*

undo timer hello

Default

The hello interval is 30 seconds.

Views

IPv6 PIM view

Predefined user roles

network-admin

Parameters

interval: Specifies a hello interval in the range of 0 to 18000 seconds. If you set the value to 0 seconds, the device does not send hello messages.

Usage guidelines

You can set the hello interval globally for all interfaces in IPv6 PIM view or for an interface in interface view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the global hello interval to 40 seconds.

```
<Switch> system-view
[Switch] ipv6 pim
[Switch-pim6] timer hello 40
```

Related commands

ipv6 pim timer hello

11.1.47. timer join-prune (IPv6 PIM view)

Use **timer join-prune** to set the join/prune interval globally.

Use **undo timer join-prune** to restore the default.

Syntax

timer join-prune *interval*

undo timer join-prune

Default

The join/prune interval is 60 seconds.

Views

IPv6 PIM view

Predefined user roles

network-admin

Parameters

interval: Specifies a join/prune interval in the range of 0 to 18000 seconds. If you set the value to 0 seconds, the device does not send join or prune messages.

Usage guidelines

You can set the join/prune interval globally for all interfaces in IPv6 PIM view or for an interface in interface view. For an interface, the interface-specific configuration takes priority over the global configuration.

The configuration takes effect after the current interval ends.

To prevent the upstream neighbors from aging out, you must set the join/prune interval to be less than the joined/pruned state holdtime.

Examples

Set the global join/prune interval to 80 seconds.

```
<Switch> system-view
[Switch] ipv6 pim
[Switch-pim6] timer join-prune 80
```

Related commands

holdtime join-prune (IPv6 PIM view)

ipv6 pim timer join-prune

Contents

A page of this section is **6-x-x**

12. PIM snooping commands 12-1
12.1. PIM snooping commands 12-1
12.1.1. display pim-snooping neighbor 12-1
12.1.2. display pim-snooping router-port 12-2
12.1.3. display pim-snooping routing-table 12-3
12.1.4. display pim-snooping statistics 12-5
12.1.5. pim-snooping enable 12-6

12. PIM snooping commands

NOTE:

PIM snooping commands are only supported when used in combination with UNIVERGE Network Operation Engine Overlay Network Extension.

12.1. PIM snooping commands

12.1.1. display pim-snooping neighbor

Use **display pim-snooping neighbor** to display PIM snooping neighbor information.

Syntax

display pim-snooping neighbor [**vlan** *vlan-id* | **vsi** *vsi-name*] [**slot** *slot-number*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays PIM snooping neighbor information for all VLANs.

vsi *vsi-name*: Specifies a VSI by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VSI, this command displays PIM snooping neighbor information for all VSIs.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays PIM snooping neighbor information for the master device.

verbose: Displays detailed information about PIM snooping neighbors. If you do not specify this keyword, the command displays brief information about PIM snooping neighbors.

Examples

Display detailed information about PIM snooping neighbors for VLAN 2.

```
<Sysname> display pim-snooping neighbor vlan 2 verbose
Total 2 neighbors.

VLAN 2: Total 2 neighbors.
  10.1.1.2
    Slots (0 in total):
    Ports (1 in total):
      GE1/0/1                              (02:02:23)    LAN Prune Delay(T)
  10.1.1.3
    Slots (0 in total):
    Ports (1 in total):
      GE1/0/2                              (02:02:25)
```

Table 12-1 Command output

Field	Description
Total 2 neighbors	Total number of PIM snooping neighbors.
VLAN 2: Total 2 neighbors	Total number of PIM snooping neighbors in VLAN 2.
10.1.1.2	IP address of the PIM snooping neighbor.
Slots (0 in total)	Member IDs and total number of the member devices that have the neighbor, except for the specified member device or the master device when no member device is specified.
Ports (1 in total)	Ports where the PIM snooping neighbors reside, and the total number of the ports.
(02:02:23)	Remaining aging timer for a PIM snooping neighbor on the port. This field is always displayed for global ports (such as Layer 2 aggregate interfaces, ACs, N-PWs, and U-PWs). For a non-global port, this field is displayed when one of the following conditions exists: • The port is on the specified member device. • The port is on the master device and no member device is specified.
LAN Prune Delay	The PIM hello message sent by the PIM snooping neighbor has the LAN_Prune_Delay option.
(T)	The join message suppression feature has been disabled for the PIM snooping neighbor.
NPW (Link ID 8)	N-PW and its link ID.
UPW (Link ID 9)	U-PW and its link ID.

12.1.2. display pim-snooping router-port

Use **display pim-snooping router-port** to display PIM snooping router port information.

Syntax

display pim-snooping router-port [**vlan** *vlan-id* | **vsi** *vsi-name*] [**slot** *slot-number*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays PIM snooping router port information for all VLANs.

verbose: Displays detailed information about PIM snooping router ports. If you do not specify this keyword, the command displays brief information about PIM snooping router ports.

vsi *vsi-name*: Specifies a VSI by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VSI, this command displays PIM snooping router port information for all VSIs.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays PIM snooping router port information for the master device.

Examples

Display brief information about PIM snooping router ports for VLAN 2.

```
<Sysname> display pim-snooping router-port vlan 2
VLAN 2:
  Router ports (2 in total):
    GE1/0/1                                 (00:01:30)
    GE1/0/2                                 (00:01:32)
```

Display detailed information about PIM snooping router ports for VLAN 2.

```
<Sysname> display pim-snooping router-port vlan 2 verbose
VLAN 2:
  Router slots (0 in total):
  Router ports (2 in total):
    GE1/0/1                                 (00:01:30)
    GE1/0/2                                 (00:01:32)
```

Table 12-2 Command output

Field	Description
VLAN 2	VLAN ID.
Router slots (0 in total)	Member IDs and total number of the member devices that have router ports, except for the specified member device or the master device when no member device is specified.
Router ports (2 in total)	Router ports and total number of router ports.
(00:01:30)	Remaining aging time for the router port. For a global port, this field is always displayed. For a non-global port, this field is displayed when one of the following conditions exists: • The port is on the specified member device. • The port is on the master device and no member device is specified.
NPW (Link ID 8)	N-PW and its link ID.
UPW (Link ID 9)	U-PW and its link ID.

12.1.3. display pim-snooping routing-table

Use **display pim-snooping routing-table** to display PIM snooping routing entries.

Syntax

display pim-snooping routing-table [**vlan** *vlan-id* | **vsi** *vsi-name*] [**slot** *slot-number*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays PIM snooping routing entries for all VLANs.

vsi *vsi-name*: Specifies a VSI by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VSI, this command displays PIM snooping routing entries for all VSIs.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays PIM snooping routing entries for the master device.

verbose: Displays detailed information about PIM snooping routing entries. If you do not specify the keyword, this command displays brief information about PIM snooping routing entries.

Examples

Display detailed information about PIM snooping routing entries for VLAN 2.

```
<Sysname> display pim-snooping routing-table vlan 2 verbose
Total 1 entries.
FSM Flag: NI-no info, J-join, PP-prune pending

VLAN 2: Total 1 entries.
  (172.10.10.1, 225.1.1.1)
    FSM information: dummy
    Upstream neighbor: 20.1.1.1
      Upstream Slots (0 in total):
      Upstream Ports (1 in total):
        GE1/0/1
      Downstream Slots (0 in total):
      Downstream Ports (2 in total):
        GE1/0/2
          Expires: 00:03:01, FSM: J
          Downstream Neighbors (2 in total):
            7.1.1.1
              Expires: 00:59:19, FSM: J
            7.1.1.11
              Expires: 00:59:20, FSM: J
        GE1/0/3
          Expires: 00:02:21, FSM: PP
```

Table 12-3 Command output

Field	Description
Total 1 entries	Total number of (S, G) entries and (*, G) entries.
FSM Flag: NI-no info, J-join, PP-prune pending	State machine flag of the downstream port: • **NI**—Initial state. • **J**—Join. • **PP**—Prune pending.
VLAN 2: Total 1 entries	Total number of (S, G) entries and (*, G) entries in VLAN 2.

Field	Description
(172.10.10.1, 225.1.1.1)	(S, G) entry.
FSM information	Finite state machine information of the entry: • **delete**—The entry attributes have been deleted. • **dummy**—The entry is a new temporary entry. • **no info**—The entry does not exist.
Upstream neighbor	Upstream neighbor of the (S, G) or (*, G) entry.
Upstream Slots (0 in total)	Member IDs and total number of the member devices that have the upstream neighbor, except for the specified member device or the master device when no member device is specified.
Upstream Ports (1 in total)	Upstream ports, and the total number of upstream ports. This field is displayed when one of the following conditions exists: • The port is on the specified member device. • The port is on the master device and no member device is specified.
Downstream Slots (0 in total)	Member IDs and total number of the member devices that have downstream ports, except for the specified member device or the master device when no member device is specified.
Downstream Ports (2 in total)	Downstream ports of the upstream neighbor, and the total number of the downstream ports.
Downstream Neighbors (2 in total)	Downstream neighbors of the downstream port, and the total number of the downstream neighbors.
Expires: 00:03:01, FSM: J	Remaining aging time for the downstream port or downstream neighbor, and the finite state machine information. For a global port, this field is always displayed. For a non-global port, this field is displayed when one of the following conditions exists: • The port is on the specified member device. • The port is on the master device and no member device is specified.
NPW (Link ID 8)	N-PW and its link ID.
UPW (Link ID 9)	U-PW and its link ID.

12.1.4. display pim-snooping statistics

Use **display pim-snooping statistics** to display statistics for the PIM messages learned through PIM snooping.

Syntax

display pim-snooping statistics

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display statistics for the PIM messages learned through PIM snooping.

```
<Sysname> display pim-snooping statistics
Received PIMv2 hello:  100
Received PIMv2 join/prune:  100
Received PIMv2 error:  0
Received PIMv2 messages in total:  200
Received PIMv1 messages in total:  0
```

Table 12-4 Command output

Field	Description
Received PIMv2 hello	Number of received PIMv2 hello messages.
Received PIMv2 join/prune	Number of received PIMv2 join/prune messages.
Received PIMv2 error	Number of received PIMv2 messages with errors.
Received PIMv2 messages in total	Total number of received PIMv2 messages.
Received PIMv1 messages in total	Total number of received PIMv1 messages.

Related commands

reset pim-snooping statistics

12.1.5. pim-snooping enable

Use **pim-snooping enable** to enable PIM snooping for a VLAN or VSI.

Use **undo pim-snooping enable** to disable PIM snooping for a VLAN or VSI.

Syntax

pim-snooping enable

undo pim-snooping enable

Default

PIM snooping is disabled for a VLAN or VSI.

Views

VLAN view

VSI view

Predefined user roles

network-admin

Usage guidelines

You must enable the IGMP snooping feature and enable IGMP snooping for a VLAN or VSI before you enable PIM snooping for the VLAN or VSI.

PIM snooping does not take effect on sub-VLANs of a multicast VLAN.

Examples

Enable the IGMP snooping feature, and then enable IGMP snooping and PIM snooping for VLAN 2.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] pim-snooping enable
```

Related commands

igmp-snooping

igmp-snooping enable

Contents

A page of this section is **6-x-x**

13. IGMP proxy commands 13-1
13.1. IGMP proxy commands 13-1
13.1.1. display igmp proxy group 13-1
13.1.2. display igmp proxy routing-table 13-2
13.1.3. igmp proxy enable 13-5

13. IGMP proxy commands

NOTE:

IGMP proxy commands are only supported when used in combination with UNIVERGE Network Operation Engine Overlay Network Extension.

13.1. IGMP proxy commands

13.1.1. display igmp proxy group

Use **display igmp proxy group** to display information about multicast groups maintained by the IGMP proxy.

Syntax

display igmp [**vpn-instance** *vpn-instance-name*] **proxy group** [*group-address* | **interface** *interface-type interface-number*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays information about multicast groups maintained by the IGMP proxy on the public network.

group-address: Specifies a multicast group by its IP address in the range of 224.0.1.0 to 239.255.255.255. If you do not specify a multicast group, this command displays information about all multicast groups maintained by the IGMP proxy.

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays information about multicast groups maintained by the IGMP proxy for all interfaces.

verbose: Displays detailed information.

Examples

Display information about multicast groups maintained by the IGMP proxy on the public network.

```
<Sysname> display igmp proxy group
IGMP proxy group records in total: 2
 Vlan-interface1(1.1.1.20):
  IGMP proxy group records in total: 2
   Group address      Member state      Expires
   225.1.1.1          Delay             00:00:02
   225.1.1.2          Idle              Off
```

Display detailed information about multicast group 225.1.1.1 maintained by the IGMP proxy on the public network.

```
<Sysname> display igmp proxy group 225.1.1.1 verbose
 Vlan-interface1(1.1.1.20):
  IGMP proxy group records in total: 2
   Group: 225.1.1.1
     Group mode: Include
     Member state: Delay
     Expires: 00:00:02
     Source list (sources in total: 1):
       1.1.1.1
```

Table 13-1 Command output

Field	Description
IGMP groups records in total	Total number of multicast groups maintained by the IGMP proxy.
Vlan-interface1(1.1.1.20)	IGMP proxy interface and its IP address.
Pending proxy group	Pending multicast groups maintained by the IGMP proxy.
Group address/Group	Multicast group address.
Member state	Member host states: • **Delay**—The member host has joined a group and started a delay timer. • **Idle**—The member host has joined a group, but didn't start a delay timer.
Expires	Remaining delay time for the member host to send a responding report. This field displays **Off** if the timer is disabled.
Group mode	Multicast source filtering mode: Include or Exclude.
Source list	Multicast source list for the multicast group maintained by the IGMP proxy.
sources in total	Total number of multicast sources.

13.1.2. display igmp proxy routing-table

Use **display igmp proxy routing-table** to display multicast routing entries maintained by the IGMP proxy.

Syntax

display igmp [**vpn-instance** *vpn-instance-name*] **proxy routing-table** [*source-address* [**mask** { *mask-length* | *mask* }] | *group-address* [**mask** { *mask-length* | *mask* }]] * [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays multicast routing entries maintained by the IGMP proxy on the public network.

source-address: Specifies a multicast source by its IP address. If you do not specify a multicast source, this command displays multicast routing entries for all multicast sources maintained by the IGMP proxy.

group-address: Specifies a multicast group address by its IP address in the range of 224.0.1.0 to 239.255.255.255. If you do not specify a multicast group, this command displays multicast routing entries for all multicast groups maintained by the IGMP proxy.

mask-length: Specifies a mask length of the multicast group address or multicast source address. For a multicast source address, the value range for this argument is 0 to 32. For a multicast group address, the value range for this argument is 4 to 32. The default value is 32 in both cases.

mask: Specifies a mask of the multicast group address or multicast source address. The default value is 255.255.255.255.

verbose: Displays detailed information about multicast routing entries maintained by the IGMP proxy.

Examples

Display multicast routing entries maintained by the IGMP proxy on the public network.

```
<Sysname> display igmp proxy routing-table
 Total 1 (*, G) entries, 2 (S, G) entries.

 (172.168.0.12, 227.0.0.1)
     Upstream interface: Vlan-interface1
     Downstream interfaces (1 in total):
         1: Vlan-interface2
             Protocol: IGMP

 (*, 225.1.1.1)
     Upstream interface: Vlan-interface1
     Downstream interfaces (1 in total):
         1: Vlan-interface2
             Protocol: STATIC

 (2.2.2.2, 225.1.1.1)
     Upstream interface: Vlan-interface1
     Downstream interfaces (2 in total):
         1: LoopBack1
             Protocol: STATIC
         2: Vlan-interface2
             Protocol: PROXY
```

Display detailed information about multicast routing entries maintained by the IGMP proxy on the public network.

```
<Sysname> display igmp proxy routing-table verbose
 Total 1 (*, G) entries, 2 (S, G) entries.

 (172.168.0.12, 227.0.0.1)
```

```
    Upstream interface: Vlan-interface1
    Downstream interfaces (1 in total):
        1: Vlan-interface2
            Protocol: IGMP
            Querier state: Querier
            Join/Prune state:Join

    Non-downstream interfaces: None

(*, 225.1.1.1)
    Upstream interface: Vlan-interface1
    Downstream interfaces (1 in total):
        1: Vlan-interface2
            Protocol: STATIC
            Querier state: Querier
            Join/Prune state:Join

    Non-downstream interfaces (1 in total):
        1: Vlan-interface3
            Protocol: IGMP
            Querier state: Non-querier
            Join/Prune state:Join

(2.2.2.2, 225.1.1.1)
    Upstream interface: Vlan-interface1
    Downstream interfaces (2 in total):
        1: LoopBack1
            Protocol: STATIC
            Querier state: Querier
            Join/Prune state: Join
        2: Vlan-interface2
            Protocol: PROXY
            Querier state: Querier
            Join/Prune state: Join

    Non-downstream interfaces: None
```

Table 13-2 Command output

Field	Description
Total 1 (*, G) entries, 2 (S, G) entries	Total number of (*, G) entries, and the total number of (S, G) entries.
(172.168.0.12, 227.0.0.1)	(S, G) entry.
Upstream interface	Incoming interface of the (S, G) entry.
Downstream interfaces (1 in total)	Outgoing interfaces of the (S, G) entry, and the total number of outgoing interfaces.
Non-downstream interfaces (1 in total)	Non-outgoing interfaces of the (S, G) entry, and the total number of non-outgoing interfaces.

Field	Description
1: Vlan-interface2	Index of an interface, and the interface.
Protocol	Protocol type: • **IGMP**—Dynamic IGMP. • **PROXY**—IGMP proxy. • **STATIC**—Static IGMP.
Querier state	Querier state: • Querier. • Non-querier.
Join/Prune state	Joined or pruned state of the interface: • **NI**—Default state. • **Join**—Joined state. • **Prune**—Pruned state.

13.1.3. igmp proxy enable

Use **igmp proxy enable** to enable IGMP proxying on an interface.

Use to **undo igmp proxy enable** to disable IGMP proxying on an interface.

Syntax

igmp proxy enable

undo igmp proxy enable

Default

IGMP proxying is disabled on an interface.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

This command takes effect only when IP multicast routing is enabled on the public network or for the VPN instance to which the interface belongs.

Examples

Enable IP multicast routing on the public network, and enable IGMP proxying on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] multicast routing-enable
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] igmp proxy enable
```

Related commands

multicast routing

QX-S5600G Series Ethernet Switches

Command References

7.MCE

This manual is including the following chapters.

01-MCE commands

02-IPv6 MEC commands

Contents

A page of this section is **7-x-x**

1. MCE commands ····· 1-1
1.1. MCE commands ····· 1-1
1.1.1. address-family ipv4 (VPN instance view) ····· 1-1
1.1.2. description (VPN instance view) ····· 1-1
1.1.3. display ip vpn-instance ····· 1-2
1.1.4. export route-policy ····· 1-4
1.1.5. import route-policy ····· 1-4
1.1.6. ip binding vpn-instance ····· 1-5
1.1.7. ip vpn-instance (system view) ····· 1-6
1.1.8. route-distinguisher (VPN instance view) ····· 1-7
1.1.9. routing-table limit ····· 1-8
1.1.10. vpn-instance-capability simple (OSPF view) ····· 1-9
1.1.11. vpn-target ····· 1-9

1. MCE commands

1.1. MCE commands

1.1.1. address-family ipv4 (VPN instance view)

Use **address-family ipv4** to enter VPN instance IPv4 VPN view.

Use **undo address-family ipv4** to remove all configurations from VPN instance IPv4 VPN view.

Syntax

address-family ipv4

undo address-family ipv4

Views

VPN instance view

Predefined user roles

network-admin

Usage guidelines

In VPN instance IPv4 VPN view, you can configure IPv4 VPN parameters such as inbound and outbound routing policies.

Examples

Enter VPN instance IPv4 VPN view.

```
<Switch> system-view
[Switch] ip vpn-instance vpn1
[Switch-vpn-instance-vpn1] address-family ipv4
[Switch-vpn-ipv4-vpn1]
```

Related commands

address-family ipv6 (VPN instance view)

1.1.2. description (VPN instance view)

Use **description** to configure a description for a VPN instance.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

No description is configured for a VPN instance.

Views

VPN instance view

Predefined user roles

network-admin

Parameters

text: Specifies a description, a case-sensitive string of 1 to 79 characters.

Examples

Configure a description of **This is vpn1** for VPN instance **vpn1**.

```
<Switch> system-view
[Switch] ip vpn-instance vpn1
[Switch-vpn-instance-vpn1] description This is vpn1
```

1.1.3. display ip vpn-instance

Use **display ip vpn-instance** to display information about VPN instances.

Syntax

display ip vpn-instance [**instance-name** *vpn-instance-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

instance-name *vpn-instance-name*: Displays information about the specified VPN instance. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays brief information about all VPN instances.

Examples

Display brief information about all VPN instances.

```
<Switch> display ip vpn-instance
  Total VPN-Instances configured : 1
  VPN-Instance Name               RD                    Create time
  abc                             1:1                   2011/05/18 10:48:17
```

Table 1-1 Command output

Field	Description
VPN-Instance Name	Name of the VPN instance.
RD	RD of the VPN instance.
Create Time	Time when the VPN instance was created.

Display detailed information about VPN instance **vpn1**.

```
<Switch> display ip vpn-instance instance-name vpn1
  VPN-Instance Name and Index : vpn1, 2
  Route Distinguisher : 100:1
  VPN ID : 1:1
  Description : vpn1
```

```
Interfaces : Vlan-interface2
Address-family IPv4:
 Export VPN Targets :
     2:2
 Import VPN Targets :
     3:3
 Export Route Policy : outpolicy
 Import Route Policy : inpolicy
 Tunnel Policy : tunnel1
 Maximum Routes Limit : 500
 Threshold Value(%): 50
Address-family IPv6:
 Export VPN Targets :
     2:2
 Import VPN Targets :
     3:3
 Export Route Policy : outpolicy
 Import Route Policy : inpolicy
 Tunnel Policy : tunnel1
 Maximum Routes Limit :500
 Threshold Value(%): 50
Address-family EVPN:
 Export VPN Targets :
     3:3
 Import VPN Targets :
     3:3
```

Table 1-2 Command output

Field	Description
Route Distinguisher	Route distinguisher of the VPN instance.
Interfaces	Interfaces that are associated with the VPN instance.
Address-family IPv4	IPv4 VPN information.
Address-family IPv6	IPv6 VPN information.
Address-family EVPN	EVPN information. For more information about EVPN, see *EVPN Configuration Guide*.
Export VPN Targets	Export route targets.
Import VPN Targets	Import route targets.
Export Route Policy	Routing policy in the outbound direction.
Import Route Policy	Routing policy in the inbound direction.
Tunnel Policy	This field is not supported in the current software version. Tunnel policy associated with the VPN instance.
Maximum Routes Limit	Maximum number of routes.
Threshold Value(%)	Alarm threshold for number of active routes.

1.1.4. export route-policy

Use **export route-policy** to apply an export routing policy to a VPN instance.

Use **undo export route-policy** to restore the default.

Syntax

export route-policy *route-policy*

undo export route-policy

Default

No export routing policy is applied to a VPN instance.

Views

VPN instance view

VPN instance IPv4 VPN view

VPN instance IPv6 VPN view

Predefined user roles

network-admin

Parameters

route-policy: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters.

Usage guidelines

You can specify an export routing policy to filter advertised routes or modify their route attributes for the VPN instance.

If you execute this command multiple times, the most recent configuration takes effect.

An export routing policy specified in VPN instance view applies to both IPv4 VPN and IPv6 VPN. An export routing policy specified in VPN instance IPv4 VPN view applies only to IPv4 VPN. An export routing policy specified in VPN instance IPv6 VPN view applies only to IPv6 VPN.

If you have specified export routing policies in both VPN instance IPv4 VPN view and VPN instance view, IPv4 VPN uses the export routing policy specified in VPN instance IPv4 VPN view.

If you have specified export routing policies in both VPN instance IPv6 VPN view and VPN instance view, IPv6 VPN uses the export routing policy specified in VPN instance IPv6 VPN view.

Examples

Apply export routing policy **poly-1** to VPN instance **vpn1**.

```
<Switch> system-view
[Switch] ip vpn-instance vpn1
[Switch-vpn-instance-vpn1] export route-policy poly-1
```

Related commands

import route-policy

route-policy (*Layer 3—IP Routing Command Reference*)

1.1.5. import route-policy

Use **import route-policy** to apply an import routing policy to a VPN instance.

Use **undo import route-policy** to restore the default.

Syntax

import route-policy *route-policy*

undo import route-policy

Default

All routes matching the import target attribute are accepted.

Views

VPN instance view

VPN instance IPv4 VPN view

VPN instance IPv6 VPN view

Predefined user roles

network-admin

Parameters

route-policy: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters.

Usage guidelines

You can specify an import routing policy to filter received routes or modify their route attributes for the VPN instance.

If you execute this command multiple times, the most recent configuration takes effect.

An import routing policy specified in VPN instance view applies to both IPv4 VPN and IPv6 VPN. An import routing policy specified in VPN instance IPv4 VPN view applies only to IPv4 VPN. An import routing policy specified in VPN instance IPv6 VPN view applies only to IPv6 VPN.

If you have specified import routing policies in both VPN instance IPv4 VPN view and VPN instance view, IPv4 VPN uses the import routing policy specified in VPN instance IPv4 VPN view.

If you have specified import routing policies in both VPN instance IPv6 VPN view and VPN instance view, IPv6 VPN uses the import routing policy specified in VPN instance IPv6 VPN view.

Examples

Apply import routing policy **poly-1** to VPN instance **vpn1**.

```
<Switch> system-view
[Switch] ip vpn-instance vpn1
[Switch-vpn-instance-vpn1] import route-policy poly-1
```

Related commands

export route-policy

route-policy (*Layer 3—IP Routing Command Reference*)

1.1.6. ip binding vpn-instance

Use **ip binding vpn-instance** to associate an interface with a VPN instance.

Use **undo ip binding vpn-instance** to restore the default.

Syntax

ip binding vpn-instance *vpn-instance-name*

undo ip binding vpn-instance

Default

An interface is associated with no VPN instance and belongs to the public network.

Views

Interface view

Predefined user roles

network-admin

Parameters

vpn-instance-name: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

Use this command to associate the VPN instance with the interface connected to the CE.

This command or its undo form clears the IP address and routing protocol configuration on the interface.

The specified VPN instance must have been created by using the **ip vpn-instance** command in system view.

To associate a new VPN instance with an interface, first execute the **undo ip binding vpn-instance** command to remove the existing association.

Examples

Associate VLAN-interface 1 with VPN instance **vpn1**.

```
<Switch> system-view
[Switch] interface vlan-interface 1
[Switch-Vlan-interface1] ip binding vpn-instance vpn1
```

Related commands

ip vpn-instance (system view)

1.1.7. ip vpn-instance (system view)

Use **ip vpn-instance** to create a VPN instance and enter its view, or enter the view of an existing VPN instance.

Use **undo ip vpn-instance** to delete a VPN instance.

Syntax

ip vpn-instance *vpn-instance-name*

undo ip vpn-instance *vpn-instance-name*

Default

No VPN instances exist.

Views

System view

Predefined user roles

network-admin

Parameters

vpn-instance-name: Specifies a VPN instance name, a case-sensitive string of 1 to 31 characters.

Examples

Create a VPN instance named **vpn1** and enter its view.

```
<Switch> system-view
[Switch] ip vpn-instance vpn1
[Switch-vpn-instance-vpn1]
```

Related commands

route-distinguisher

1.1.8. route-distinguisher (VPN instance view)

Use **route-distinguisher** to configure an RD for a VPN instance.

Use **undo route-distinguisher** to restore the default.

Syntax

route-distinguisher *route-distinguisher*

undo route-distinguisher

Default

No RD is specified for a VPN instance.

Views

VPN instance view

Predefined user roles

network-admin

Parameters

route-distinguisher: Specifies an RD for the VPN instance, a string of 3 to 21 characters in one of the following formats:

- *16-bit AS number*:*32-bit user-defined number*. For example, 101:3.
- *32-bit IP address*:*16-bit user-defined number*. For example, 192.168.122.15:1.
- *32-bit AS number*:*16-bit user-defined number*, where the minimum value of the AS number is 65536. For example, 65536:1.

Usage guidelines

RDs enable VPNs to use the same address space. An RD and an IPv4 prefix form a unique VPN-IPv4 prefix.

To guarantee global uniqueness for a VPN-IPv4 address, do not set the AS number or IP address in an RD to any private AS number or private IP address.

To modify an RD, execute the **undo route-distinguisher** command to remove the RD and then execute the **route-distinguisher** command.

Examples

Configure RD 22:1 for VPN instance **vpn1**.

```
<Switch> system-view
[Switch] ip vpn-instance vpn1
```

```
[Switch-vpn-instance-vpn1] route-distinguisher 22:1
```

1.1.9. routing-table limit

Use **routing-table limit** to set the maximum number of active routes in a VPN instance.

Use **undo routing-table limit** to restore the default.

Syntax

routing-table limit *number* { *warn-threshold* | **simply-alert** }

undo routing-table limit

Default

The number of active routes in a VPN instance is not limited.

Views

VPN instance view

VPN instance IPv4 VPN view

VPN instance IPv6 VPN view

Predefined user roles

network-admin

Parameters

number: Specifies the maximum number of active routes. In VPN instance view, the value range for this argument is 1 to 24576. In VPN instance IPv4 VPN view, the value range for this argument is 1 to 49152. In VPN instance IPv6 VPN view, the value range for this argument is 1 to 24576.

warn-threshold: Specifies a warning threshold in the range of 1 to 100 in percentage. When the percentage of the existing active routes to the maximum active routes exceeds the threshold, the system gives a log message but still allows new active routes. If active routes in the VPN instance reach the maximum, no more active routes are added.

simply-alert: Specifies that when active routes exceed the maximum number, the system still accepts active routes but generates a log message.

Usage guidelines

Setting the maximum number of active routes for a VPN instance can prevent a PE from learning too many routes.

A limit configured in VPN instance view applies to both the IPv4 VPN and the IPv6 VPN. A limit configured in VPN instance IPv4 VPN view applies only to the IPv4 VPN. A limit configured in VPN instance IPv6 VPN view applies only to the IPv6 VPN.

If you have specified the limit in both VPN instance IPv4 VPN view and VPN instance view, IPv4 VPN uses the limit specified in VPN instance IPv4 VPN view.

If you have specified the limit in both VPN instance IPv6 VPN view and VPN instance view, IPv6 VPN uses the limit specified in VPN instance IPv6 VPN view.

Examples

Specify that VPN instance **vpn1** supports a maximum of 1000 active routes. When active routes exceed this limit, the device can receive new active routes but generates a log message.

```
<Switch> system-view
[Switch] ip vpn-instance vpn1
[Switch-vpn-instance-vpn1] route-distinguisher 100:1
```

```
[Switch-vpn-instance-vpn1] routing-table limit 1000 simply-alert
```

1.1.10. vpn-instance-capability simple (OSPF view)

Use **vpn-instance-capability simple** to disable routing loop detection for a VPN OSPF process.

Use **undo vpn-instance-capability** to enable routing loop detection for a VPN OSPF process.

Syntax

vpn-instance-capability simple

undo vpn-instance-capability

Default

Routing loop detection is enabled for a VPN OSPF process.

Views

OSPF view

Predefined user roles

network-admin

Usage guidelines

For the MCE to receive OSPF routes from the PE, you must disable routing loop detection for a VPN OSPF process on the MCE.

This command is applicable only to VPN OSPF processes.

Examples

Disable routing loop detection for VPN OSPF process 100.

```
<Switch> system-view
[Switch] ospf 100 vpn-instance vpna
[Switch-ospf-100] vpn-instance-capability simple
```

1.1.11. vpn-target

Use **vpn-target** to configure route targets for a VPN instance.

Use **undo vpn-target** to remove the specified or all route targets of a VPN instance.

Syntax

vpn-target *vpn-target*&<1-8> [**both** | **export-extcommunity** | **import-extcommunity**]

undo vpn-target { **all** | *vpn-target*&<1-8> [**both** | **export-extcommunity** | **import-extcommunity**] }

Default

No route targets are configured for a VPN instance.

Views

VPN instance view

VPN instance IPv4 VPN view

VPN instance IPv6 VPN view

Predefined user roles

network-admin

Parameters

vpn-target&<1-8>: Specifies a space-separated list of up to eight route targets.

A route target is a string of 3 to 21 characters in one of the following formats:

- *16-bit AS number*:*32-bit user-defined number*. For example, 101:3.
- *32-bit IP address*:*16-bit user-defined number*. For example, 192.168.122.15:1.
- *32-bit AS number*:*16-bit user-defined number*, where the AS number must not be less than 65536. For example, 65536:1.

both: Uses the specified route targets as both import targets and export targets. The **both** keyword is also used when you do not specify any of the following keywords: **both**, **export-extcommunity**, and **import-extcommunity**.

export-extcommunity: Uses the specified route targets as export targets.

import-extcommunity: Uses the specified route targets as import targets.

all: Removes all route targets.

Usage guidelines

Route targets are used to control the advertisement of VPN routing information. A PE adds the configured export targets into the route target attribute of routes advertised to a peer. The peer uses the local import targets to match the route targets of received routes. If a match is found, the peer adds the routes to the routing table of the VPN instance.

Route targets configured in VPN instance view apply to both the IPv4 VPN and the IPv6 VPN. Route targets configured in VPN instance IPv4 VPN view apply only to the IPv4 VPN. Route targets configured in VPN instance IPv6 VPN view apply only to the IPv6 VPN.

IPv4 VPN prefers the route targets configured in VPN instance IPv4 VPN view over those configured in VPN instance view.

IPv6 VPN prefers the route targets configured in VPN instance IPv6 VPN view over those configured in VPN instance view.

Examples

Configure route targets for VPN instance **vpn1**.

```
<Switch> system-view
[Switch] ip vpn-instance vpn1
[Switch-vpn-instance-vpn1] vpn-target 3:3 export-extcommunity
[Switch-vpn-instance-vpn1] vpn-target 4:4 import-extcommunity
[Switch-vpn-instance-vpn1] vpn-target 5:5 both
```

Contents

A page of this section is **7-x-x**

2. IPv6 MCE commands 2-1
2.1. IPv6 MCE commands 2-1
2.1.1. address-family ipv6 (VPN instance view) 2-1
2.1.2. vpn-instance-capability simple (OSPFv3 view) 2-1

2. IPv6 MCE commands

2.1. IPv6 MCE commands

This chapter describes only IPv6 MCE-specific commands. For information about the commands available for both IPv4 MCE and IPv6 MCE, see "MCE commands."

2.1.1. address-family ipv6 (VPN instance view)

Use **address-family ipv6** to enter VPN instance IPv6 VPN view.

Use **undo address-family ipv6** to remove all configurations from VPN instance IPv6 VPN view.

Syntax

address-family ipv6

undo address-family ipv6

Views

VPN instance view

Predefined user roles

network-admin

Usage guidelines

In VPN instance IPv6 VPN view, you can configure IPv6 VPN parameters such as inbound and outbound routing policies.

Examples

Enter VPN instance IPv6 VPN view.

```
<Switch> system-view
[Switch] ip vpn-instance vpn1
[Switch-vpn-instance-vpn1] address-family ipv6
[Switch-vpn-ipv6-vpn1]
```

Related commands

address-family ipv4 (VPN instance view)

2.1.2. vpn-instance-capability simple (OSPFv3 view)

Use **vpn-instance-capability simple** to disable routing loop detection for a VPN OSPFv3 process.

Use **undo vpn-instance-capability** to enable routing loop detection for a VPN OSPFv3 process.

Syntax

vpn-instance-capability simple

undo vpn-instance-capability

Default

Routing loop detection is enabled for a VPN OSPFv3 process.

Views

OSPFv3 view

Predefined user roles

network-admin

Usage guidelines

For the MCE to receive OSPFv3 routes from the PE, you must disable routing loop detection for a VPN OSPFv3 process on the MCE.

This command is applicable only to VPN OSPFv3 processes.

Examples

Disable routing loop detection for VPN OSPFv3 process 100.

```
<Switch> system-view
[Switch] ospfv3 100 vpn-instance vpn1
[Switch-ospfv3-100] vpn-instance-capability simple
```

QX-S5600G Series Ethernet Switches

Command References

8.ACL and QoS

This manual is including the following chapters.

01-ACL commands

02-QoS policy commands

03-Priority mapping commands

04-GTS and rate limit commands

05-Congestion management commands

06-Data buffer commands

07-Time range commands

Contents

A page of this section is **8-x-x**

1. ACL commands 1-1
1.1. ACL commands 1-1
1.1.1. acl 1-1
1.1.2. acl copy 1-3
1.1.3. acl logging interval 1-4
1.1.4. description 1-5
1.1.5. display acl 1-5
1.1.6. display packet-filter 1-7
1.1.7. display packet-filter statistics 1-8
1.1.8. display packet-filter statistics sum 1-11
1.1.9. display packet-filter verbose 1-12
1.1.10. display qos-acl resource 1-14
1.1.11. packet-filter 1-15
1.1.12. packet-filter filter 1-17
1.1.13. reset acl counter 1-17
1.1.14. reset packet-filter statistics 1-18
1.1.15. rule (IPv4 advanced ACL view) 1-19
1.1.16. rule (IPv4 basic ACL view) 1-24
1.1.17. rule (IPv6 advanced ACL view) 1-26
1.1.18. rule (IPv6 basic ACL view) 1-31
1.1.19. rule (Layer 2 ACL view) 1-33
1.1.20. rule comment 1-35
1.1.21. step 1-35

1. ACL commands

1.1. ACL commands

1.1.1. acl

Use **acl** to create an ACL and enter its view, or enter the view of an existing ACL.

Use **undo acl** to delete the specified or all ACLs.

Syntax

Command set 1:

acl [**ipv6**] { **name** *acl-name* | **number** *acl-number* [**name** *acl-name*] [**match-order** { **auto** | **config** }] }

undo acl [**ipv6**] { **all** | **name** *acl-name* | **number** *acl-number* }

Command set 2:

acl [**ipv6**] { **advanced** | **basic** } { *acl-number* | **name** *acl-name* } [**match-order** { **auto** | **config** }]

acl mac { *acl-number* | **name** *acl-name* } [**match-order** { **auto** | **config** }]

undo acl [**ipv6**] { **all** | { **advanced** | **basic** } { *acl-number* | **name** *acl-name* } }

undo acl mac { **all** | *acl-number* | **name** *acl-name* }

Default

No ACLs exist.

Views

System view

Predefined user roles

network-admin

Parameters

ipv6: Specifies the IPv6 ACL type. To specify the IPv4 ACL type, do not use this keyword.

basic: Specifies the basic ACL type.

advanced: Specifies the advanced ACL type.

mac: Specifies the Layer 2 ACL type.

acl-number: Assigns a number to the ACL. The following are available value ranges:

- 2000 to 2999 for basic ACLs.
- 3000 to 3999 for advanced ACLs.
- 4000 to 4999 for Layer 2 ACLs.

name *acl-name*: Assigns a name to the ACL. The *acl-name* argument is a case-insensitive string of 1 to 63 characters. It must start with an English letter and to avoid confusion, it cannot be **all**.

match-order: Specifies the order in which ACL rules are compared against packets.

- **auto**: Compares ACL rules in depth-first order.
- **config**: Compares ACL rules in ascending order of rule ID. The rule with a smaller ID has a higher priority. If you do not specify a match order, the **config** order applies by default.

all: Specifies all ACLs of the specified type.

Usage guidelines

If you create a numbered ACL, you can enter the view of the ACL by using the following commands:

- **acl** [**ipv6**] **number** *acl-number*
- **acl** { [**ipv6**] { **advanced** | **basic** } | **mac** } *acl-number*

If you create an ACL by using the **acl** [**ipv6**] **number** *acl-number* **name** *acl-name* command, you can enter the view of the ACL by using the following commands:

- **acl** [**ipv6**] **name** *acl-name* (for basic ACLs and advanced ACLs only)
- **acl** [**ipv6**] **number** *acl-number* [**name** *acl-name*]
- **acl** { [**ipv6**] { **advanced** | **basic** } | **mac** } **name** *acl-name*

If you create a named ACL by using the **acl** { [**ipv6**] { **advanced** | **basic** } | **mac** } **name** *acl-name* command, you can enter the view of the ACL by using the following commands:

- **acl** [**ipv6**] **name** *acl-name* (for basic ACLs and advanced ACLs only)
- **acl** { [**ipv6**] { **advanced** | **basic** } | **mac** } **name** *acl-name*

You can change the match order only for ACLs that do not contain any rules.

Matching packets are forwarded through slow forwarding if an ACL rule contains match criteria or has functions enabled in addition to the following match criteria and functions:

- Source and destination IP addresses.
- Source and destination ports.
- Transport layer protocol.
- ICMP or ICMPv6 message type, message code, and message name.
- Logging.
- Time range.

Slow forwarding requires packets to be sent to the control plane for forwarding entry calculation, which affects the device forwarding performance.

Examples

Create IPv4 basic ACL 2000 and enter its view.

```
<Switch> system-view
[Switch] acl basic 2000
[Switch-acl-ipv4-basic-2000]
```

Create IPv4 basic ACL **flow** and enter its view.

```
<Switch> system-view
[Switch] acl basic name flow
[Switch-acl-ipv4-basic-flow]
```

Create IPv4 advanced ACL 3000 and enter its view.

```
<Switch> system-view
[Switch] acl advanced 3000
[Switch-acl-ipv4-adv-3000]
```

Create IPv6 basic ACL 2000 and enter its view.

```
<Switch> system-view
[Switch] acl ipv6 basic 2000
[Switch-acl-ipv6-basic-2000]
```

Create IPv6 basic ACL **flow** and enter its view.

```
<Switch> system-view
[Switch] acl ipv6 basic name flow
[Switch-acl-ipv6-basic-flow]
```

Create IPv6 advanced ACL **abc** and enter its view.

```
<Switch> system-view
[Switch] acl ipv6 advanced name abc
[Switch-acl-ipv6-adv-abc]
```

Create Layer 2 ACL 4000 and enter its view.

```
<Switch> system-view
[Switch] acl mac 4000
[Switch-acl-mac-4000]
```

Create Layer 2 ACL **flow** and enter its view.

```
<Switch> system-view
[Switch] acl mac name flow
[Switch-acl-mac-flow]
```

Related commands

display acl

1.1.2. acl copy

Use **acl copy** to create an ACL by copying an ACL that already exists.

Syntax

acl [**ipv6** | **mac**] **copy** { *source-acl-number* | **name** *source-acl-name* } **to** { *dest-acl-number* | **name** *dest-acl-name* }

Views

System view

Predefined user roles

network-admin

Parameters

ipv6: Specifies the IPv6 ACL type.

mac: Specifies the Layer 2 ACL type.

source-acl-number: Specifies an existing source ACL by its number. The following are available value ranges:

- 2000 to 2999 for basic ACLs.
- 3000 to 3999 for advanced ACLs.
- 4000 to 4999 for Layer 2 ACLs.

name *source-acl-name*: Specifies an existing source ACL by its name. The *source-acl-name* argument is a case-insensitive string of 1 to 63 characters.

dest-acl-number: Assigns a unique number to the new ACL. The following are available value ranges:

- 2000 to 2999 for basic ACLs.
- 3000 to 3999 for advanced ACLs.
- 4000 to 4999 for Layer 2 ACLs.

name *dest-acl-name*: Assigns a unique name to the new ACL. The *dest-acl-name* argument is a case-insensitive string of 1 to 63 characters. It must start with an English letter and to avoid confusion, it cannot be **all**.

Usage guidelines

The new ACL and the source ACL must be the same type.

The new ACL has the same properties and content as the source ACL, but uses a different number or name from the source ACL.

To specify the IPv4 ACL type, do not specify the **ipv6** or **mac** keyword.

Examples

Create IPv4 basic ACL 2002 by copying IPv4 basic ACL 2001.

```
<Switch> system-view
[Switch] acl copy 2001 to 2002
```

Create IPv4 basic ACL **paste** by copying IPv4 basic ACL **test**.

```
<Switch> system-view
[Switch] acl copy name test to name paste
```

1.1.3. acl logging interval

Use **acl logging interval** to enable logging for packet filtering and set the interval.

Use **undo acl logging interval** to restore the default.

Syntax

acl logging interval *interval*

undo acl logging interval

Default

The interval is 0. The device does not generate log entries for packet filtering.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the interval at which log entries are generated and output. It must be a multiple of 5, in the range of 0 to 1440 minutes. To disable the logging, set the value to 0.

Usage guidelines

The logging feature is available for IPv4 or IPv6 ACL rules that have the **logging** keyword.

You can configure the ACL module to generate log entries for packet filtering and output them to the information center at the output interval. The log entry records the number of matching packets and the matched ACL rules. When the first packet of a flow matches an ACL rule, the output interval

starts. When the output interval ends, the device outputs a log entry for all matching packets. For more information about the information center, see *Network Management and Monitoring Configuration Guide*.

Examples

Configure the device to generate and output packet filtering log entries every 10 minutes.

```
<Switch> system-view
[Switch] acl logging interval 10
```

Related commands

rule (IPv4 advanced ACL view)

rule (IPv4 basic ACL view)

rule (IPv6 advanced ACL view)

rule (IPv6 basic ACL view)

1.1.4. description

Use **description** to configure a description for an ACL.

Use **undo description** to delete an ACL description.

Syntax

description *text*

undo description

Default

An ACL does not have a description.

Views

IPv4 basic/advanced ACL view

IPv6 basic/advanced ACL view

Layer 2 ACL view

Predefined user roles

network-admin

Parameters

text: Specifies a description, a case-sensitive string of 1 to 127 characters.

Examples

Configure a description for IPv4 basic ACL 2000.

```
<Switch> system-view
[Switch] acl basic 2000
[Switch-acl-ipv4-basic-2000] description This is an IPv4 basic ACL.
```

Related commands

display acl

1.1.5. display acl

Use **display acl** to display ACL configuration and match statistics.

Syntax

display acl [**ipv6** | **mac**] { *acl-number* | **all** | **name** *acl-name* }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ipv6: Specifies the IPv6 ACL type.

mac: Specifies the Layer 2 ACL type.

acl-number: Specifies an ACL by its number. The following are available value ranges:

- 2000 to 2999 for basic ACLs.
- 3000 to 3999 for advanced ACLs.
- 4000 to 4999 for Layer 2 ACLs.

all: Specifies all ACLs of the specified type.

name *acl-name*: Specifies an ACL by its name. The *acl-name* argument is a case-insensitive string of 1 to 63 characters.

Usage guidelines

This command displays ACL rules in **config** or **auto** order, whichever is configured.

To specify the IPv4 ACL type, do not specify the **ipv6** or **mac** keyword.

Examples

Display configuration and match statistics for IPv4 basic ACL 2001.

```
<Switch> display acl 2001
Basic IPv4 ACL 2001, 1 rule, match-order is auto,
This is an IPv4 basic ACL.
ACL's step is 5, start ID is 0
 rule 5 permit source 1.1.1.1 0
 rule 5 comment This rule is used on GigabitEthernet1/0/1.
```

Table 1-1 Command output

Field	Description
Basic IPv4 ACL 2001	Type and number of the ACL. The following field information is about IPv4 basic ACL 2001.
1 rule	The ACL contains one rule.
match-order is auto	The match order for the ACL is **auto**, which sorts ACL rules in depth-first order. This field is not displayed when the match order is **config**.
This is an IPv4 basic ACL.	Description of the ACL.
ACL's step is 5	The rule numbering step is 5.
start ID is 0	The start rule ID is 0.
rule 5 permit source 1.1.1.1	Content of rule 5. The rule permits packets sourced from the

Field	Description
0	IP address 1.1.1.1.
rule 5 comment This rule is used on GigabitEthernet1/0/1.	Comment of rule 5.

1.1.6. display packet-filter

Use **display packet-filter** to display ACL application information for packet filtering.

Syntax

display packet-filter interface [*interface-type interface-number*] [**inbound** | **outbound**] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface [*interface-type interface-number*]: Specifies an interface by its type and number. If you do not specify an interface, this command displays ACL application information for packet filtering on all interfaces. If you specify an Ethernet interface, you do not need to specify the **slot** *slot-number* option.

inbound: Specifies the inbound direction.

outbound: Specifies the outbound direction.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays ACL application information for packet filtering for the master device.

Usage guidelines

If neither the **inbound** keyword nor the **outbound** keyword is specified, this command displays ACL application information for packet filtering in both directions.

Examples

Display ACL application information for inbound packet filtering on interface GigabitEthernet 1/0/1.

```
<Switch> display packet-filter interface gigabitethernet 1/0/1 inbound
Interface: GigabitEthernet1/0/1
 Inbound policy:
  IPv4 ACL 2001
  IPv6 ACL 2002 (Failed)
  MAC ACL 4003
```

Table 1-2 Command output

Field	Description
Interface	Interface to which the ACL applies.
Inbound policy	ACL used for filtering incoming traffic.

Field	Description
Outbound policy	ACL used for filtering outgoing traffic.
IPv4 ACL 2001	IPv4 basic ACL 2001 has been successfully applied.
IPv6 ACL 2002 (Failed)	The device has failed to apply IPv6 basic ACL 2002.
Hardware-count	ACL rule match counting in hardware has been successfully enabled.
Hardware-count (Failed)	The device has failed to enable counting ACL rule matches in hardware.
IPv4 default action	Packet filter default action for packets that do not match any IPv4 ACLs: • **Deny**—The default action **deny** has been successfully applied for packet filtering. • **Deny (Failed)**—The device has failed to apply the default action **deny** for packet filtering. The action **permit** still functions. • **Permit**—The default action **permit** has been successfully applied for packet filtering.
IPv6 default action	Packet filter default action for packets that do not match any IPv6 ACLs: • **Deny**—The default action **deny** has been successfully applied for packet filtering. • **Deny (Failed)**—The device has failed to apply the default action **deny** for packet filtering. The action **permit** still functions. • **Permit**—The default action **permit** has been successfully applied for packet filtering.
MAC default action	Packet filter default action for packets that do not match any Layer 2 ACLs: • **Deny**—The default action **deny** has been successfully applied for packet filtering. • **Deny (Failed)**—The device has failed to apply the default action **deny** for packet filtering. The action **permit** still functions. • **Permit**—The default action **permit** has been successfully applied for packet filtering.

1.1.7. display packet-filter statistics

Use **display packet-filter statistics** to display packet filtering statistics.

Syntax

display packet-filter statistics interface *interface-type interface-number* { **inbound** | **outbound** } [[**ipv6** | **mac**] { *acl-number* | **name** *acl-name* }] [**brief**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number.

inbound: Specifies the inbound direction.

outbound: Specifies the outbound direction.

ipv6: Specifies the IPv6 ACL type.

mac: Specifies the Layer 2 ACL type.

acl-number: Specifies an ACL by its number.

- 2000 to 2999 for basic ACLs.
- 3000 to 3999 for advanced ACLs.
- 4000 to 4999 for Layer 2 ACLs.

name *acl-name*: Specifies an ACL by its name. The *acl-name* argument is a case-insensitive string of 1 to 63 characters.

brief: Displays brief statistics.

Usage guidelines

If *acl-number*, **name** *acl-name*, **ipv6**, or **mac** is not specified, this command displays packet filtering statistics for all ACLs.

To specify the IPv4 ACL type, do not specify the **ipv6** or **mac** keyword.

Examples

Display packet filtering statistics for all ACLs on incoming packets of GigabitEthernet 1/0/1.

```
<Switch> display packet-filter statistics interface gigabitethernet 1/0/1 inbound
Interface: GigabitEthernet1/0/1
 Inbound policy:
  IPv4 ACL 2001, Hardware-count
   From 2011-06-04 10:25:21 to 2011-06-04 10:35:57
   rule 0 permit source 2.2.2.2 0 (2 packets)
   rule 5 permit source 1.1.1.1 0 (Failed)
   Totally 2 packets permitted, 0 packets denied
   Totally 100% permitted, 0% denied

  IPv6 ACL 2000

  MAC ACL 4000
   rule 0 permit
```

Table 1-3 Command output

Field	Description
Interface	Interface to which the ACL applies.
Inbound policy	ACL used for filtering incoming traffic.
Outbound policy	ACL used for filtering outgoing traffic.
IPv4 ACL 2001	IPv4 basic ACL 2001 has been successfully applied.
IPv4 ACL 2002 (Failed)	The device has failed to apply IPv4 basic ACL 2002.

Field	Description
Hardware-count	ACL rule match counting in hardware has been successfully enabled.
Hardware-count (Failed)	The device has failed to enable counting ACL rule matches in hardware.
From 2011-06-04 10:25:21 to 2011-06-04 10:35:57	Start time and end time of the statistics.
2 packets	Two packets matched the rule. This field is not displayed when no packets matched the rule.
No resource	Resources are not enough for counting matches for the rule. In packet filtering statistics, this field is displayed for a rule when resources are not sufficient for rule match counting.
rule 5 permit source 1.1.1.1 0 (Failed)	The device has failed to apply rule 5.
Totally 2 packets permitted, 0 packets denied	Number of packets permitted and denied by the ACL.
Totally 100% permitted, 0% denied	Ratios of permitted and denied packets to all packets.
IPv4 default action	Packet filter default action for packets that do not match any IPv4 ACLs: • **Deny**—The default action **deny** has been successfully applied for packet filtering. • **Deny (Failed)**—The device has failed to apply the default action **deny** for packet filtering. The action **permit** still functions. • **Permit**—The default action **permit** has been successfully applied for packet filtering.
IPv6 default action	Packet filter default action for packets that do not match any IPv6 ACLs: • **Deny**—The default action **deny** has been successfully applied for packet filtering. • **Deny (Failed)**—The device has failed to apply the default action **deny** for packet filtering. The action **permit** still functions. • **Permit**—The default action **permit** has been successfully applied for packet filtering.
MAC default action	Packet filter default action for packets that do not match any Layer 2 ACLs: • **Deny**—The default action **deny** has been successfully applied for packet filtering. • **Deny (Failed)**—The device has failed to apply the default action **deny** for packet filtering. The action **permit** still functions. • **Permit**—The default action **permit** has been successfully applied for packet filtering.

Related commands

reset packet-filter statistics

1.1.8. display packet-filter statistics sum

Use **display packet-filter statistics sum** to display accumulated packet filtering statistics for an ACL.

Syntax

display packet-filter statistics sum { **inbound** | **outbound** } [**ipv6** | **mac**] { *acl-number* | **name** *acl-name* } [**brief**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

inbound: Specifies the inbound direction.

outbound: Specifies the outbound direction.

ipv6: Specifies the IPv6 ACL type.

mac: Specifies the Layer 2 ACL type.

acl-number: Specifies an ACL by its number.

- 2000 to 2999 for basic ACLs.
- 3000 to 3999 for advanced ACLs.
- 4000 to 4999 for Layer 2 ACLs.

name *acl-name*: Specifies an ACL by its name. The *acl-name* argument is a case-insensitive string of 1 to 63 characters.

brief: Displays brief statistics.

Usage guidelines

To specify the IPv4 ACL type, do not specify the **ipv6** or **mac** keyword.

Examples

Display accumulated packet filtering statistics for IPv4 basic ACL 2001 on incoming packets.

```
<Switch> display packet-filter statistics sum inbound 2001
Sum:
 Inbound policy:
  IPv4 ACL 2001
   rule 0 permit source 2.2.2.2 0 (2 packets)
   rule 5 permit source 1.1.1.1 0
   Totally 2 packets permitted, 0 packets denied
   Totally 100% permitted, 0% denied
```

Display brief accumulated packet filtering statistics for IPv4 basic ACL 2000 on incoming packets.

```
<Switch> display packet-filter statistics sum inbound 2000 brief
Sum:
 Inbound policy:
  IPv4 ACL 2000
```

```
Totally 2 packets permitted, 0 packets denied
Totally 100% permitted, 0% denied
```

Table 1-4 Command output

Field	Description
Sum	Accumulated packet filtering statistics.
Inbound policy	Accumulated packet filtering statistics in the inbound direction.
Outbound policy	Accumulated packet filtering statistics in the outbound direction.
IPv4 ACL 2001	Accumulated packet filtering statistics of IPv4 basic ACL 2001.
2 packets	Two packets matched the rule. This field is not displayed when no packets matched the rule.
Totally 2 packets permitted, 0 packets denied	Number of packets permitted and denied by the ACL.
Totally 100% permitted, 0% denied	Ratios of permitted and denied packets to all packets.

Related commands

reset packet-filter statistics

1.1.9. display packet-filter verbose

Use **display packet-filter verbose** to display ACL application details for packet filtering.

Syntax

display packet-filter verbose interface *interface-type interface-number* { **inbound** | **outbound** } [[**ipv6** | **mac**] { *acl-number* | **name** *acl-name* }] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. The **slot** *slot-number* option is not available for an Ethernet interface.

inbound: Specifies the inbound direction.

outbound: Specifies the outbound direction.

ipv6: Specifies the IPv6 ACL type.

mac: Specifies the Layer 2 ACL type.

acl-number: Specifies an ACL by its number.

- 2000 to 2999 for basic ACLs.

- 3000 to 3999 for advanced ACLs.
- 4000 to 4999 for Layer 2 ACLs.

name *acl-name*: Specifies an ACL by its name. The *acl-name* argument is a case-insensitive string of 1 to 63 characters.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays ACL application details for packet filtering for the master device.

Usage guidelines

If *acl-number*, **name** *acl-name*, **ipv6**, or **mac** is not specified, this command displays application details of all ACLs for packet filtering.

To specify the IPv4 ACL type, do not specify the **ipv6** or **mac** keyword.

Examples

Display application details of all ACLs for inbound packet filtering on GigabitEthernet 1/0/1.

```
<Switch> display packet-filter verbose interface gigabitethernet 1/0/1 inbound
Interface: GigabitEthernet1/0/1
 Inbound policy:
  IPv4 ACL 2001
   rule 0 permit
   rule 5 permit source 1.1.1.1 0 (Failed)

  IPv6 ACL 2000
   rule 0 permit

  MAC ACL 4000

  IPv4 default action: Deny

  IPv6 default action: Deny, Hardware-count

  MAC default action: Deny
```

Table 1-5 Command output

Field	Description
Interface	Interface to which the ACL applies.
Inbound policy	ACL used for filtering incoming traffic.
Outbound policy	ACL used for filtering outgoing traffic.
IPv4 ACL 2001	IPv4 basic ACL 2001 has been successfully applied.
IPv4 ACL 2002 (Failed)	The device has failed to apply IPv4 basic ACL 2002.
Hardware-count	ACL rule match counting in hardware has been successfully enabled.
Hardware-count (Failed)	The device has failed to enable counting ACL rule matches in hardware.
rule 5 permit source 1.1.1.1 0 (Failed)	The device has failed to apply rule 5.

Field	Description
IPv4 default action	Packet filter default action for packets that do not match any IPv4 ACLs: • **Deny**—The default action **deny** has been successfully applied for packet filtering. • **Deny (Failed)**—The device has failed to apply the default action **deny** for packet filtering. The action **permit** still functions. • **Permit**—The default action **permit** has been successfully applied for packet filtering.
IPv6 default action	Packet filter default action for packets that do not match any IPv6 ACLs: • **Deny**—The default action **deny** has been successfully applied for packet filtering. • **Deny (Failed)**—The device has failed to apply the default action **deny** for packet filtering. The action **permit** still functions. • **Permit**—The default action **permit** has been successfully applied for packet filtering.
MAC default action	Packet filter default action for packets that do not match any Layer 2 ACLs: • **Deny**—The default action **deny** has been successfully applied for packet filtering. • **Deny (Failed)**—The device has failed to apply the default action **deny** for packet filtering. The action **permit** still functions. • **Permit**—The default action **permit** has been successfully applied for packet filtering.

1.1.10. display qos-acl resource

Use **display qos-acl resource** to display QoS and ACL resource usage.

Syntax

display qos-acl resource [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays QoS and ACL resource usage for all member devices.

Examples

Display QoS and ACL resource usage.

```
<Switch> display qos-acl resource
Interfaces: GE1/0/1 to GE1/0/24, XGE1/0/25 to XGE1/0/28
            GE1/1/1 to GE1/1/8 (slot 1)
```

```
-------------------------------------------------------------------------
 Type              Total      Reserved   Configured Remaining  Usage
-------------------------------------------------------------------------
 TTI ACL           3072       0          2          3070       0%
 IPCL0+IPCL2 ACL   1024       32         5          987        3%
 IPCL Counter      2048       28         2          2018       1%
 EPCL+IPCL1 ACL    512        0          0          512        0%
 EPCL Counter      1024       0          0          1024       0%
 IPCL Meter        4888       30         0          4858       0%
 EPCL Meter        4096       0          0          4096       0%
```

Table 1-6 Command output

Field	Description
Interfaces	Interface range for the resources.
Type	Resource type: • **TTI ACL**—ACL resources used for tunnel termination and interfaces. • **IPCL0+IPCL2 ACL**—ACL resources used for inbound policies. • **IPCL Counter**—Accounting resources used for inbound policies. • **EPCL+IPCL1 ACL**—ACL resources used for inbound and outbound policies. • **EPCL Counter**—Accounting resources used for outbound policies. • **IPCL Meter**—Traffic policing resources used in inbound QoS policies. • **EPCL Meter**—Traffic policing resources used in outbound QoS policies.
Total	Total number of resources.
Reserved	Number of reserved resources.
Configured	Number of resources that has been applied.
Remaining	Number of resources that you can apply.
Usage	Configured and reserved resources as a percentage of total resources. If the percentage is not an integer, this field displays the integer part. For example, if the actual usage is 50.8%, this field displays 50%.

1.1.11. packet-filter

Use **packet-filter** to apply an ACL to an interface to filter packets.

Use **undo packet-filter** to remove an ACL from an interface.

Syntax

packet-filter [**ipv6** | **mac**] { *acl-number* | **name** *acl-name* } { **inbound** | **outbound** } [**hardware-count**]

undo packet-filter [**ipv6** | **mac**] { *acl-number* | **name** *acl-name* } { **inbound** | **outbound** }

Default

No ACL is applied to an interface to filter packets.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

VLAN interface view

VSI interface view

Predefined user roles

network-admin

Parameters

ipv6: Specifies the IPv6 ACL type.

mac: Specifies the Layer 2 ACL type.

acl-number: Specifies an ACL by its number.

- 2000 to 2999 for basic ACLs.
- 3000 to 3999 for advanced ACLs.
- 4000 to 4999 for Layer 2 ACLs.

name *acl-name*: Specifies an ACL by its name. The *acl-name* argument is a case-insensitive string of 1 to 63 characters.

inbound: Filters incoming packets.

outbound: Filters outgoing packets.

hardware-count: Enables counting ACL rule matches performed in hardware. If you do not specify this keyword, rule matches for the ACL are not counted in hardware.

Usage guidelines

To specify the IPv4 ACL type, do not specify the **ipv6** or **mac** keyword.

The **hardware-count** keyword in this command enables match counting in hardware for all rules in an ACL, and the **counting** keyword in the **rule** command enables match counting specific to rules.

To disable ACL rule match counting in hardware when resources are insufficient, you must execute the **undo packet-filter** command and then reconfigure the **packet-filter** command without specifying the **hardware-count** keyword.

To disable ACL rule match counting in hardware when resources are sufficient, you can directly reconfigure the **packet-filter** command without specifying the **hardware-count** keyword.

To the same direction of an interface, you can apply a maximum of three ACLs: one IPv4 ACL, one IPv6 ACL, and one Layer 2 ACL.

Examples

Apply IPv4 basic ACL 2001 to filter incoming traffic on GigabitEthernet 1/0/1, and enable counting ACL rule matches performed in hardware.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] packet-filter 2001 inbound hardware-count
```

Related commands

display packet-filter

display packet-filter statistics

display packet-filter verbose

NOTE:

When you configure same **packet-filter** command in same vlan-interface, the packet-filter is conflicted on the vlan-interface. You can check the failed command by **display packet-filter verbose interface Vlan-interface** command.

1.1.12. packet-filter filter

NOTE:

packet-filter filter command is being supported with after Ver7.2.17.

Use **packet-filter filter** to specify the applicable scope of packet filtering on a VLAN interface.

Use **undo packet-filter filter** to restore the default.

Syntax

packet-filter filter [**route** | **all**]

undo packet-filter filter

Default

The packet filtering filters packets forwarded at Layer 3.

Views

VLAN interface view

Predefined user roles

network-admin

Parameters

route: Filters packets forwarded at Layer 3 by the VLAN interface.

all: Filters all packets, including packets forwarded at Layer 3 by the VLAN interface and packets forwarded at Layer 2 by the physical ports associated with the VLAN interface.

Examples

Configure the packet filtering on VLAN-interface 2 to filter packets forwarded at Layer 3.

```
<Switch> system-view
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] packet-filter filter route
```

1.1.13. reset acl counter

Use **reset acl counter** to clear statistics for ACLs.

Syntax

reset acl [**ipv6** | **mac**] **counter** { *acl-number* | **all** | **name** *acl-name* }

Views

User view

Predefined user roles

network-admin

Parameters

ipv6: Specifies the IPv6 ACL type.

mac: Specifies the Layer 2 ACL type.

acl-number: Specifies an ACL by its number.

- 2000 to 2999 for basic ACLs.
- 3000 to 3999 for advanced ACLs.
- 4000 to 4999 for Layer 2 ACLs.

all: Clears statistics for all ACLs of the specified type.

name *acl-name*: Clears statistics of an ACL specified by its name. The *acl-name* argument is a case-insensitive string of 1 to 63 characters.

Usage guidelines

To specify the IPv4 ACL type, do not specify the **ipv6** or **mac** keyword.

Examples

Clear statistics for IPv4 basic ACL 2001.

```
<Switch> reset acl counter 2001
```

Related commands

display acl

1.1.14. reset packet-filter statistics

Use **reset packet-filter statistics** to clear the packet filtering statistics.

Syntax

reset packet-filter statistics interface [*interface-type interface-number*] { **inbound** | **outbound** } [[**ipv6** | **mac**] { *acl-number* | **name** *acl-name* }]

Views

User view

Predefined user roles

network-admin

Parameters

interface [*interface-type interface-number*]: Specifies an interface by its type and number. If you do not specify an interface, this command clears packet filtering statistics for all interfaces.

inbound: Specifies the inbound direction.

outbound: Specifies the outbound direction.

ipv6: Specifies the IPv6 ACL type.

mac: Specifies the Layer 2 ACL type.

acl-number: Specifies an ACL by its number.

- 2000 to 2999 for basic ACLs.
- 3000 to 3999 for advanced ACLs.
- 4000 to 4999 for Layer 2 ACLs.

name *acl-name*: Specifies an ACL by its name. The *acl-name* argument is a case-insensitive string of 1 to 63 characters.

Usage guidelines

If *acl-number*, **name** *acl-name*, **ipv6**, or **mac** is not specified, this command clears the packet filtering statistics for all ACLs.

To specify the IPv4 ACL type, do not specify the **ipv6** or **mac** keyword.

Examples

Clear IPv4 basic ACL 2001 statistics for inbound packet filtering on GigabitEthernet 1/0/1.

```
<Switch> reset packet-filter statistics interface gigabitethernet 1/0/1 inbound 2001
```

Related commands

display packet-filter statistics

display packet-filter statistics sum

1.1.15. rule (IPv4 advanced ACL view)

Use **rule** to create or edit an IPv4 advanced ACL rule.

Use **undo rule** to delete an entire IPv4 advanced ACL rule or some attributes in the rule.

Syntax

rule [*rule-id*] { **deny** | **permit** } *protocol* [{ { **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } * | **established** } | **counting** | **destination** { *dest-address dest-wildcard* | **any** } | **destination-port** *operator port* | { **dscp** *dscp* | { **precedence** *precedence* | **tos** *tos* } * } | **fragment** | **icmp-type** { *icmp-type* [*icmp-code*] | *icmp-message* } | **logging** | **source** { *source-address source-wildcard* | **any** } | **source-port** *operator port* | **time-range** *time-range-name*] *

undo rule *rule-id* [{ { **ack** | **fin** | **psh** | **rst** | **syn** | **urg** } * | **established** } | **counting** | **destination** | **destination-port** | { **dscp** | { **precedence** | **tos** } * } | **fragment** | **icmp-type** | **logging** | **source** | **source-port** | **time-range**] *

undo rule { **deny** | **permit** } *protocol* [{ { **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } * | **established** } | **counting** | **destination** { *dest-address dest-wildcard* | **any** } | **destination-port** *operator port* | { **dscp** *dscp* | { **precedence** *precedence* | **tos** *tos* } * } | **fragment** | **icmp-type** { *icmp-type* [*icmp-code*] | *icmp-message* } | **logging** | **source** { *source-address source-wildcard* | **any** } | **source-port** *operator port* | **time-range** *time-range-name*] *

Default

No IPv4 advanced ACL rules exist.

Views

IPv4 advanced ACL view

Predefined user roles

network-admin

Parameters

rule-id: Specifies a rule ID in the range of 0 to 65534. If you do not specify a rule ID when creating an ACL rule, the system automatically assigns it a rule ID. This rule ID is the nearest higher multiple of the numbering step to the current highest rule ID, starting from the start rule ID. For example, if the rule numbering step is 5 and the current highest rule ID is 28, the rule is numbered 30.

deny: Denies matching packets.

permit: Allows matching packets to pass.

protocol: Specifies one of the following values:

- A protocol number in the range of 0 to 255.
- A protocol by its name: **gre** (47), **icmp** (1), **igmp** (2), **ip**, **ipinip** (4), **ospf** (89), **tcp** (6), or **udp** (17). The **ip** keyword specifies all protocols.

Table 1-7 describes the parameters that you can specify regardless of the value for the *protocol* argument.

Table 1-7 Match criteria and other rule information for IPv4 advanced ACL rules

Parameters	Function	Description
source { *source-address source-wildcard* | **any** }	Specifies a source address.	The *source-address source-wildcard* arguments specify a source IP address and a wildcard mask in dotted decimal notation. An all-zero wildcard represents a host address. The **any** keyword specifies any source IP address.
destination { *dest-address dest-wildcard* | **any** }	Specifies a destination address.	The *dest-address dest-wildcard* arguments specify a destination IP address and a wildcard mask in dotted decimal notation. An all-zero wildcard mask represents a host address. The **any** keyword represents any destination IP address.
counting	Enables rule match counting in software.	The **counting** keyword enables match counting specific to rules, and the **hardware-count** keyword in the **packet-filter** command enables match counting in hardware for all rules in an ACL. If the **counting** keyword is not specified, matches for the rule are not counted in software.
precedence *precedence*	Specifies an IP precedence value.	The *precedence* argument can be a number in the range of 0 to 7, or in words: **routine** (0), **priority** (1), **immediate** (2), **flash** (3), **flash-override** (4), **critical** (5),

Parameters	Function	Description
		internet (6), or **network** (7).
tos *tos*	Specifies a ToS preference.	The *tos* argument can be a number in the range of 0 to 15, or in words: **max-reliability** (2), **max-throughput** (4), **min-delay** (8), **min-monetary-cost** (1), or **normal** (0).
dscp *dscp*	Specifies a DSCP priority.	The *dscp* argument can be a number in the range of 0 to 63, or in words: **af11** (10), **af12** (12), **af13** (14), **af21** (18), **af22** (20), **af23** (22), **af31** (26), **af32** (28), **af33** (30), **af41** (34), **af42** (36), **af43** (38), **cs1** (8), **cs2** (16), **cs3** (24), **cs4** (32), **cs5** (40), **cs6** (48), **cs7** (56), **default** (0), or **ef** (46).
fragment	Applies the rule only to fragments.	If you do not specify this keyword, the rule applies to all fragments and non-fragments.
logging	Logs matching packets.	This feature requires that the module (for example, packet filtering) that uses the ACL supports logging.
time-range *time-range-name*	Specifies a time range for the rule.	The *time-range-name* argument is a case-insensitive string of 1 to 32 characters. It must start with an English letter. If the time range is not configured, the system creates the rule. However, the rule using the time range can take effect only after you configure the time range. For more information about time range, see *ACL and QoS Configuration Guide*.

If the *protocol* argument is **tcp** (6) or **udp** (17), set the parameters shown in Table 1-8 .

Table 1-8 TCP/UDP-specific parameters for IPv4 advanced ACL rules

Parameters	Function	Description
source-port *operator port*	Specifies one or more UDP or TCP source ports.	The *operator* argument can be **eq** (equal to). The *port* argument is TCP or UDP port numbers in the range of 0 to 65535. TCP port numbers can be represented as: **chargen** (19), **bgp** (179), **cmd** (514), **daytime** (13), **discard** (9), **dns** (53), **domain** (53), **echo** (7), **exec** (512), **finger** (79), **ftp** (21), **ftp-data** (20), **gopher** (70), **hostname** (101), **irc** (194), **klogin** (543), **kshell** (544), **login** (513), **lpd** (515), **nntp** (119), **pop2** (109), **pop3** (110), **smtp** (25), **sunrpc** (111), **tacacs** (49), **talk** (517), **telnet** (23), **time** (37), **uucp** (540), **whois** (43), and **www** (80). UDP port numbers can be represented as: **biff** (512), **bootpc** (68), **bootps** (67), **discard** (9), **dns** (53), **dnsix** (90), **echo** (7), **mobilip-ag** (434), **mobilip-mn** (435), **nameserver** (42), **netbios-dgm** (138), **netbios-ns** (137), **netbios-ssn** (139), **ntp**
destination-port *operator port*	Specifies one or more UDP or TCP destination ports.	

Parameters	Function	Description
		(123), **rip** (520), **snmp** (161), **snmptrap** (162), **sunrpc** (111), **syslog** (514), **tacacs-ds** (65), **talk** (517), **tftp** (69), **time** (37), **who** (513), and **xdmcp** (177).
{ **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* }*	Specifies one or more TCP flags including ACK, FIN, PSH, RST, SYN, and URG.	Parameters specific to TCP. The value for each argument can be 0 (flag bit not set) or 1 (flag bit set). The TCP flags in a rule are ANDed. For example, a rule configured with **ack** 0 **psh** 1 matches packets that have the ACK flag bit not set and the PSH flag bit set.
established	Specifies the flags for indicating the established status of a TCP connection.	Parameter specific to TCP. The rule matches TCP connection packets with the ACK or RST flag bit set.

If the *protocol* argument is **icmp** (1), set the parameters shown in Table 1-9 .

Table 1-9 ICMP-specific parameters for IPv4 advanced ACL rules

Parameters	Function	Description
icmp-type { *icmp-type* *icmp-code* | *icmp-message* }	Specifies the ICMP message type and code.	The *icmp-type* argument is in the range of 0 to 255. The *icmp-code* argument is in the range of 0 to 255. The *icmp-message* argument specifies a message name. Supported ICMP message names and their corresponding type and code values are listed in Table 1-10 .

Table 1-10 ICMP message names supported in IPv4 advanced ACL rules

ICMP message name	ICMP message type	ICMP message code
echo	8	0
echo-reply	0	0
fragmentneed-DFset	3	4
host-redirect	5	1
host-tos-redirect	5	3
host-unreachable	3	1
information-reply	16	0
information-request	15	0
net-redirect	5	0
net-tos-redirect	5	2
net-unreachable	3	0
parameter-problem	12	0

ICMP message name	ICMP message type	ICMP message code
port-unreachable	3	3
protocol-unreachable	3	2
reassembly-timeout	11	1
source-quench	4	0
source-route-failed	3	5
timestamp-reply	14	0
timestamp-request	13	0
ttl-exceeded	11	0

Usage guidelines

Within an ACL, the permit or deny statement of each rule must be unique. If the rule you are creating or editing has the same deny or permit statement as another rule in the ACL, the rule will not be created or changed.

You can edit ACL rules only when the match order is **config**.

When an IPv4 advanced ACL is used for QoS traffic classification or packet filtering in a VXLAN network, the ACL matches packets as follows:

- If the ACL is applied to the outgoing VXLAN packets on a VTEP, the ACL matches outer IPv4 header information.
- If the ACL is applied to the incoming VXLAN packets on a VTEP, the ACL matches inner IPv4 header information.
- If the ACL is applied to the incoming VXLAN packets on an intermediate transport device, the ACL matches outer IPv4 header information.

To view the existing IPv4 basic and advanced ACL rules, use the **display acl all** command.

The **undo rule** *rule-id* command without any optional parameters deletes an entire rule. If you specify optional parameters, the **undo rule** *rule-id* command deletes the specified attributes for the rule.

The **undo rule** { **deny** | **permit** } command can only be used to delete an entire rule. You must specify all the attributes of the rule for the command.

Examples

Create an IPv4 advanced ACL rule to permit TCP packets with the destination port 80 from 129.9.0.0/16 to 202.38.160.0/24.

```
<Switch> system-view
[Switch] acl advanced 3000
[Switch-acl-ipv4-adv-3000] rule permit tcp source 129.9.0.0 0.0.255.255 destination
202.38.160.0 0.0.0.255 destination-port eq 80
```

Create IPv4 advanced ACL rules to permit all IP packets but the ICMP packets destined for 192.168.1.0/24.

```
<Switch> system-view
[Switch] acl advanced 3001
[Switch-acl-ipv4-adv-3001] rule deny icmp destination 192.168.1.0 0.0.0.255
[Switch-acl-ipv4-adv-3001] rule permit ip
```

Create IPv4 advanced ACL rules to permit inbound and outbound FTP packets.

```
<Switch> system-view
```

```
[Switch] acl advanced 3002
[Switch-acl-ipv4-adv-3002] rule permit tcp source-port eq ftp
[Switch-acl-ipv4-adv-3002] rule permit tcp source-port eq ftp-data
[Switch-acl-ipv4-adv-3002] rule permit tcp destination-port eq ftp
[Switch-acl-ipv4-adv-3002] rule permit tcp destination-port eq ftp-data
```

Create IPv4 advanced ACL rules to permit inbound and outbound SNMP and SNMP trap packets.

```
<Switch> system-view
[Switch] acl advanced 3003
[Switch-acl-ipv4-adv-3003] rule permit udp source-port eq snmp
[Switch-acl-ipv4-adv-3003] rule permit udp source-port eq snmptrap
[Switch-acl-ipv4-adv-3003] rule permit udp destination-port eq snmp
[Switch-acl-ipv4-adv-3003] rule permit udp destination-port eq snmptrap
```

Related commands

acl

acl logging interval

display acl

step

time-range

1.1.16. rule (IPv4 basic ACL view)

Use **rule** to create or edit an IPv4 basic ACL rule.

Use **undo rule** to delete an entire IPv4 basic ACL rule or some attributes in the rule.

Syntax

rule [*rule-id*] { **deny** | **permit** } [**counting** | **fragment** | **logging** | **source** { *source-address source-wildcard* | **any** } | **time-range** *time-range-name*] *

undo rule *rule-id* [**counting** | **fragment** | **logging** | **source** | **time-range**] *

undo rule { **deny** | **permit** } [**counting** | **fragment** | **logging** | **source** { *source-address source-wildcard* | **any** } | **time-range** *time-range-name*] *

Default

No IPv4 basic ACL rules exist.

Views

IPv4 basic ACL view

Predefined user roles

network-admin

Parameters

rule-id: Specifies a rule ID in the range of 0 to 65534. If you do not specify a rule ID when creating an ACL rule, the system automatically assigns it a rule ID. This rule ID is the nearest higher multiple of the numbering step to the current highest rule ID, starting from the start rule ID. For example, if the rule numbering step is 5 and the current highest rule ID is 28, the rule is numbered 30.

deny: Denies matching packets.

permit: Allows matching packets to pass.

counting: Enables rule match counting in software. If you do not specify this keyword, matches for the rule are not counted in software.

fragment: Applies the rule only to fragments. If you do not specify this keyword, the rule applies to both fragments and non-fragments.

logging: Logs matching packets. This feature is available only when the application module (for example, packet filtering) that uses the ACL supports the logging feature.

source { *source-address source-wildcard* | **any** }: Matches a source address. The *source-address* and *source-wildcard* arguments specify a source IP address and a wildcard mask in dotted decimal notation. A wildcard mask of zeros represents a host address. The **any** keyword represents any source IP address.

time-range *time-range-name*: Specifies a time range for the rule. The *time-range-name* argument is a case-insensitive string of 1 to 32 characters. It must start with an English letter. If the time range is not configured, the system creates the rule. However, the rule using the time range can take effect only after you configure the time range. For more information about time range, see *ACL and QoS Configuration Guide*.

Usage guidelines

Within an ACL, the permit or deny statement of each rule must be unique. If the rule you are creating or editing has the same deny or permit statement as another rule in the ACL, the rule will not be created or changed.

You can edit ACL rules only when the match order is **config**.

When an IPv4 basic ACL is used for QoS traffic classification or packet filtering in a VXLAN network, the ACL matches packets as follows:

- If the ACL is applied to the outgoing VXLAN packets on a VTEP, the ACL matches outer IPv4 header information.
- If the ACL is applied to the incoming VXLAN packets on a VTEP, the ACL matches inner IPv4 header information.
- If the ACL is applied to the incoming VXLAN packets on an intermediate transport device, the ACL matches outer IPv4 header information.

The **counting** keyword in this command enables match counting specific to rules, and the **hardware-count** keyword in the **packet-filter** command enables match counting in hardware for all rules in an ACL.

To view the existing IPv4 basic and advanced ACL rules, use the **display acl all** command.

The **undo rule** *rule-id* command without any optional parameters deletes an entire rule. If you specify optional parameters, the **undo rule** *rule-id* command deletes the specified attributes for the rule.

The **undo rule** { **deny** | **permit** } command can only be used to delete an entire rule. You must specify all the attributes of the rule for the command.

Examples

Create a rule in IPv4 basic ACL 2000 to deny the packets from any source IP subnet but 10.0.0.0/8, 172.17.0.0/16, or 192.168.1.0/24.

```
<Switch> system-view
[Switch] acl basic 2000
[Switch-acl-ipv4-basic-2000] rule permit source 10.0.0.0 0.255.255.255
[Switch-acl-ipv4-basic-2000] rule permit source 172.17.0.0 0.0.255.255
[Switch-acl-ipv4-basic-2000] rule permit source 192.168.1.0 0.0.0.255
[Switch-acl-ipv4-basic-2000] rule deny source any
```

Related commands

acl

acl logging interval

display acl

step

time-range

1.1.17. rule (IPv6 advanced ACL view)

Use **rule** to create or edit an IPv6 advanced ACL rule.

Use **undo rule** to delete an entire IPv6 advanced ACL rule or some attributes in the rule.

Syntax

rule [*rule-id*] { **deny** | **permit** } *protocol* [{ { **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } * | **established** } | **counting** | **destination** { *dest-address dest-prefix* | *dest-address/dest-prefix* | **any** } | **destination-port** *operator port* | **dscp** *dscp* | **flow-label** *flow-label-value* | **fragment** | **icmp6-type** { *icmp6-type icmp6-code* | *icmp6-message* } | **logging** | **routing** [**type** *routing-type*] | **source** { *source-address source-prefix* | *source-address/source-prefix* | **any** } | **source-port** *operator port* | **time-range** *time-range-name*] *

undo rule *rule-id* [{ { **ack** | **fin** | **psh** | **rst** | **syn** | **urg** } * | **established** } | **counting** | **destination** | **destination-port** | **dscp** | **flow-label** | **fragment** | **icmp6-type** | **logging** | **routing** | **source** | **source-port** | **time-range**] *

undo rule { **deny** | **permit** } *protocol* [{ { **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } * | **established** } | **counting** | **destination** { *dest-address dest-prefix* | *dest-address/dest-prefix* | **any** } | **destination-port** *operator port* | **dscp** *dscp* | **flow-label** *flow-label-value* | **fragment** | **icmp6-type** { *icmp6-type icmp6-code* | *icmp6-message* } | **logging** | **routing** [**type** *routing-type*] | **source** { *source-address source-prefix* | *source-address/source-prefix* | **any** } | **source-port** *operator port* | **time-range** *time-range-name*] *

Default

No IPv6 advanced ACL rules exist.

Views

IPv6 advanced ACL view

Predefined user roles

network-admin

Parameters

rule-id: Specifies a rule ID in the range of 0 to 65534. If you do not specify a rule ID when creating an ACL rule, the system automatically assigns it a rule ID. This rule ID is the nearest higher multiple of the numbering step to the current highest rule ID, starting from the start rule ID. For example, if the rule numbering step is 5 and the current highest rule ID is 28, the rule is numbered 30.

deny: Denies matching packets.

permit: Allows matching packets to pass.

protocol: Specifies one of the following values:

- A protocol number in the range of 0 to 255.
- A protocol name: **gre** (47), **icmpv6** (58), **ipv6**, **ipv6-ah** (51), **ipv6-esp** (50), **ospf** (89), **tcp** (6), or **udp** (17). The **ipv6** keyword specifies all protocols.

Table 1-11 describes the parameters that you can specify regardless of the value for the *protocol* argument.

Table 1-11 Match criteria and other rule information for IPv6 advanced ACL rules

Parameters	Function	Description
source { *source-address source-prefix* | *source-address/source-prefix* | **any** }	Specifies a source IPv6 address.	The *source-address* argument specifies an IPv6 source address. The *source-prefix* argument specifies a prefix length in the range of 1 to 128. The **any** keyword represents any IPv6 source address.
destination { *dest-address dest-prefix* | *dest-address/dest-prefix* | **any** }	Specifies a destination IPv6 address.	The *dest-address* argument specifies a destination IPv6 address. The *dest-prefix* argument specifies a prefix length in the range of 1 to 128. The **any** keyword represents any IPv6 destination address.
counting	Enables rule match counting in software.	The **counting** keyword enables match counting specific to rules, and the **hardware-count** keyword in the **packet-filter ipv6** command enables match counting in hardware for all rules in an ACL. If the **counting** keyword is not specified, matches for the rule are not counted in software.
dscp *dscp*	Specifies a DSCP preference.	The *dscp* argument can be a number in the range of 0 to 63, or in words, **af11** (10), **af12** (12), **af13** (14), **af21** (18), **af22** (20), **af23** (22), **af31** (26), **af32** (28), **af33** (30), **af41** (34), **af42** (36), **af43** (38), **cs1** (8), **cs2** (16), **cs3** (24), **cs4** (32), **cs5** (40), **cs6** (48), **cs7** (56), **default** (0), or **ef** (46).
flow-label *flow-label-value*	Specifies a flow label value in an IPv6 packet header.	The *flow-label-value* argument is in the range of 0 to 1048575.
fragment	Applies the rule only to fragments.	If you do not specify this keyword, the rule applies to all fragments and non-fragments.
logging	Logs matching packets.	This feature requires that the module (for example, packet filtering) that uses the ACL supports

Parameters	Function	Description
		logging.
routing [**type** *routing-type*]	Specifies an IPv6 routing header type.	*routing-type*: Value of the IPv6 routing header type, in the range of 0 to 255. If you specify the **type** *routing-type* option, the rule applies to the specified type of IPv6 routing header. If you do not specify the **type** *routing-type* option, the rule applies to all types of IPv6 routing headers.
time-range *time-range-name*	Specifies a time range for the rule.	The *time-range-name* argument is a case-insensitive string of 1 to 32 characters. It must start with an English letter. If the time range is not configured, the system creates the rule. However, the rule using the time range can take effect only after you configure the time range. For more information about time range, see *ACL and QoS Configuration Guide*.

If the *protocol* argument is **tcp** (6) or **udp** (17), set the parameters shown in Table 1-12 .

Table 1-12 TCP/UDP-specific parameters for IPv6 advanced ACL rules

Parameters	Function	Description
source-port *operator port*	Specifies one or more UDP or TCP source ports.	The *operator* argument can be **eq** (equal to). The *port* argument is TCP or UDP port numbers in the range of 0 to 65535. TCP port numbers can be represented as: **chargen** (19), **bgp** (179), **cmd** (514), **daytime** (13), **discard** (9), **dns** (53), **domain** (53), **echo** (7), **exec** (512), **finger** (79), **ftp** (21), **ftp-data** (20), **gopher** (70), **hostname** (101), **irc** (194), **klogin** (543), **kshell** (544), **login** (513), **lpd** (515), **nntp** (119), **pop2** (109), **pop3** (110), **smtp** (25), **sunrpc** (111), **tacacs** (49), **talk** (517), **telnet** (23), **time** (37), **uucp** (540), **whois** (43), and **www** (80). UDP port numbers can be represented as: **biff** (512), **bootpc** (68), **bootps** (67), **discard** (9), **dns** (53), **dnsix** (90), **echo** (7), **mobilip-ag** (434), **mobilip-mn** (435), **nameserver** (42), **netbios-dgm** (138), **netbios-ns** (137), **netbios-ssn** (139), **ntp** (123), **rip** (520), **snmp** (161), **snmptrap** (162), **sunrpc** (111), **syslog** (514), **tacacs-ds** (65), **talk** (517), **tftp** (69), **time** (37), **who** (513), and **xdmcp** (177).
destination-port *operator port*	Specifies one or more UDP or TCP destination ports.	

Parameters	Function	Description
{ **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* }*	Specifies one or more TCP flags, including ACK, FIN, PSH, RST, SYN, and URG.	Parameters specific to TCP. The value for each argument can be 0 (flag bit not set) or 1 (flag bit set). The TCP flags in a rule are ANDed. For example, a rule configured with **ack** 0 **psh** 1 matches packets that have the ACK flag bit not set and the PSH flag bit set.
established	Specifies the flags for indicating the established status of a TCP connection.	Parameter specific to TCP. The rule matches TCP packets with the ACK or RST flag bit set.

If the *protocol* argument is **icmpv6** (58), set the parameters shown in Table 1-13 .

Table 1-13 ICMPv6-specific parameters for IPv6 advanced ACL rules

Parameters	Function	Description
icmp6-type { *icmp6-type icmp6-code* | *icmp6-message* }	Specifies the ICMPv6 message type and code.	The *icmp6-type* argument is in the range of 0 to 255. The *icmp6-code* argument is in the range of 0 to 255. The *icmp6-message* argument specifies a message name. Supported ICMP message names and their corresponding type and code values are listed in Table 1-14 .

Table 1-14 ICMPv6 message names supported in IPv6 advanced ACL rules

ICMPv6 message name	ICMPv6 message type	ICMPv6 message code
echo-reply	129	0
echo-request	128	0
err-Header-field	4	0
frag-time-exceeded	3	1
hop-limit-exceeded	3	0
host-admin-prohib	1	1
host-unreachable	1	3
neighbor-advertisement	136	0
neighbor-solicitation	135	0
network-unreachable	1	0
packet-too-big	2	0
port-unreachable	1	4
redirect	137	0
router-advertisement	134	0

ICMPv6 message name	ICMPv6 message type	ICMPv6 message code
router-solicitation	133	0
unknown-ipv6-opt	4	2
unknown-next-hdr	4	1

Usage guidelines

If an IPv6 advanced ACL is for QoS traffic classification or packet filtering:

- Do not specify the **fragment** keyword.
- Do not specify the **routing**, or **flow-label** keyword if the ACL is for outbound application.
- Do not specify **ipv6-ah** for the *protocol* argument, or set its value to 0, 43, 44, 51, or 60 if the ACL is for outbound application.

Within an ACL, the permit or deny statement of each rule must be unique. If the rule you are creating or editing has the same deny or permit statement as another rule in the ACL, the rule will not be created or changed.

You can edit ACL rules only when the match order is **config**.

To view the existing IPv6 basic and advanced ACL rules, use the **display acl ipv6 all** command.

The **undo rule** *rule-id* command without any optional parameters deletes an entire rule. If you specify optional parameters, the **undo rule** *rule-id* command deletes the specified attributes for a rule.

The **undo rule** { **deny** | **permit** } command can only be used to delete an entire rule. You must specify all the attributes of the rule for the command.

Examples

Create an IPv6 advanced ACL rule to permit TCP packets with the destination port 80 from 2030:5060::/64 to FE80:5060::/96.

```
<Switch> system-view
[Switch] acl ipv6 advanced 3000
[Switch-acl-ipv6-adv-3000] rule permit tcp source 2030:5060::/64 destination
fe80:5060::/96 destination-port eq 80
```

Create IPv6 advanced ACL rules to permit all IPv6 packets but the ICMPv6 packets destined for FE80:5060:1001::/48.

```
<Switch> system-view
[Switch] acl ipv6 advanced 3001
[Switch-acl-ipv6-adv-3001] rule deny icmpv6 destination fe80:5060:1001:: 48
[Switch-acl-ipv6-adv-3001] rule permit ipv6
```

Create IPv6 advanced ACL rules to permit inbound and outbound FTP packets.

```
<Switch> system-view
[Switch] acl ipv6 advanced 3002
[Switch-acl-ipv6-adv-3002] rule permit tcp source-port eq ftp
[Switch-acl-ipv6-adv-3002] rule permit tcp source-port eq ftp-data
[Switch-acl-ipv6-adv-3002] rule permit tcp destination-port eq ftp
[Switch-acl-ipv6-adv-3002] rule permit tcp destination-port eq ftp-data
```

Create IPv6 advanced ACL rules to permit inbound and outbound SNMP and SNMP trap packets.

```
<Switch> system-view
[Switch] acl ipv6 advanced 3003
[Switch-acl-ipv6-adv-3003] rule permit udp source-port eq snmp
[Switch-acl-ipv6-adv-3003] rule permit udp source-port eq snmptrap
[Switch-acl-ipv6-adv-3003] rule permit udp destination-port eq snmp
[Switch-acl-ipv6-adv-3003] rule permit udp destination-port eq snmptrap
```

Related commands

acl

acl logging interval

display acl

step

time-range

1.1.18. rule (IPv6 basic ACL view)

Use **rule** to create or edit an IPv6 basic ACL rule.

Use **undo rule** to delete an entire IPv6 basic ACL rule or some attributes in the rule.

Syntax

rule [*rule-id*] { **deny** | **permit** } [**counting** | **fragment** | **logging** | **routing** [**type** *routing-type*] | **source** { *source-address source-prefix* | *source-address*/*source-prefix* | **any** } | **time-range** *time-range-name*] *

undo rule *rule-id* [**counting** | **fragment** | **logging** | **routing** | **source** | **time-range**] *

undo rule { **deny** | **permit** } [**counting** | **fragment** | **logging** | **routing** [**type** *routing-type*] | **source** { *source-address source-prefix* | *source-address*/*source-prefix* | **any** } | **time-range** *time-range-name*] *

Default

No IPv6 basic ACL rules exist.

Views

IPv6 basic ACL view

Predefined user roles

network-admin

Parameters

rule-id: Specifies a rule ID in the range of 0 to 65534. If you do not specify a rule ID when creating an ACL rule, the system automatically assigns it a rule ID. This rule ID is the nearest higher multiple of the numbering step to the current highest rule ID, starting from the start rule ID. For example, if the rule numbering step is 5 and the current highest rule ID is 28, the rule is numbered 30.

deny: Denies matching packets.

permit: Allows matching packets to pass.

counting: Enables rule match counting in software. If you do not specify this keyword, matches for the rule are not counted in software.

fragment: Applies the rule only to non-first fragments. If you do not specify this keyword, the rule applies to both fragments and non-fragments.

logging: Logs matching packets. This feature is available only when the application module (for example, packet filtering) that uses the ACL supports the logging feature.

routing [**type** *routing-type*]: Applies the rule to the specified type of IPv6 routing header or all types of IPv6 routing headers. The *routing-type* argument specifies the value of the IPv6 routing header type, in the range of 0 to 255. If you do not specify the **type** *routing-type* option, the rule applies to all types of IPv6 routing headers.

source { *source-address source-prefix* | *source-address*/*source-prefix* | **any** }: Matches a source IPv6 address. The *source-address* argument specifies a source IPv6 address. The *source-prefix* argument specifies an address prefix length in the range of 1 to 128. The **any** keyword represents any IPv6 source address.

time-range *time-range-name*: Specifies a time range for the rule. The *time-range-name* argument is a case-insensitive string of 1 to 32 characters. It must start with an English letter. If the time range is not configured, the system creates the rule. However, the rule using the time range can take effect only after you configure the time range. For more information about time range, see *ACL and QoS Configuration Guide*.

Usage guidelines

The **fragment** keyword is not supported for a QoS policy or a packet filter.

The **routing** keyword is not supported for an outbound QoS policy or packet filter.

Within an ACL, the permit or deny statement of each rule must be unique. If the rule you are creating or editing has the same deny or permit statement as another rule in the ACL, the rule will not be created or changed.

You can edit ACL rules only when the match order is **config**.

The **counting** keyword in this command enables match counting specific to rules, and the **hardware-count** keyword in the **packet-filter ipv6** command enables match counting in hardware for all rules in an ACL.

To view the existing IPv6 basic and advanced ACL rules, use the **display acl ipv6 all** command.

The **undo rule** *rule-id* command without any optional parameters deletes an entire rule. If you specify optional parameters, the **undo rule** *rule-id* command deletes the specified attributes for a rule.

The **undo rule** { **deny** | **permit** } command can only be used to delete an entire rule. You must specify all the attributes of the rule for the command.

Examples

Create an IPv6 basic ACL rule to deny the packets from any source IP subnet but 1001::/16, 3124:1123::/32, or FE80:5060:1001::/48.

```
<Switch> system-view
[Switch] acl ipv6 basic 2000
[Switch-acl-ipv6-basic-2000] rule permit source 1001:: 16
[Switch-acl-ipv6-basic-2000] rule permit source 3124:1123:: 32
[Switch-acl-ipv6-basic-2000] rule permit source fe80:5060:1001:: 48
[Switch-acl-ipv6-basic-2000] rule deny source any
```

Related commands

acl

acl logging interval

display acl

step

time-range

1.1.19. rule (Layer 2 ACL view)

Use **rule** to create or edit a Layer 2 ACL rule.

Use **undo rule** to delete an entire Layer 2 ACL rule or some attributes in the rule.

Syntax

rule [*rule-id*] { **deny** | **permit** } [**cos** *dot1p* | **counting** | **dest-mac** *dest-address dest-mask* | { **lsap** *lsap-type lsap-type-mask* | **type** *protocol-type protocol-type-mask* } | **source-mac** *source-address source-mask* | **time-range** *time-range-name*] *

undo rule *rule-id* [**counting** | **time-range**] *

undo rule { **deny** | **permit** } [**cos** *dot1p* | **counting** | **dest-mac** *dest-address dest-mask* | { **lsap** *lsap-type lsap-type-mask* | **type** *protocol-type protocol-type-mask* } | **source-mac** *source-address source-mask* | **time-range** *time-range-name*] *

Default

No Layer 2 ACL rules exist.

Views

Layer 2 ACL view

Predefined user roles

network-admin

Parameters

rule-id: Specifies a rule ID in the range of 0 to 65534. If you do not specify a rule ID when creating an ACL rule, the system automatically assigns it a rule ID. This rule ID is the nearest higher multiple of the numbering step to the current highest rule ID, starting from the start rule ID. For example, if the rule numbering step is 5 and the current highest rule ID is 28, the rule is numbered 30.

deny: Denies matching packets.

permit: Allows matching packets to pass.

cos *dot1p*: Matches an 802.1p priority. The 802.1p priority can be specified by one of the following values:

- A priority number in the range of 0 to 7.
- A priority name: **best-effort** (0), **background** (1), **spare** (2), **excellent-effort** (3), **controlled-load** (4), **video** (5), **voice** (6), or **network-management** (7).

counting: Enables rule match counting in software. If you do not specify this keyword, matches for the rule are not counted in software.

dest-mac *dest-address dest-mask*: Matches a destination MAC address range. The *dest-address* and *dest-mask* arguments represent a destination MAC address and mask in the H-H-H format.

lsap *lsap-type lsap-type-mask:* Matches the DSAP and SSAP fields in LLC encapsulation. The *lsap-type* argument is a hexadecimal number that represents the encapsulation format. The value range for the *lsap-type* argument is 0 to ffff. The *lsap-type-mask* argument is a hexadecimal number that represents the LSAP mask. The value range for the *lsap-type-mask* argument is 0 to ffff.

type *protocol-type protocol-type-mask*: Matches one or more protocols in the Layer 2. The *protocol-type* argument is a hexadecimal number that represents a protocol type in Ethernet_II and Ethernet_SNAP frames. The value range for the *protocol-type* argument is 0 to ffff. The *protocol-type-mask* argument is a hexadecimal number that represents a protocol type mask. The value range for the *protocol-type-mask* argument is 0 to ffff.

source-mac *source-address source-mask:* Matches a source MAC address range. The *source-address* argument represents a source MAC address, and the *sour-mask* argument represents a mask in the H-H-H format.

time-range *time-range-name*: Specifies a time range for the rule. The *time-range-name* argument is a case-insensitive string of 1 to 32 characters. It must start with an English letter. If the time range is not configured, the system creates the rule. However, the rule using the time range can take effect only after you configure the time range. For more information about time range, see *ACL and QoS Configuration Guide*.

Usage guidelines

Within an ACL, the permit or deny statement of each rule must be unique. If the rule you are creating or editing has the same deny or permit statement as another rule in the ACL, the rule will not be created or changed.

You can edit ACL rules only when the match order is **config**.

The **counting** keyword in this command enables match counting specific to rules, and the **hardware-count** keyword in the **packet-filter** command enables match counting in hardware for all rules in an ACL.

To view the existing Layer 2 ACL rules, use the **display acl mac all** command.

The **undo rule** *rule-id* command without any optional parameters deletes an entire rule. If you specify optional parameters, the **undo rule** *rule-id* command deletes the specified attributes for the rule.

The **undo rule** { **deny** | **permit** } command can only be used to delete an entire rule. You must specify all the attributes of the rule for the command.

Examples

Create a rule in Layer 2 ACL 4000 to permit ARP packets and deny RARP packets.

```
<Switch> system-view
[Switch] acl mac 4000
[Switch-acl-mac-4000] rule permit type 0806 ffff
[Switch-acl-mac-4000] rule deny type 8035 ffff
```

Related commands

acl

display acl

step

time-range

1.1.20. rule comment

Use **rule comment** to configure a comment for an ACL rule.

Use **undo rule comment** to delete an ACL rule comment.

Syntax

rule *rule-id* **comment** *text*

undo rule *rule-id* **comment**

Default

A rule does not have a comment.

Views

IPv4 basic/advanced ACL view

IPv6 basic/advanced ACL view

Layer 2 ACL view

Predefined user roles

network-admin

Parameters

rule-id: Specifies an ACL rule ID in the range of 0 to 65534. The ACL rule must already exist.

text: Specifies a comment about the ACL rule, a case-sensitive string of 1 to 127 characters.

Usage guidelines

This command adds a comment to a rule if the rule does not have a comment. It modifies the comment for a rule if the rule already has a comment.

Examples

Create a rule for IPv4 basic ACL 2000, and add a comment about the rule.

```
<Switch> system-view
[Switch] acl basic 2000
[Switch-acl-ipv4-basic-2000] rule 0 deny source 1.1.1.1 0
[Switch-acl-ipv4-basic-2000] rule 0 comment This rule is used on gigabitethernet 1/0/1.
```

Related commands

display acl

1.1.21. step

Use **step** to set a rule numbering step for an ACL.

Use **undo step** to restore the default.

Syntax

step *step-value*

undo step

Default

The rule numbering step is 5, and the start rule ID is 0.

Views

IPv4 basic/advanced ACL view

IPv6 basic/advanced ACL view

Layer 2 ACL view

Predefined user roles

network-admin

Parameters

step-value: Specifies the ACL rule numbering step in the range of 1 to 20.

Usage guidelines

The rule numbering step sets the increment by which the system numbers rules automatically. If you do not specify a rule ID when creating an ACL rule, the system automatically assigns it a rule ID. This rule ID is the nearest higher multiple of the numbering step to the current highest rule ID, starting from the start rule ID. For example, if the rule numbering step is 5 and the current highest rule ID is 12, the rule is numbered 15.

The wider the numbering step, the more rules you can insert between two rules. Whenever the step or start rule ID changes, the rules are renumbered, starting from the start rule ID. For example, if there are five rules numbered 0, 5, 9, 10, and 15, changing the step from 5 to 2 causes the rules to be renumbered 0, 2, 4, 6, and 8.

Examples

Set the rule numbering step to 2 for IPv4 basic ACL 2000.

```
<Switch> system-view
[Switch] acl basic 2000
[Switch-acl-ipv4-basic-2000] step 2
```

Related commands

display acl

Contents

A page of this section is **8-x-x**

2. QoS policy commands ····· 2-1
2.1. Traffic class commands ····· 2-1
2.1.1. display traffic classifier ····· 2-1
2.1.2. if-match ····· 2-2
2.1.3. traffic classifier ····· 2-5
2.2. Traffic behavior commands ····· 2-6
2.2.1. accounting ····· 2-6
2.2.2. car ····· 2-7
2.2.3. display traffic behavior ····· 2-9
2.2.4. filter ····· 2-10
2.2.5. nest top-most ····· 2-10
2.2.6. redirect ····· 2-11
2.2.7. remark dot1p ····· 2-12
2.2.8. remark drop-precedence ····· 2-13
2.2.9. remark dscp ····· 2-14
2.2.10. remark local-precedence ····· 2-15
2.2.11. remark service-vlan-id ····· 2-16
2.2.12. traffic behavior ····· 2-16
2.3. QoS policy commands ····· 2-17
2.3.1. classifier behavior ····· 2-17
2.3.2. display qos policy ····· 2-18
2.3.3. display qos policy global ····· 2-19
2.3.4. display qos policy interface ····· 2-20
2.3.5. display qos vlan-policy ····· 2-23
2.3.6. qos apply policy (interface view) ····· 2-25
2.3.7. qos apply policy global ····· 2-26
2.3.8. qos policy ····· 2-26
2.3.9. qos vlan-policy ····· 2-27
2.3.10. reset qos policy global ····· 2-28
2.3.11. reset qos vlan-policy ····· 2-28

2. QoS policy commands

2.1. Traffic class commands

2.1.1. display traffic classifier

Use **display traffic classifier** to display traffic classes.

Syntax

display traffic classifier user-defined [*classifier-name*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

user-defined: Specifies user-defined traffic classes.

classifier-name: Specifies a traffic class by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a traffic class, this command displays all traffic classes.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays the traffic classes for the master device.

Examples

Display all user-defined traffic classes.

```
<Switch> display traffic classifier user-defined

  User-defined classifier information:

   Classifier: 1 (ID 100)
     Operator: AND
     Rule(s) :
      If-match acl 2000

   Classifier: 2 (ID 101)
     Operator: AND
     Rule(s) :
      If-match protocol ipv6

   Classifier: 3 (ID 102)
     Operator: AND
     Rule(s) :
      -none-
```

Table 2-1 Command output

Field	Description
Classifier	Traffic class name and its match criteria.
Operator	Match operator you set for the traffic class. If the operator is AND, the traffic class matches the packets that match all its match criteria. If the operator is OR, the traffic class matches the packets that match any of its match criteria.
Rule(s)	Match criteria.

2.1.2. if-match

Use **if-match** to define a match criterion.

Use **undo if-match** to delete a match criterion.

Syntax

if-match *match-criteria*

undo if-match *match-criteria*

Default

No match criterion is configured.

Views

Traffic class view

Predefined user roles

network-admin

Parameters

match-criteria: Specifies a match criterion. Table 2-2 shows the available match criteria.

Table 2-2 Available match criteria

Option	Description
acl [**ipv6** | **mac**] { *acl-number* | **name** *acl-name* }	Matches an ACL. The value range for the *acl-number* argument is as follows: • 2000 to 3999 for IPv4 ACLs. • 2000 to 3999 for IPv6 ACLs. • 4000 to 4999 for Layer 2 MAC ACLs. The *acl-name* argument is a case-insensitive string of 1 to 63 characters, which must start with an English letter. To avoid confusion, make sure the argument is not **all**.
any	Matches all packets.
customer-dot1p *dot1p-value*&<1-8>	Matches 802.1p priority values in inner VLAN tags of double-tagged packets. The *dot1p-value*&<1-8> argument specifies a space-separated list of up to eight 802.1p priority values. The value range for the *dot1p-value* argument is 0 to 7.

Option	Description
customer-vlan-id *vlan-id-list*	Matches VLAN IDs in inner VLAN tags of double-tagged packets. The *vlan-id-list* argument specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* **to** *vlan-id2*. The value for *vlan-id2* must be greater than or equal to the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094.
destination-mac *mac-address*	Matches a destination MAC address. This option takes effect only on Ethernet interfaces.
dscp *dscp-value&<1-8>*	Matches DSCP values. The *dscp-value&<1-8>* argument specifies a space-separated list of up to eight DSCP values. The value range for the *dscp-value* argument is 0 to 63 or keywords shown in Table 2-4 .
protocol *protocol-name*	Matches a protocol. The *protocol-name* argument can be **ip** or **ipv6**.
service-dot1p *dot1p-value&<1-8>*	Matches 802.1p priority values in outer VLAN tags. The *dot1p-value&<1-8>* argument specifies a space-separated list of up to eight 802.1p priority values. The value range for the *dot1p-value* argument is 0 to 7.
service-vlan-id *vlan-id-list*	Matches VLAN IDs in outer VLAN tags. The *vlan-id-list* argument specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* **to** *vlan-id2*. The value for *vlan-id2* must be greater than or equal to the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094. You can use this option to match single-tagged packets.
source-mac *mac-address*	Matches a source MAC address. This option takes effect only on Ethernet interfaces.
tunnel-id *tunnel-id*	Matches a VXLAN tunnel ID. For the traffic class to take effect, the tunnel must be a VXLAN tunnel.
vxlan { **any** | *vxlan-id* }	Matches a VXLAN ID.

Usage guidelines

In a traffic class with the logical OR operator, you can configure multiple **if match** commands for any of the available match criteria.

When you configure a match criterion that can have multiple values in one **if-match** command, follow these restrictions and guidelines:

- You can specify up to eight values for any of the following match criteria in one **if-match** command:
  - 802.1p priority.
  - DSCP.
  - VLAN ID.
- If a packet matches one of the specified values, it matches the **if-match** command.
- To delete a criterion that has multiple values, the specified values in the **undo if-match** command must be the same as those specified in the **if-match** command. The order of the values can be different.

When you configure ACL-based match criteria, follow these restrictions and guidelines:

- The ACL must already exist.
- The ACL is used for classification only and the permit/deny actions in ACL rules are ignored. Actions taken on matching packets are defined in traffic behaviors.

You can use both AND and OR operators to define the match relationships between the criteria for a class. For example, you can define relationships among three match criteria in traffic class **classA** as follows:

```
traffic classifier classB operator and
if-match criterion 1
if-match criterion 2
traffic classifier classA operator or
if-match criterion 3
```

Examples

Define a match criterion for traffic class **class1** to match the packets with a destination MAC address of 0050-ba27-bed3.

```
<Switch> system-view
[Switch] traffic classifier class1
[Switch-classifier-class1] if-match destination-mac 0050-ba27-bed3
```

Define a match criterion for traffic class **class2** to match the packets with a source MAC address of 0050-ba27-bed2.

```
<Switch> system-view
[Switch] traffic classifier class2
[Switch-classifier-class2] if-match source-mac 0050-ba27-bed2
```

Define a match criterion for traffic class **class1** to match the packets with 802.1p priority 5 in the outer VLAN tag.

```
<Switch> system-view
[Switch] traffic classifier class1
[Switch-classifier-class1] if-match service-dot1p 5
```

Define a match criterion for traffic class **class1** to match advanced ACL 3101.

```
<Switch> system-view
[Switch] traffic classifier class1
[Switch-classifier-class1] if-match acl 3101
```

Define a match criterion for traffic class **class1** to match the ACL named **flow**.

```
<Switch> system-view
[Switch] traffic classifier class1
[Switch-classifier-class1] if-match acl name flow
```

Define a match criterion for traffic class **class1** to match advanced IPv6 ACL 3101.

```
<Switch> system-view
[Switch] traffic classifier class1
[Switch-classifier-class1] if-match acl ipv6 3101
```

Define a match criterion for traffic class **class1** to match the IPv6 ACL named **flow**.

```
<Switch> system-view
[Switch] traffic classifier class1
[Switch-classifier-class1] if-match acl ipv6 name flow
```

Define a match criterion for traffic class **class1** to match all packets.

```
<Switch> system-view
[Switch] traffic classifier class1
[Switch-classifier-class1] if-match any
```

Define a match criterion for traffic class **class1** to match the packets with a DSCP value of 1, 6, or 9.

```
<Switch> system-view
[Switch] traffic classifier class1 operator or
[Switch-classifier-class1] if-match dscp 1 6 9
```

Define a match criterion for traffic class **class1** to match IP packets.

```
<Switch> system-view
[Switch] traffic classifier class1
[Switch-classifier-class1] if-match protocol ip
```

Define a match criterion for traffic class **class1** to match the packets with VLAN ID 2, 7, or 10 in the outer VLAN tag.

```
<Switch> system-view
[Switch] traffic classifier class1 operator or
[Switch-classifier-class1] if-match service-vlan-id 2 7 10
```

Define a match criterion for traffic class **class1** to match the VXLAN packets with tunnel ID 2.

```
<Switch> system-view
[Switch] traffic classifier class1
[Switch-classifier-class1] if-match tunnel-id 2
```

Define a match criterion for traffic class **class1** to match the packets with VXLAN 10.

```
<Switch> system-view
[Switch] traffic classifier class1
[Switch-classifier-class1] if-match vxlan 10
```

2.1.3. traffic classifier

Use **traffic classifier** to create a traffic class and enter its view, or enter the view of an existing traffic class.

Use **undo traffic classifier** to delete a traffic class.

Syntax

traffic classifier *classifier-name* [**operator** { **and** | **or** }]

undo traffic classifier *classifier-name*

Default

No traffic classes exist.

Views

System view

Predefined user roles

network-admin

Parameters

classifier-name: Specifies a name for the traffic class, a case-sensitive string of 1 to 31 characters.

operator: Sets the operator to logic AND (the default) or OR for the traffic class.

and: Specifies the logic AND operator. The traffic class matches the packets that match all its criteria.

or: Specifies the logic OR operator. The traffic class matches the packets that match any of its criteria.

Examples

Create a traffic class named **class1**.

```
<Switch> system-view
[Switch] traffic classifier class1
[Switch-classifier-class1]
```

Related commands

display traffic classifier

2.2. Traffic behavior commands

2.2.1. accounting

Use **accounting** to configure a traffic accounting action in a traffic behavior.

Use **undo accounting** to restore the default.

Syntax

accounting { **byte** | **packet** }

undo accounting

Default

No traffic accounting action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

byte: Counts traffic in bytes.

packet: Counts traffic in packets.

Examples

Configure a traffic accounting action in traffic behavior **database** to count traffic in bytes.

```
<Switch> system-view
[Switch] traffic behavior database
[Switch-behavior-database] accounting byte
```

2.2.2. car

Use **car** to configure a CAR action in absolute value in a traffic behavior.

Use **undo car** to restore the default.

Syntax

car cir *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size*]] [**green** *action* | **red** *action* | **yellow** *action*] *

car cir *committed-information-rate* [**cbs** *committed-burst-size*] **pir** *peak-information-rate* [**ebs** *excess-burst-size*] [**green** *action* | **red** *action* | **yellow** *action*] *

undo car

Default

No CAR action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

cir *committed-information-rate*: Specifies the committed information rate (CIR) in the range of 1 to 160000000 kbps.

cbs *committed-burst-size*: Specifies the committed burst size (CBS) in bytes. The value range for *committed-burst-size* is 512 to 256000000, in increments of 512. The default value for this argument is the product of 62.5 and the CIR and must be an integral multiple of 512. When the product is not an integral multiple of 512, it is rounded up to the nearest integral multiple of 512 that is greater than the product. A default value greater than 256000000 is converted to 256000000.

ebs *excess-burst-size*: Specifies the excess burst size (EBS) in bytes. The value range for *excess-burst-size* is 0 to 256000000, in increments of 512. If the PIR is configured, the default EBS is the product of 62.5 and the PIR and must be an integral multiple of 512. When the product is not an integral multiple of 512, it is rounded up to the nearest integral multiple of 512. A default value greater than 256000000 is converted to 256000000.

pir *peak-information-rate*: Specifies the peak information rate (PIR) in the range of 1 to 160000000 kbps.

green *action*: Specifies the action to take on packets that conform to the CIR. The default setting is **pass**.

red *action*: Specifies the action to take on packets that conform to neither CIR nor PIR. The default setting is **discard**.

yellow *action*: Specifies the action to take on packets that conform to the PIR but not to the CIR. The default setting is **pass**.

action: Sets the action to take on the packet:

- **discard**: Drops the packet.

- **pass**: Permits the packet to pass through.
- **remark-dot1p-pass** *new-cos*: Sets the 802.1p priority value of the 802.1p packet to *new-cos* and permits the packet to pass through. The *new-cos* argument is in the range of 0 to 7.
- **remark-dscp-pass** *new-dscp*: Sets the DSCP value of the packet to *new-dscp* and permits the packet to pass through. The *new-dscp* argument is in the range of 0 to 63.
- **remark-lp-pass** *new-local-precedence*: Sets the local precedence value of the packet to *new-local-precedence* and permits the packet to pass through. The *new-local-precedence* argument is in the range of 0 to 7.

Usage guidelines

To use two rates for traffic policing, configure the **car** command with the **pir** *peak-information-rate* option. To use one rate for traffic policing, configure the **car** command without the **pir** *peak-information-rate* option.

If you execute the **car** command multiple times in the same traffic behavior, the most recent configuration takes effect.

IMPORTANT

For TCP communications (e.g., FTP, CIFS, SMTP, HTTP, etc.), a low CBS value can cause retransmission processing more likely and may slow down.

Setting the CBS value to a sufficiently larger value reduces the retransmission process and prevents slowing down.

The CIR value must be adjusted based on the CBS value and is recommended to be set in units of 1000 Kbps (1 Mbps) or higher.

Type	CIR		CBS		
	Granularity (Kbps)	Maximum (Kbps)	Granularity (B)	Minimum (B)	Maximum (B)
3	1,000	102,300,000	512	4,194,304	33,553,920
4	10,000	1,023,000,000	4,096	33,554,432	256,000,000

・If you want to set the CIR to a range of up to 102,300,000Kbps, set the CIR in 1000Kbps (1Mbps).CBS should range from 4,194,304 to 33,553,920B and be set at an integer multiple of 512.
・If you set the CIR to more than 102,300,000Kbps (up to 1,023,000,000Kbps), CBS should be set in the range of 33,554,432 to 256,000,000B and an integer multiple of 4,096.

Examples

Configure a CAR action in traffic behavior **database**:

- Set the CIR to 200 kbps, CBS to 51200 bytes, and EBS to 0.
- Transmit the conforming packets, and mark the excess packets with DSCP value 0 and transmit them.

```
<Switch> system-view
[Switch] traffic behavior database
[Switch-behavior-database] car cir 200 cbs 51200 ebs 0 green pass red remark-dscp-pass
0
```

2.2.3. display traffic behavior

Use **display traffic behavior** to display traffic behaviors.

Syntax

display traffic behavior user-defined [*behavior-name*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

user-defined: Specifies user-defined traffic behaviors.

behavior-name: Specifies a behavior by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a traffic behavior, this command displays all traffic behaviors.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays the traffic behaviors for the master device.

Examples

Display all user-defined traffic behaviors.

```
<Switch> display traffic behavior user-defined

  User-defined behavior information:

    Behavior: 1 (ID 100)
      Marking:
        Remark dscp 3
      Committed Access Rate:
        CIR 112 (kbps), CBS 5120 (Bytes), EBS 512 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : discard

    Behavior: 2 (ID 101)
      Accounting enable: Packet
      Filter enable: Permit
      Redirecting:
        Redirect to the CPU

    Behavior: 3 (ID 102)
      -none-
```

Table 2-3 Command output

Field	Description
Behavior	Name and contents of a traffic behavior.

Field	Description
Marking	Information about priority marking.
Remark dscp	Action of setting the DSCP value for packets.
Committed Access Rate	Information about the CAR action.
Green action	Action to take on green packets.
Yellow action	Action to take on yellow packets.
Red action	Action to take on red packets.
Accounting enable	Class-based accounting action.
Filter enable	Traffic filtering action.
Redirecting	Information about traffic redirecting.
Mirroring	Information about traffic mirroring.
none	No other traffic behavior is configured.

2.2.4. filter

Use **filter** to configure a traffic filtering action in a traffic behavior.

Use **undo filter** to restore the default.

Syntax

filter { **deny** | **permit** }

undo filter

Default

No traffic filtering action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

deny: Drops packets.

permit: Transmits packets.

Examples

Configure a traffic filtering action as **deny** in traffic behavior **database**.

```
<Switch> system-view
[Switch] traffic behavior database
[Switch-behavior-database] filter deny
```

2.2.5. nest top-most

Use **nest top-most** to configure an outer VLAN tag adding action in a traffic behavior.

Use **undo nest top-most** to restore the default.

Syntax

nest top-most vlan *vlan-id*

undo nest top-most

Default

No outer VLAN tag adding action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

vlan-id *vlan-id*: Specifies the VLAN ID to be added in the outer VLAN tag, in the range of 1 to 4094.

Usage guidelines

If a QoS policy contains an outer VLAN tag adding action, apply it only to the incoming traffic of an interface.

If you execute the **nest top-most** command multiple times in the same traffic behavior, the most recent configuration takes effect.

Examples

Configure traffic behavior **b1** to add an outer VLAN tag with VLAN ID 123.

```
<Switch> system-view
[Switch] traffic behavior b1
[Switch-behavior-b1] nest top-most vlan 123
```

2.2.6. redirect

Use **redirect** to configure a traffic redirecting action in a traffic behavior.

Use **undo redirect** to restore the default.

Syntax

redirect { **cpu** | **interface** *interface-type interface-number* }

undo redirect { **cpu** | **interface** *interface-type interface-number* }

Default

No traffic redirecting action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

cpu: Redirects traffic to the CPU.

interface *interface-type interface-number*: Redirects traffic to an interface specified by its type and number.

Usage guidelines

If you execute the **redirect** command multiple times in the same traffic behavior, the most recent configuration takes effect.

A traffic redirecting action takes effect only when the QoS policy is applied to the inbound direction.

For traffic redirecting to an access port, make sure the PVID of the interfaces to which the QoS policy is applied is the same as the PVID of the access port. Otherwise, the access port drops redirected packets.

For traffic redirecting to a trunk port, make sure the PVID of the interfaces to which the QoS policy is applied is in the allowed VLAN list of the trunk port. Otherwise, the trunk port drops redirected packets.

If a QoS policy applied to a user profile contains the **redirect interface** action, make sure the interface and the incoming interface of packets are in the same VLAN.

Examples

Configure redirecting traffic to GigabitEthernet 1/0/1 in traffic behavior **database**.

```
<Switch> system-view
[Switch] traffic behavior database
[Switch-behavior-database] redirect interface gigabitethernet 1/0/1
```

Related commands

classifier behavior

qos policy

traffic behavior

2.2.7. remark dot1p

Use **remark dot1p** to configure an 802.1p priority marking action or an inner-to-outer tag priority copying action in a traffic behavior.

Use **undo remark dot1p** to restore the default.

Syntax

remark [**green** | **red** | **yellow**] **dot1p** *dot1p-value*

undo remark [**green** | **red** | **yellow**] **dot1p**

remark dot1p customer-dot1p-trust

undo remark dot1p

Default

No 802.1p priority marking action or inner-to-outer tag priority copying action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

green: Specifies green packets.

red: Specifies red packets.

yellow: Specifies yellow packets.

dot1p-value: Specifies the 802.1p priority to be marked for packets, in the range of 0 to 7.

customer-dot1p-trust: Copies the 802.1p priority value in the inner VLAN tag to the outer VLAN tag.

Usage guidelines

The **remark dot1p** and **remark dot1p customer-dot1p-trust** commands override each other in the same traffic behavior. The **remark dot1p customer-dot1p-trust** command does not take effect on single-tagged packets.

If you execute the **remark dot1p** command multiple times for the same color, the most recent configuration takes effect.

An 802.1p priority marking action takes effect only when the QoS policy is applied to the inbound direction.

Examples

Configure traffic behavior **database** to mark matching traffic with 802.1p 2.

```
<Switch> system-view
[Switch] traffic behavior database
[Switch-behavior-database] remark dot1p 2
```

Configure an inner-to-outer tag priority copying action in traffic behavior **database**.

```
<Switch> system-view
[Switch] traffic behavior database
[Switch-behavior-database] remark dot1p customer-dot1p-trust
```

2.2.8. remark drop-precedence

Use **remark drop-precedence** to configure a drop priority marking action in a traffic behavior.

Use **undo remark drop-precedence** to restore the default.

Syntax

remark drop-precedence *drop-precedence-value*

undo remark drop-precedence

Default

No drop priority marking action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

drop-precedence-value: Specifies the drop priority to be marked for packets, in the range of 0 to 2.

Usage guidelines

A drop priority marking action takes effect only when the QoS policy is applied to the inbound direction.

If you execute the **remark drop-precedence** command multiple times in the same traffic behavior, the most recent configuration takes effect.

Examples

Configure traffic behavior **database** to mark matching traffic with drop priority 2.

```
<Switch> system-view
[Switch] traffic behavior database
[Switch-behavior-database] remark drop-precedence 2
```

2.2.9. remark dscp

Use **remark dscp** to configure a DSCP marking action in a traffic behavior.

Use **undo remark dscp** to restore the default.

Syntax

remark [**green** | **red** | **yellow**] **dscp** *dscp-value*

undo remark [**green** | **red** | **yellow**] **dscp**

Default

No DSCP marking action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

green: Specifies green packets.

red: Specifies red packets.

yellow: Specifies yellow packets.

dscp-value: Specifies a DSCP value, which can be a number from 0 to 63 or a keyword in Table 2-4 .

Table 2-4 DSCP keywords and values

Keyword	DSCP value (binary)	DSCP value (decimal)
af11	001010	10
af12	001100	12
af13	001110	14
af21	010010	18
af22	010100	20
af23	010110	22
af31	011010	26
af32	011100	28
af33	011110	30
af41	100010	34

Keyword	DSCP value (binary)	DSCP value (decimal)
af42	100100	36
af43	100110	38
cs1	001000	8
cs2	010000	16
cs3	011000	24
cs4	100000	32
cs5	101000	40
cs6	110000	48
cs7	111000	56
default	000000	0
ef	101110	46

Examples

Configure traffic behavior **database** to mark matching traffic with DSCP 6.

```
<Switch> system-view
[Switch] traffic behavior database
[Switch-behavior-database] remark dscp 6
```

2.2.10. remark local-precedence

Use **remark local-precedence** to configure a local precedence marking action in a traffic behavior.

Use **undo remark local-precedence** to restore the default.

Syntax

remark local-precedence *local-precedence-value*

undo remark local-precedence

Default

No local precedence marking action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

local-precedence-value: Specifies the local precedence to be marked for packets, in the range of 0 to 7.

Examples

Configure traffic behavior **database** to mark matching traffic with local precedence 2.

```
<Switch> system-view
[Switch] traffic behavior database
```

```
[Switch-behavior-database] remark local-precedence 2
```

2.2.11. remark service-vlan-id

Use **remark service-vlan-id** to configure an SVLAN marking action in a traffic behavior.

Use **undo remark service-vlan-id** to restore the default.

Syntax

remark service-vlan-id *vlan-id*

undo remark service-vlan-id

Default

No SVLAN marking action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

vlan-id: Specifies an SVLAN ID in the range of 1 to 4094.

Examples

Configure traffic behavior **b1** to mark matching packets with SVLAN 222.

```
<Switch> system-view
[Switch] traffic behavior b1
[Switch-behavior-b1] remark service-vlan-id 222
```

2.2.12. traffic behavior

Use **traffic behavior** to create a traffic behavior and enter its view, or enter the view of an existing traffic behavior.

Use **undo traffic behavior** to delete a traffic behavior.

Syntax

traffic behavior *behavior-name*

undo traffic behavior *behavior-name*

Default

No traffic behaviors exist.

Views

System view

Predefined user roles

network-admin

Parameters

behavior-name: Specifies a name for the traffic behavior, a case-sensitive string of 1 to 31 characters.

Examples

Create a traffic behavior named **behavior1**.

```
<Switch> system-view
[Switch] traffic behavior behavior1
[Switch-behavior-behavior1]
```

Related commands

display traffic behavior

2.3. QoS policy commands

2.3.1. classifier behavior

Use **classifier behavior** to associate a traffic behavior with a traffic class in a QoS policy.

Use **undo classifier** to delete a class-behavior association from a QoS policy.

Syntax

classifier *classifier-name* **behavior** *behavior-name* [**insert-before** *before-classifier-name*]

undo classifier *classifier-name*

Default

No traffic behavior is associated with a traffic class.

Views

QoS policy view

Predefined user roles

network-admin

Parameters

classifier-name: Specifies a traffic class by its name, a case-sensitive string of 1 to 31 characters.

behavior-name: Specifies a traffic behavior by its name, a case-sensitive string of 1 to 31 characters.

insert-before *before-classifier-name*: Inserts the new traffic class before an existing traffic class in the QoS policy. The *before-classifier-name* argument specifies an existing traffic class by its name, a case-sensitive string of 1 to 31 characters. If you do not specify the **insert-before** *before-classifier-name* option, the new traffic class is placed at the end of the QoS policy.

Usage guidelines

A traffic class can be associated only with one traffic behavior in a QoS policy.

If the specified traffic class or traffic behavior does not exist, the system defines a null traffic class or traffic behavior.

Examples

Associate traffic class **database** with traffic behavior **test** in QoS policy **user1**.

```
<Switch> system-view
[Switch] qos policy user1
```

```
[Switch-qospolicy-user1] classifier database behavior test
```

Associate traffic class **database** with traffic behavior **test** in QoS policy **user1**, and insert traffic class **database** before an existing traffic class named **class-a**.

```
<Switch> system-view
[Switch] qos policy user1
[Switch-qospolicy-user1] classifier database behavior test insert-before class-a
```

Related commands

qos policy

2.3.2. display qos policy

Use **display qos policy** to display QoS policies.

Syntax

display qos policy user-defined [*policy-name* [**classifier** *classifier-name*]] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

user-defined: Specifies user-defined QoS policies.

policy-name: Specifies a QoS policy by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a QoS policy, this command displays all user-defined QoS policies.

classifier *classifier-name*: Specifies a traffic class by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a traffic class, this command displays all traffic classes.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays the QoS policies for the master device.

Examples

Display all user-defined QoS policies.

```
<Switch> display qos policy user-defined

  User-defined QoS policy information:

  Policy: 1 (ID 100)
   Classifier: 1 (ID 100)
     Behavior: 1
      Marking:
        Remark dscp 3
      Committed Access Rate:
        CIR 112 (kbps), CBS 51200 (Bytes), EBS 512 (Bytes)
        Green action  : pass
        Yellow action : pass
```

```
      Red action    : discard
  Classifier: 2 (ID 101)
    Behavior: 2
     Accounting enable: Packet
     Filter enable: Permit
     Marking:
       Remark dot1p 4
  Classifier: 3 (ID 102)
    Behavior: 3
     -none-
```

Table 2-5 Command output

Field	Description
User-defined QoS policy information	Information about a user-defined QoS policy.
System-defined QoS policy information	Information about a system-defined QoS policy.
Policy	QoS policy name.

For the description of other fields, see Table 2-1 and Table 2-3 .

2.3.3. display qos policy global

Use **display qos policy global** to display QoS policies applied globally.

Syntax

display qos policy global [**slot** *slot-number*] [**inbound** | **outbound**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

inbound: Specifies the QoS policy applied in the inbound direction.

outbound: Specifies the QoS policy applied in the outbound direction.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays global QoS policies for the master device.

Usage guidelines

If you do not specify a direction, this command displays both inbound and outbound global QoS policies.

Examples

Display QoS policies applied globally.

```
<Switch> display qos policy global
  Direction: Inbound
  Policy: 1
```

```
Classifier: 1
  Operator: AND
  Rule(s) :
   If-match acl 2000
  Behavior: 1
   Marking:
     Remark dscp 3
   Committed Access Rate:
     CIR 112 (kbps), CBS 51200 (Bytes), EBS 512 (Bytes)
     Green action  : pass
     Yellow action : pass
     Red action    : discard
     Green packets : 0 (Packets) 0 (Bytes)
     Yellow packets: 0 (Packets) 0 (Bytes)
     Red packets   : 0 (Packets) 0 (Bytes)
Classifier: 2
  Operator: AND
  Rule(s) :
   If-match protocol ipv6
  Behavior: 2
   Accounting enable:
     0 (Packets)
   Filter enable: Permit
   Marking:
     Remark dscp 3
Classifier: 3
  Operator: AND
  Rule(s) :
   -none-
  Behavior: 3
   -none-
```

Table 2-6 Command output

Field	Description
Direction	Direction in which the QoS policy is applied.
Green packets	Statistics about green packets.
Yellow packets	Statistics about yellow packets.
Red packets	Statistics about red packets.

For the description of other fields, see Table 2-1 and Table 2-3 .

2.3.4. display qos policy interface

Use **display qos policy interface** to display the QoS policies applied to interfaces.

Syntax

display qos policy interface [*interface-type interface-number*] [**inbound** | **outbound**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number: Specifies an interface by its type and number.

inbound: Specifies the QoS policy applied to incoming traffic.

outbound: Specifies the QoS policy applied to outgoing traffic.

Usage guidelines

If you do not specify a direction, this command displays the QoS policy applied to incoming traffic and the QoS policy applied to outgoing traffic.

Examples

Display the QoS policy applied to the incoming traffic of GigabitEthernet 1/0/1.

```
<Switch> display qos policy interface gigabitethernet 1/0/1 inbound
Interface: GigabitEthernet1/0/1
  Direction: Inbound
  Policy: 1
   Classifier: 1
     Matched : 0 (Packets) 0 (Bytes)
     5-minute statistics:
      Forwarded: 0/0 (pps/bps)
      Dropped  : 0/0 (pps/bps)
     Operator: AND
     Rule(s) :
      If-match acl 2000
     Behavior: 1
      Marking:
        Remark dscp 3
      Committed Access Rate:
        CIR 112 (kbps), CBS 51200 (Bytes), EBS 512 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : discard
        Green packets : 0 (Packets) 0 (Bytes)
        Yellow packets: 0 (Packets) 0 (Bytes)
        Red packets   : 0 (Packets) 0 (Bytes)
   Classifier: 2
     Matched : 0 (Packets) 0 (Bytes)
     5-minute statistics:
      Forwarded: 0/0 (pps/bps)
```

```
      Dropped  : 0/0 (pps/bps)
    Operator: AND
    Rule(s) :
     If-match protocol ipv6
    Behavior: 2
     Accounting enable:
       0 (Packets)
     Filter enable: Permit
     Marking:
       Remark dscp 3
  Classifier: 3
    Matched : 0 (Packets) 0 (Bytes)
    5-minute statistics:
     Forwarded: 0/0 (pps/bps)
     Dropped  : 0/0 (pps/bps)
    Operator: AND
    Rule(s) :
     -none-
    Behavior: 3
     -none-
```

Display the QoS policies applied to all interfaces.

```
<Switch> display qos policy interface
Interface: GigabitEthernet1/0/1
  Direction: Inbound
  Policy: a
   Classifier: a
     Operator: AND
     Rule(s) :
      If-match any
     Behavior: a
      Mirroring:
        Mirror to the interface: GigabitEthernet1/0/2
      Committed Access Rate:
        CIR 112 (kbps), CBS 51200 (Bytes), EBS 0 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : discard
        Green packets : 0 (Packets)
        Red packets   : 0 (Packets)

Interface: GigabitEthernet1/0/3
  Direction: Inbound
  Policy: b
   Classifier: b
     Operator: AND
     Rule(s) :
      If-match any
```

```
    Behavior: b
     Committed Access Rate:
       CIR 112 (kbps), CBS 51200 (Bytes), EBS 0 (Bytes)
       Green action  : pass
       Yellow action : pass
       Red action    : discard
       Green packets : 0(Packets)
       Red packets   : 0 (Packets)

Interface: GigabitEthernet1/0/3
  Direction: Inbound
  Policy: a
   Classifier: a
     Operator: AND
     Rule(s) :
      If-match any
     Behavior: a
      Mirroring:
        Mirror to the interface: GigabitEthernet1/0/4
      Committed Access Rate:
        CIR 112 (kbps), CBS 51200 (Bytes), EBS 0 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : discard
        Green packets : 0 (Packets)
        Red packets   : 0 (Packets)
```

Table 2-7 Command output

Field	Description
Direction	Direction in which the QoS policy is applied.
Policy	QoS policy name.
Matched	Number of matching packets.
Forwarded	Average rate of successfully forwarded matching packets in a statistics collection period.
Dropped	Average rate of dropped matching packets in a statistics collection period.
Green packets	Traffic statistics for green packets.
Yellow packets	Traffic statistics for yellow packets.
Red packets	Traffic statistics for red packets.

For the description of other fields, see Table 2-1 and Table 2-3 .

2.3.5. display qos vlan-policy

Use **display qos vlan-policy** to display QoS policies applied to VLANs.

Syntax

display qos vlan-policy { **name** *policy-name* | **vlan** [*vlan-id*] } [**slot** *slot-number*] [**inbound** | **outbound**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

name *policy-name*: Specifies a QoS policy by its name, a case-sensitive string of 1 to 31 characters.

vlan *vlan-id*: Specifies a VLAN by its ID in the range of 1 to 4094.

inbound: Displays QoS policies applied to incoming traffic.

outbound: Displays QoS policies applied to outgoing traffic.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays QoS policies applied to VLANs for the master device.

Usage guidelines

If you do not specify a direction, this command displays QoS policies applied to VLANs in both the inbound and outbound directions.

Examples

Display QoS policies applied to VLAN 2.

```
<Switch> display qos vlan-policy vlan 2
Vlan 2
  Direction: Inbound
  Policy: 1
   Classifier: 1
     Operator: AND
     Rule(s) :
      If-match acl 2000
     Behavior: 1
      Marking:
        Remark dscp 3
      Committed Access Rate:
        CIR 112 (kbps), CBS 5120 (Bytes), EBS 512 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : discard
        Green packets : 0 (Packets) 0 (Bytes)
        Yellow packets: 0 (Packets) 0 (Bytes)
        Red packets   : 0 (Packets) 0 (Bytes)
   Classifier: 2
     Operator: AND
     Rule(s) :
      If-match protocol ipv6
```

```
    Behavior: 2
     Accounting enable:
       0 (Packets)
     Filter enable: Permit
     Marking:
       Remark dscp 3
  Classifier: 3
    Operator: AND
    Rule(s) :
     -none-
    Behavior: 3
     -none-
```

Table 2-8 Command output

Field	Description
Direction	Direction in which the QoS policy is applied.
Green packets	Statistics about green packets.
Yellow packets	Statistics about yellow packets.
Red packets	Statistics about red packets.

For the description of other fields, see Table 2-1 and Table 2-3 .

2.3.6. qos apply policy (interface view)

Use **qos apply policy** to apply a QoS policy to an interface.

Use **undo qos apply policy** to remove an applied QoS policy.

Syntax

qos apply policy *policy-name* { **inbound** | **outbound** }

undo qos apply policy *policy-name* { **inbound** | **outbound** }

Default

No QoS policy is applied.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Predefined user roles

network-admin

Parameters

policy-name: Specifies a QoS policy by its name, a case-sensitive string of 1 to 31 characters.

inbound: Applies the QoS policy to incoming traffic.

outbound: Applies the QoS policy to outgoing traffic.

Examples

Apply QoS policy **USER1** to the outgoing traffic of GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] qos apply policy USER1 outbound
```

2.3.7. qos apply policy global

Use **qos apply policy global** to apply a QoS policy globally.

Use **undo qos apply policy global** to remove a globally applied QoS policy.

Syntax

qos apply policy *policy-name* **global** { **inbound** | **outbound** }

undo qos apply policy *policy-name* **global** { **inbound** | **outbound** }

Default

No QoS policy is applied globally.

Views

System view

Predefined user roles

network-admin

Parameters

policy-name: Specifies a QoS policy by its name, a case-sensitive string of 1 to 31 characters.

inbound: Applies the QoS policy to the incoming packets on all interfaces.

outbound: Applies the QoS policy to the outgoing packets on all interfaces.

Usage guidelines

A global QoS policy takes effect on all incoming or outgoing traffic depending on the direction in which the QoS policy is applied.

Examples

Globally apply QoS policy **user1** to the incoming traffic.

```
<Switch> system-view
[Switch] qos apply policy user1 global inbound
```

2.3.8. qos policy

Use **qos policy** to create a QoS policy and enter its view, or enter the view of an existing QoS policy.

Use **undo qos policy** to delete a QoS policy.

Syntax

qos policy *policy-name*

undo qos policy *policy-name*

Default

No QoS policies exist.

Views

System view

Predefined user roles

network-admin

Parameters

policy-name: Specifies a name for the QoS policy, a case-sensitive string of 1 to 31 characters.

Usage guidelines

To delete a QoS policy that has been applied to an object, you must first remove the QoS policy from the object.

Examples

Create a QoS policy named **user1**.

```
<Switch> system-view
[Switch] qos policy user1
[Switch-qospolicy-user1]
```

Related commands

classifier behavior

qos apply policy

qos apply policy global

qos vlan-policy

NOTE:

- This command and **packet-filter** command cannot use on a same port.
- The **mirror-to** command cannot use on an **outbound** port.

2.3.9. qos vlan-policy

Use **qos vlan-policy** to apply a QoS policy to the specified VLANs.

Use **undo qos vlan-policy** to remove a QoS policy from the specified VLANs.

Syntax

qos vlan-policy *policy-name* **vlan** *vlan-id-list* { **inbound** | **outbound** }

undo qos vlan-policy *policy-name* **vlan** *vlan-id-list* { **inbound** | **outbound** }

Default

No QoS policy is applied to a VLAN.

Views

System view

Predefined user roles

network-admin

Parameters

policy-name: Specifies a QoS policy by its name, a case-sensitive string of 1 to 31 characters.

vlan *vlan-id-list*: Specifies a space-separated list of up to eight VLAN IDs or a VLAN ID range in the form of *vlan-id1* **to** *vlan-id2*. The value for *vlan-id2* must be greater than or equal to the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094.

inbound: Applies the QoS policy to incoming packets.

outbound: Applies the QoS policy to outgoing packets.

Examples

Apply QoS policy **test** to the incoming traffic of VLAN 200, VLAN 300, VLAN 400, and VLAN 500.

```
<Switch> system-view
[Switch] qos vlan-policy test vlan 200 300 400 500 inbound
```

2.3.10. reset qos policy global

Use **reset qos policy global** to clear the statistics of a global QoS policy.

Syntax

reset qos policy global [**inbound** | **outbound**]

Views

User view

Predefined user roles

network-admin

Parameters

inbound: Clears the statistics of the global QoS policy applied to incoming traffic globally.

outbound: Clears the statistics of the global QoS policy applied to outgoing traffic globally.

Usage guidelines

If you do not specify a direction, this command clears the statistics of the global QoS policies in both directions.

Examples

Clear the statistics of the global QoS policy applied to the incoming traffic globally.

```
<Switch> reset qos policy global inbound
```

2.3.11. reset qos vlan-policy

Use **reset qos vlan-policy** to clear the statistics for QoS policies applied to VLANs.

Syntax

reset qos vlan-policy [**vlan** *vlan-id*] [**inbound** | **outbound**]

Views

User view

Predefined user roles

network-admin

Parameters

vlan *vlan-id*: Specifies a VLAN ID in the range of 1 to 4094.

inbound: Specifies the QoS policy applied to incoming traffic.

outbound: Specifies the QoS policy applied to outgoing traffic.

Usage guidelines

If you do not specify a direction, this command clears the statistics of the QoS policies in both directions of the VLAN.

Examples

Clear the statistics of QoS policies applied to VLAN 2.

```
<Switch> reset qos vlan-policy vlan 2
```

Contents

A page of this section is **8-x-x**

3. Priority mapping commands 3-1
3.1. Priority map commands 3-1
3.1.1. display qos map-table 3-1
3.1.2. import 3-2
3.1.3. qos map-table 3-2
3.2. Priority trust mode commands 3-3
3.2.1. display qos trust interface 3-3
3.2.2. qos trust 3-4
3.3. Port priority commands 3-4
3.3.1. qos priority 3-4

3. Priority mapping commands

3.1. Priority map commands

3.1.1. display qos map-table

Use **display qos map-table** to display the configuration of priority maps.

Syntax

display qos map-table [**dot1p-lp** | **dscp-dot1p** | **dscp-dscp**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

The device provides the following types of priority map.

Table 3-1 Priority maps

Priority mapping	Description
dot1p-lp	802.1p-local priority map.
dscp-dot1p	DSCP-802.1p priority map.
dscp-dscp	DSCP-DSCP priority map.

Usage guidelines

If you do not specify a priority map, this command displays the configuration of all priority maps.

Examples

Display the configuration of the 802.1p-local priority map.

```
<Switch> display qos map-table dot1p-lp
MAP-TABLE NAME: dot1p-lp   TYPE: pre-define
IMPORT  :  EXPORT
   0    :    2
   1    :    0
   2    :    1
   3    :    3
   4    :    4
   5    :    5
   6    :    6
   7    :    7
```

Table 3-2 Command output

Field	Description
MAP-TABLE NAME	Name of the priority map.
TYPE	Type of the priority map.
IMPORT	Input values of the priority map.
EXPORT	Output values of the priority map.

3.1.2. import

Use **import** to configure mappings for a priority map.

Use **undo import** to restore the specified or all mappings to the default for a priority map.

Syntax

import *import-value-list* **export** *export-value*

undo import { *import-value-list* | **all** }

Default

The default priority maps are used. For more information, see *ACL and QoS Configuration Guide*.

Views

Priority map view

Predefined user roles

network-admin

Parameters

import-value-list: Specifies a list of input values.

export-value: Specifies the output value.

all: Restores all mappings in the priority map to the default.

Examples

Configure the 802.1p-local priority map to map 802.1p priority values 4 and 5 to local priority 1.

```
<Switch> system-view
[Switch] qos map-table dot1p-lp
[Switch-maptbl-dot1p-lp] import 4 5 export 1
```

Related commands

display qos map-table

3.1.3. qos map-table

Use **qos map-table** to enter the specified priority map view.

Syntax

qos map-table { **dot1p-lp** | **dscp-dot1p** | **dscp-dscp** }

Views

System view

Predefined user roles

network-admin

Parameters

For the description of the keywords, see Table 3-1 .

Examples

Enter 802.1p-local priority map view.

```
<Switch> system-view
[Switch] qos map-table dot1p-lp
[Switch-maptbl-dot1p-lp]
```

Related commands

display qos map-table

import

3.2. Priority trust mode commands

3.2.1. display qos trust interface

Use **display qos trust interface** to display the priority trust mode and port priorities of an interface.

Syntax

display qos trust interface [*interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number: Specifies an interface by its type and number. If you do not specify an interface, this command displays the priority trust mode and port priorities of all interfaces.

Examples

Display the priority trust mode and port priority of GigabitEthernet 1/0/1.

```
<Switch> display qos trust interface gigabitethernet 1/0/1
Interface: GigabitEthernet1/0/1
 Port priority trust information
  Port priority:4
  Port priority trust type: dscp
```

Table 3-3 Command output

Field	Description
Interface	Interface type and interface number.

Field	Description
Port priority	Port priority set for the interface.
Port priority trust type	Priority trust mode on the interface: • **dot1p**—Uses the 802.1p priority of received packets for mapping. • **dscp**—Uses the DSCP precedence of received IP packets for mapping. • **none**—Trusts no packet priority.

3.2.2. qos trust

Use **qos trust** to configure the priority trust mode for an interface.

Use **undo qos trust** to restore the default.

Syntax

qos trust { **dot1p** | **dscp** }

undo qos trust

Default

An interface does not trust any packet priority and uses the port priority as the 802.1p priority for mapping.

Views

Layer 2/Layer 3 Ethernet interface view

Predefined user roles

network-admin

Parameters

dot1p: Uses the 802.1p priority in incoming packets for priority mapping.

dscp: Uses the DSCP value in incoming packets for priority mapping.

Examples

Set the priority trust mode to 802.1p priority on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] qos trust dot1p
```

Related commands

display qos trust interface

3.3. Port priority commands

3.3.1. qos priority

Use **qos priority** to change the port priority of an interface.

Use **undo qos priority** to restore the default.

Syntax

qos priority *priority-value*

undo qos priority

Default

The port priority is 0.

Views

Layer 2/Layer 3 Ethernet interface view

Predefined user roles

network-admin

Parameters

priority-value: Specifies a port priority value in the range of 0 to 7.

Examples

Set the port priority of GigabitEthernet 1/0/1 to 2.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] qos priority 2
```

Related commands

display qos trust interface

Contents

A page of this section is **8-x-x**

4. GTS and rate limit commands ····· 4-1
4.1. GTS commands ····· 4-1
4.1.1. display qos gts interface ····· 4-1
4.1.2. qos gts ····· 4-1
4.2. Rate limit commands ····· 4-2
4.2.1. display qos lr interface ····· 4-2
4.2.2. qos lr ····· 4-3

4. GTS and rate limit commands

4.1. GTS commands

4.1.1. display qos gts interface

Use **display qos gts interface** to display the GTS configuration and statistics for interfaces.

Syntax

display qos gts interface [*interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number: Specifies an interface by its type and number. If you do not specify an interface, this command displays the GTS configuration and statistics for all interfaces.

Examples

Display the GTS configuration and statistics for all interfaces.

```
<Switch> display qos gts interface
Interface: GigabitEthernet1/0/1
 Rule: If-match queue 1
  CIR 512 (kbps), CBS 51200 (Bytes)
```

Table 4-1 Command output

Field	Description
Interface	Interface name, including the interface type and interface number.
Rule	Match criteria.
CIR	CIR in kbps.
CBS	CBS in bytes.

4.1.2. qos gts

Use **qos gts** to set GTS parameters on an interface.

Use **undo qos gts** to delete the GTS configuration on an interface.

Syntax

qos gts queue *queue-id* **cir** *committed-information-rate* [**cbs** *committed-burst-size*]

undo qos gts queue *queue-id*

Default

No GTS parameters are configured.

Views

Layer 2/Layer 3 Ethernet interface view

Predefined user roles

network-admin

Parameters

queue *queue-id*: Shapes the packets in a queue specified by its ID. The value range for *queue-id* is 0 to 7.

cir *committed-information-rate*: Specifies the CIR in kbps. The value range for *committed-information-rate* is 1000 to 1048576 for GE interfaces and 1000 to 10485760 for 10-GE interfaces.

cbs *committed-burst-size*: Specifies the CBS in bytes. The value range for *committed-burst-size* is 512 to 16777216, in increments of 512. The default value for this argument is the product of 62.5 and the CIR and must be an integral multiple of 512. When the product is not an integral multiple of 512, it is rounded up to the nearest integral multiple of 512 that is greater than the product. A default value greater than 16777216 is converted to 16777216.

Examples

Shape the packets of queue 1 on GigabitEthernet 1/0/1. The GTS parameters are as follows:

- The CIR is 6400 kbps.
- The CBS is 51200 bytes.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] qos gts queue 1 cir 6400 cbs 51200
```

4.2. Rate limit commands

4.2.1. display qos lr interface

Use **display qos lr interface** to display the rate limit configuration for interfaces.

Syntax

display qos lr interface [*interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number: Specifies an interface by its type and number. If you do not specify an interface, this command displays the rate limit configuration for all interfaces.

Examples

Display the rate limit configuration for all interfaces.

```
<Switch> display qos lr interface
Interface: GigabitEthernet1/0/1
 Direction: Outbound
  CIR 2000 (kbps), CBS 20480 (Bytes)
```

Table 4-2 Command output

Field	Description
Interface	Interface name, including the interface type and interface number.
Direction	Direction in which the rate limit configuration is applied.
CIR	CIR in kbps.
CBS	CBS in bytes.

4.2.2. qos lr

Use **qos lr** to configure rate limiting on an interface.

Use **undo qos lr** to delete the rate limit configuration on an interface.

Syntax

qos lr { **inbound** | **outbound** } **cir** *committed-information-rate* [**cbs** *committed-burst-size*]

undo qos lr { **inbound** | **outbound** }

Default

No rate limit is configured.

Views

Layer 2/Layer 3 Ethernet interface view

Predefined user roles

network-admin

Parameters

inbound: Limits the rate of incoming packets.

outbound: Limits the rate of outgoing packets.

cir *committed-information-rate*: Specifies the CIR in kbps. The value range for *committed-information-rate* is 1000 to 1048576 for GE interfaces and 1000 to 10485760 for 10-GE interfaces.

cbs *committed-burst-size*: Specifies the CBS in bytes. The value range for *committed-burst-size* is 512 to 134217728, in increments of 512. The default value for this argument is the product of 62.5 and the CIR and must be an integral multiple of 512. When the product is not an integral multiple of 512, it is rounded up to the nearest integral multiple of 512 that is greater than the product. A default value greater than 134217728 is converted to 134217728.

Examples

Limit the rate of outgoing packets on GigabitEthernet 1/0/1, with CIR 256 kbps and CBS 51200 bytes.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
```

```
[Switch-GigabitEthernet1/0/1] qos lr outbound cir 256 cbs 51200
```

Contents

A page of this section is **8-x-x**

5. Congestion management commands 5-1
5.1. SP commands 5-1
5.1.1. display qos queue sp interface 5-1
5.1.2. qos sp 5-1
5.2. WRR commands 5-2
5.2.1. display qos queue wrr interface 5-2
5.2.2. qos wrr 5-3
5.2.3. qos wrr weight 5-3
5.2.4. qos wrr group sp 5-5
5.3. Queue-based accounting commands 5-5
5.3.1. display qos queue-statistics interface outbound 5-5

5. Congestion management commands

5.1. SP commands

5.1.1. display qos queue sp interface

Use **display qos queue sp interface** to display the SP queuing configuration of an interface.

Syntax

display qos queue sp interface [*interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number: Specifies an interface by its type and number. If you do not specify an interface, this command displays the SP queuing configuration of all interfaces.

Examples

Display the SP queuing configuration of GigabitEthernet 1/0/1.

```
<Switch> display qos queue sp interface gigabitethernet 1/0/1
Interface: GigabitEthernet1/0/1
 Output queue: Strict Priority queuing
```

Table 5-1 Command output

Field	Description
Interface	Interface type and interface number.
Output queue	Type of the current output queue.

5.1.2. qos sp

Use **qos sp** to enable SP queuing on an interface.

Use **undo qos sp** to restore the default.

Syntax

qos sp

undo qos sp

Default

An interface uses packet-count WRR queuing.

Views

Layer 2/Layer 3 Ethernet interface view

Predefined user roles

network-admin

Examples

Enable SP queuing on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] qos sp
```

Related commands

display qos queue sp interface

5.2. WRR commands

5.2.1. display qos queue wrr interface

Use **display qos queue wrr interface** to display the WRR queuing configuration of an interface.

Syntax

display qos queue wrr interface [*interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number: Specifies an interface by its type and number. If you do not specify an interface, this command displays the WRR queuing configuration of all interfaces.

Examples

Display the WRR queuing configuration of GigabitEthernet 1/0/1.

```
<Switch> display qos queue wrr interface gigabitethernet 1/0/1
Interface: GigabitEthernet1/0/1
 Output queue: Weighted Round Robin queuing
 Queue ID        Queue name      Group           Weight
 ------------------------------------------------------
 0               be              1               1
 1               af1             1               1
 2               af2             1               1
 3               af3             1               1
 4               af4             1               1
 5               ef              1               1
 6               cs6             1               1
 7               cs7             sp              N/A
```

Table 5-2 Command output

Field	Description
Interface	Interface type and interface number.
Output queue	Type of the current output queue.
Group	ID of the group a queue is assigned to. The group ID can only be 1.
Weight	Packet-count queue scheduling weight of a queue. N/A is displayed for a queue that uses the SP scheduling algorithm.

5.2.2. qos wrr

Use **qos wrr** to enable WRR queuing on an interface.

Use **undo qos wrr** to restore the default.

Syntax

qos wrr weight

undo qos wrr weight

Default

An interface uses packet-count WRR queuing.

Views

Layer 2/Layer 3 Ethernet interface view

Predefined user roles

network-admin

Parameters

weight: Allocates bandwidth to queues in packets.

Usage guidelines

You must use the **qos wrr** command to enable WRR queuing before you can configure WRR queuing parameters for a queue on an interface.

Examples

Enable packet-count WRR queuing on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] qos wrr weight
```

Related commands

display qos queue wrr interface

5.2.3. qos wrr weight

Use **qos wrr weight** to configure the WRR queuing parameters for a queue on an interface.

Use **undo qos wrr** to restore the default.

Syntax

qos wrr *queue-id* **group 1 weight** *schedule-value*

undo qos wrr *queue-id*

Default

All queues on a WRR-enabled interface are in WRR group 1, and queues 0 through 7 have a weight of 1, 2, 3, 4, 5, 9, 13, and 15, respectively.

Views

Layer 2/Layer 3 Ethernet interface view

Predefined user roles

network-admin

Parameters

queue-id: Specifies a queue by its ID. The value range for this argument is 0 to 7 or keywords in Table 5-3 .

Table 5-3 The number-keyword map for the queue-id argument

Number	Keyword
0	be
1	af1
2	af2
3	af3
4	af4
5	ef
6	cs6
7	cs7

group 1: Specifies WRR group 1. Only WRR group 1 is supported in the current software version.

weight: Allocates bandwidth to queues in packets.

schedule-value: Specifies a scheduling weight in the range of 1 to 15.

Usage guidelines

You must use the **qos wrr** command to enable WRR queuing before you can configure WRR queuing parameters for a queue on an interface.

Examples

Enable packet-based WRR queuing on GigabitEthernet 1/0/1, assign queue 0 to WRR group 1, and specify scheduling weight 10 for queue 0.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] qos wrr weight
[Switch-GigabitEthernet1/0/1] qos wrr 0 group 1 weight 10
```

Related commands

display qos queue wrr interface

qos wrr

5.2.4. qos wrr group sp

Use **qos wrr group sp** to assign a queue to the SP group.

Use **undo qos wrr group sp** to remove a queue from the SP group.

Syntax

qos wrr *queue-id* **group sp**

undo qos wrr *queue-id*

Default

All queues on a WRR-enabled interface are in WRR group 1.

Views

Layer 2/Layer 3 Ethernet interface view

Predefined user roles

network-admin

Parameters

queue-id: Specifies a queue by its ID. The value range for this argument is 0 to 7 or keywords in Table 5-3 .

Usage guidelines

This command is available only on a WRR-enabled interface. Queues in the SP group are scheduled with SP. The SP group has higher scheduling priority than the WRR groups.

You must use the **qos wrr** command to enable WRR queuing before you can configure this command on an interface.

Examples

Enable WRR queuing on GigabitEthernet 1/0/1, and assign queue 0 to the SP group.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] qos wrr weight
[Switch-GigabitEthernet1/0/1] qos wrr 0 group sp
```

Related commands

display qos queue wrr interface

qos wrr

5.3. Queue-based accounting commands

5.3.1. display qos queue-statistics interface outbound

Use **display qos queue-statistics interface outbound** to display queue-based outgoing traffic statistics for interfaces.

Syntax

display qos queue-statistics interface [*interface-type interface-number*] **outbound**

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number: Specifies an interface by its type and number. If you do not specify an interface, this command displays the queue-based outgoing traffic statistics for all interfaces.

Examples

Display queue-based outgoing traffic statistics for GigabitEthernet 1/0/1.

```
<Switch> display qos queue-statistics interface gigabitethernet 1/0/1 outbound
Interface: GigabitEthernet1/0/1
 Direction: outbound
 Forwarded: 0 packets, 0 bytes
 Dropped: 0 packets, 0 bytes
 Queue 0
  Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps
  Dropped: 0 packets, 0 bytes
  Current queue length: 0 packets
 Queue 1
  Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps
  Dropped: 0 packets, 0 bytes
  Current queue length: 0 packets
 Queue 2
  Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps
  Dropped: 0 packets, 0 bytes
  Current queue length: 0 packets
 Queue 3
  Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps
  Dropped: 0 packets, 0 bytes
  Current queue length: 0 packets
 Queue 4
  Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps
  Dropped: 0 packets, 0 bytes
  Current queue length: 0 packets
 Queue 5
  Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps
  Dropped: 0 packets, 0 bytes
  Current queue length: 0 packets
 Queue 6
  Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps
  Dropped: 0 packets, 0 bytes
  Current queue length: 0 packets
 Queue 7
  Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps
```

```
Dropped: 0 packets, 0 bytes
Current queue length: 0 packets
```

Table 5-4 Command output

Field	Description
Interface	Interface for which queue-based traffic statistics are displayed.
Direction	Direction of traffic for which statistics are collected.
Forwarded	Counts forwarded traffic both in packets and in bytes.
Dropped	Counts dropped traffic both in packets and in bytes.
Current queue length	Number of packets in the queue.

Related commands

`reset counters interface` (*Interface Command Reference*)

Contents

A page of this section is **8-x-x**

6. Data buffer commands 6-1
6.1. Data buffer commands 6-1
6.1.1. buffer apply 6-1
6.1.2. buffer shared 6-1
6.1.3. burst-mode enable 6-2
6.1.4. display buffer 6-3

6. Data buffer commands

6.1. Data buffer commands

6.1.1. buffer apply

Use **buffer apply** to apply manually configured data buffer settings.

Use **undo buffer apply** to restore the default.

Syntax

buffer apply

undo buffer apply

Views

System view

Predefined user roles

network-admin

Usage guidelines

For data buffer settings to take effect, you must execute this command after configuring data buffer settings.

After applying manually configured data buffer settings, you cannot directly modify the applied settings. To modify them, you must cancel the application, reconfigure data buffer settings, and reapply the new settings.

Examples

Apply manually configured data buffer settings.

```
<Switch> system-view
[Switch] buffer apply
```

NOTE:

buffer apply command is supported from later software, including Version 7.3.24.

6.1.2. buffer shared

Use **buffer shared** to set the maximum shared-area ratio for each port or a queue.

Use **undo buffer shared** to delete the maximum shared-area ratio setting of each port or a queue.

Syntax

buffer egress [**slot** *slot-number*] **cell** [**queue** *queue-id*] **shared ratio** *ratio*

undo buffer egress [**slot** *slot-number*] **cell** [**queue** *queue-id*] **shared**

Default

The maximum cell resource ratio for a port is 33% of the total cell resources.

The maximum cell resource ratio for a queue is 33% of the total cell resources.

Views

System view

Predefined user roles

network-admin

Parameters

egress: Specifies the egress buffer.

slot *slot-number*: Specifies an IRF member device by its member ID (slot number). If you do not specify an IRF member device, this command applies to all IRF member devices.

cell: Specifies cell resources.

queue-id: Specifies a queue by its ID in the range of 0 to 7.

ratio *ratio*: Specifies the maximum shared-area space ratio, in percentage. The value range for *ratio* is 0 to 100.

Usage guidelines

By default, all ports or queueshave an equal share of the shared area. You can set the shared-area ratio for each port or a queue. The unconfigured queues use the default setting. The shared-area space for each port or queue is finally determined by the chip based on your configuration and the number of packets to be received and sent.

Examples

Configure queue 0 to use up to 10% shared-area space of cell resources in the egress buffer.

```
<Switch> system-view
[Switch] buffer egress cell queue 0 shared ratio 4
```

NOTE:

- **buffer shared** command is supported from later software, including Version 7.3.24.
- NEC recommends that you use this command for only QoS Congestion management such as SP queuing, and NEC recommends the following parameters:

  buffer egress cell queue 7 shared ratio 4
  buffer egress cell queue 6 shared ratio 4
  buffer egress cell queue 5 shared ratio 4
  buffer egress cell queue 4 shared ratio 4
  buffer egress cell queue 3 shared ratio 4
  buffer egress cell queue 2 shared ratio 4
  buffer egress cell queue 1 shared ratio 4
  buffer egress cell queue 0 shared ratio 4
- Inappropriate data buffer changes can cause system problems. Before manually changing data buffer settings, make sure you understand its impact on your device. NEC recommends testing before manually changing to other parameters.

6.1.3. burst-mode enable

Use **burst-mode enable** to enable the Burst feature.

Use **undo burst-mode enable** to disable the Burst feature.

Syntax

burst-mode enable

undo burst-mode enable

Default

The Burst feature is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

The Burst feature is especially useful for reducing packet losses under the following circumstances:

- Broadcast or multicast traffic is intensive, resulting in bursts of traffic.
- Traffic enters a device from a high-speed interface and goes out of a low-speed interface.
- Traffic enters a device from multiple same-rate interfaces and goes out of an interface with the same rate.

Examples

Enable the Burst feature.

```
<Switch> system-view
[Switch] burst-mode enable
```

6.1.4. display buffer

Use **display buffer** to display buffer size settings.

Syntax

display buffer [**slot** *slot-number*][**queue** [*queue-id*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID (slot number). If you do not specify an IRF member device, this command displays buffer size settings for all IRF member devices.

queue *queue-id*: Specifies a queue by its number in the range of 0 to 7. If you specify a queue, this command displays the fixed-area ratio and shared-area ratio for the specified queue. If you specify the **queue** keyword without the *queue-id* argument, this command displays the fixed-area ratio and shared-area ratio for each queue. If you do not specify the **queue** keyword, this command displays the total shared-area ratio.

Examples

Display buffer size settings.

```
<Switch> display buffer
Slot  Type    Eg(Total-shared , Shared)
1     cell    77 , 33

          Eg: Size of the sending buffer
Total-shared: Size of the shared buffer for all ports
      Shared: Size of the maximum shared buffer per port
        Unit: Ratio
```

Display the fixed-area ratio and shared-area ratio for the queues.

```
<Switch> display buffer queue
Slot  Queue        Type    Eg(Guaranteed , Shared)
1     0-7          cell    12 , 10

          Eg: Size of the sending buffer
  Guaranteed: Size of the minimum guaranteed buffer per queue
      Shared: Size of the maximum shared buffer per queue
        Unit: Ratio
```

Table 6-1 Command output

Field	Description
Type	Resource type.
Queue	Queue ID in the range of 0 to 7.
Eg	Egress buffer.
(Total-shared , Shared)	Total-shared indicates the total shared-area ratio. Shared indicates the shared-area ratio of a port.
(Guaranteed , Shared)	• **Guaranteed** indicates the fixed-area ratio of a queue. • **Shared** indicates the shared-area ratio of a queue.

NOTE:

display buffer command is supported from later software, including Version 7.3.24.

Contents

A page of this section is **8-x-x**

7. Time range commands 7-1
7.1. Time range commands 7-1
7.1.1. display time-range 7-1
7.1.2. time-range 7-1

7. Time range commands

7.1. Time range commands

7.1.1. display time-range

Use **display time-range** to display time range configuration and status.

Syntax

display time-range { *time-range-name* | **all** }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

time-range-name: Specifies a time range name, a case-insensitive string of 1 to 32 characters. It must start with an English letter.

all: Displays the configuration and status of all existing time ranges.

Examples

Display the configuration and status of time range **t4**.

```
<Switch> display time-range t4
Current time is 17:12:34 11/23/2010 Tuesday

Time-range : t4 (Inactive)
 10:00 to 12:00 Mon
 14:00 to 16:00 Wed
 from 00:00 1/1/2011 to 00:00 1/1/2012
 from 00:00 6/1/2011 to 00:00 7/1/2011
```

Table 7-1 Command output

Field	Description
Current time	Current system time.
Time-range	Configuration and status of the time range, including its name, status (active or inactive), and start time and end time.

7.1.2. time-range

Use **time-range** to create or edit a time range.

Use **undo time-range** to delete a time range or a statement in the time range.

Syntax

time-range *time-range-name* { *start-time* **to** *end-time days* [**from** *time1 date1*] [**to** *time2 date2*] | **from** *time1 date1* [**to** *time2 date2*] | **to** *time2 date2* }

undo time-range *time-range-name* [*start-time* **to** *end-time days* [**from** *time1 date1*] [**to** *time2 date2*] | **from** *time1 date1* [**to** *time2 date2*] | **to** *time2 date2*]

Default

No time ranges exist.

Views

System view

Predefined user roles

network-admin

Parameters

time-range-name: Specifies a time range name. The name is a case-insensitive string of 1 to 32 characters. It must start with an English letter. To avoid confusion, it cannot be **all**.

start-time **to** *end-time*: Specifies a periodic statement. Both *start-time* and *end-time* are in hh:mm format (24-hour clock). The value is in the range of 00:00 to 23:59 for the start time, and 00:00 to 24:00 for the end time. The end time must be greater than the start time.

days: Specifies the day or days of the week (in words or digits) on which the periodic statement is valid. If you specify multiple values, separate each value with a space, and make sure they do not overlap. These values can take one of the following forms:

- A digit in the range of 0 to 6, for Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday.
- A day of a week in abbreviated words: **Sun**, **Mon**, **Tue**, **Wed**, **Thu**, **Fri**, and **Sat**.
- **working-day** for Monday through Friday.
- **off-day** for Saturday and Sunday.
- **daily** for the whole week.

from *time1 date1*: Specifies the start time and date of an absolute statement. The *time1* argument specifies the time of the day in hh:mm format (24-hour clock). Its value is in the range of 00:00 to 23:59. The *date1* argument specifies a date in MM/DD/YYYY or YYYY/MM/DD format, where MM is the month of the year in the range of 1 to 12, DD is the day of the month with the range varying by MM, and YYYY is the year in the calendar in the range of 1970 to 2100. If you do not specify this option, the start time is 01/01/1970 00:00 AM, the earliest time available in the system.

to *time2 date2*: Specifies the end time and date of the absolute time statement. The *time2* argument has the same format as the *time1* argument, but its value is in the range of 00:00 to 24:00. The *date2* argument has the same format and value range as the *date1* argument. The end time must be greater than the start time. If you do not specify this option, the end time is 12/31/2100 24:00 PM, the maximum time available in the system.

Usage guidelines

If an existing time range name is provided, this command adds a statement to the time range.

You can create multiple statements in a time range. Each time statement can take one of the following forms:

- Periodic statement in the *start-time* **to** *end-time days* format. A periodic statement recurs periodically on a day or days of the week.

- Absolute statement in the **from** *time1 date1* **to** *time2 date2* format. An absolute statement does not recur.
- Compound statement in the *start-time* **to** *end-time days* **from** *time1 date1* **to** *time2 date2* format. A compound statement recurs on a day or days of the week only within the specified period. For example, to create a time range that is active from 08:00 to 12:00 on Monday between January 1, 2015, 00:00 and December 31, 2015, 23:59, use the **time-range test 08:00 to 12:00 Mon from 00:00 01/01/2015 to 23:59 12/31/2015** command.

You can create a maximum of 1024 time ranges, each with a maximum of 32 periodic statements and 12 absolute statements. The active period of a time range is calculated as follows:

1. Combining all periodic statements.
2. Combining all absolute statements.
3. Taking the intersection of the two statement sets as the active period of the time range.

Examples

Create a periodic time range **t1**, setting it to be active between 8:00 to 18:00 during working days.

```
<Switch> system-view
[Switch] time-range t1 08:00 to 18:00 working-day
```

Create an absolute time range **t2**, setting it to be active in the whole year of 2011.

```
<Switch> system-view
[Switch] time-range t2 from 00:00 1/1/2011 to 24:00 12/31/2011
```

Create a compound time range **t3**, setting it to be active from 08:00 to 12:00 on Saturdays and Sundays of the year 2011.

```
<Switch> system-view
[Switch] time-range t3 08:00 to 12:00 off-day from 00:00 1/1/2011 to 24:00 12/31/2011
```

Create a compound time range **t4**, setting it to be active from 10:00 to 12:00 on Mondays and from 14:00 to 16:00 on Wednesdays in January and June of the year 2011.

```
<Switch> system-view
[Switch] time-range t4 10:00 to 12:00 1 from 00:00 1/1/2011 to 24:00 1/31/2011
[Switch] time-range t4 14:00 to 16:00 3 from 00:00 6/1/2011 to 24:00 6/30/2011
```

Related commands

display time-range

QX-S5600G Series Ethernet Switches

Command References

9.Security

This manual is including the following chapters.

01-AAA commands

02-802.1X commands

03-MAC authentication commands

04-Web authentication commands

05-Port security commands

06-Password control commands

07-Public key management commands

08-PKI commands

09-SSH commands

10-SSL commands

11-Attack detection and prevention commands

12-IP source guard commands

13-ARP attack protection commands

14-IPv4 uRPF commands

Contents

A page of this section is **9-x-x**

1. AAA commands 1-1
1.1. General AAA commands 1-1
1.1.1. aaa session-limit 1-1
1.1.2. accounting default 1-1
1.1.3. accounting lan-access 1-2
1.1.4. accounting login 1-3
1.1.5. accounting start-fail 1-4
1.1.6. accounting update-fail 1-5
1.1.7. authentication default 1-6
1.1.8. authentication lan-access 1-7
1.1.9. authentication login 1-8
1.1.10. authorization command 1-9
1.1.11. authorization default 1-10
1.1.12. authorization lan-access 1-11
1.1.13. authorization login 1-12
1.1.14. display domain 1-13
1.1.15. domain 1-17
1.1.16. domain default enable 1-18
1.1.17. state (ISP domain view) 1-18
1.2. Local user commands 1-19
1.2.1. access-limit 1-19
1.2.2. authorization-attribute (local user view/user group view) 1-20
1.2.3. bind-attribute 1-21
1.2.4. display local-user 1-23
1.2.5. display user-group 1-26
1.2.6. group 1-27
1.2.7. local-user 1-28
1.2.8. password (device management user view) 1-29
1.2.9. password (network access user view) 1-30
1.2.10. service-type 1-31
1.2.11. state (local user view) 1-31
1.2.12. user-group 1-32
1.3. RADIUS commands 1-33
1.3.1. accounting-on enable 1-33
1.3.2. data-flow-format (RADIUS scheme view) 1-34
1.3.3. display radius scheme 1-35
1.3.4. display radius statistics 1-38
1.3.5. display stop-accounting-buffer (for RADIUS) 1-39
1.3.6. key (RADIUS scheme view) 1-40
1.3.7. nas-ip (RADIUS scheme view) 1-41
1.3.8. primary accounting (RADIUS scheme view) 1-43
1.3.9. primary authentication (RADIUS scheme view) 1-44
1.3.10. radius dscp 1-45
1.3.11. radius nas-ip 1-46
1.3.12. radius scheme 1-47
1.3.13. reauthentication server-select 1-48
1.3.14. reset radius statistics 1-49
1.3.15. reset stop-accounting-buffer (for RADIUS) 1-50
1.3.16. retry 1-50
1.3.17. retry realtime-accounting 1-51
1.3.18. retry stop-accounting (RADIUS scheme view) 1-53
1.3.19. secondary accounting (RADIUS scheme view) 1-54

1.3.20. secondary authentication (RADIUS scheme view) ····· 1-55
1.3.21. snmp-agent trap enable radius ····· 1-57
1.3.22. state primary ····· 1-58
1.3.23. state secondary ····· 1-59
1.3.24. stop-accounting-buffer enable (RADIUS scheme view) ····· 1-60
1.3.25. timer quiet (RADIUS scheme view) ····· 1-61
1.3.26. timer realtime-accounting (RADIUS scheme view) ····· 1-62
1.3.27. timer response-timeout (RADIUS scheme view) ····· 1-63
1.3.28. user-name-format (RADIUS scheme view) ····· 1-64

1. AAA commands

1.1. General AAA commands

1.1.1. aaa session-limit

Use **aaa session-limit** to set the maximum number of concurrent users that can log on to the device through the specified method.

Use **undo aaa session-limit** to restore the default maximum number of concurrent users for the specified login method.

Syntax

aaa session-limit { **ftp** | **http** | **https** | **ssh** | **telnet** } *max-sessions*

undo aaa session-limit { **ftp** | **http** | **https** | **ssh** | **telnet** }

Default

The maximum number of concurrent users is 32 for each user type.

Views

System view

Predefined user roles

network-admin

Parameters

ftp: FTP users.

http: HTTP users.

https: HTTPS users.

ssh: SSH users.

telnet: Telnet users.

max-sessions: Specifies the maximum number of concurrent login users. The value range is 1 to 32 for FTP, SSH, and Telnet services, and is 1 to 64 for HTTP and HTTPS services.

Usage guidelines

After the maximum number of concurrent login users for a user type exceeds the upper limit, the system denies the subsequent users of this type.

Examples

Set the maximum number of concurrent FTP users to 4.

```
<Switch> system-view
[Switch] aaa session-limit ftp 4
```

1.1.2. accounting default

Use **accounting default** to specify default accounting methods for an ISP domain.

Use **undo accounting default** to restore the default.

Syntax

accounting default { **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo accounting default

Default

The default accounting method of an ISP domain is local.

Views

ISP domain view

Predefined user roles

network-admin

Parameters

local: Performs local accounting.

none: Does not perform accounting.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

The default accounting method is used for all users that support this method and do not have an accounting method configured.

Local accounting is only used for monitoring and controlling the number of local user connections. It does not provide the statistics function that the accounting feature generally provides.

You can specify one primary default accounting method and multiple backup default accounting methods.

When the primary method is invalid, the device attempts to use the backup methods in sequence. For example, the **accounting default radius-scheme** *radius-scheme-name* **local none** command specifies the primary default RADIUS accounting method and two backup methods (local accounting and no accounting). The device performs RADIUS accounting by default and performs local accounting when the RADIUS server is invalid. The device does not perform accounting when both of the previous methods are invalid.

Examples

In ISP domain **test**, use RADIUS scheme **rd** as the primary default accounting method and use local accounting as the backup.

```
<Switch> system-view
[Switch] domain test
[Switch-isp-test] accounting default radius-scheme rd local
```

Related commands

local-user

radius scheme

1.1.3. accounting lan-access

Use **accounting lan-access** to specify accounting methods for LAN users.

Use **undo accounting lan-access** to restore the default.

Syntax

accounting lan-access { **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo accounting lan-access

Default

The default accounting methods of the ISP domain are used for LAN users.

Views

ISP domain view

Predefined user roles

network-admin

Parameters

local: Performs local accounting.

none: Does not perform accounting.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

You can specify one primary accounting method and multiple backup accounting methods.

When the primary method is invalid, the device attempts to use the backup methods in sequence. For example, the **accounting lan-access radius-scheme** *radius-scheme-name* **local none** command specifies a primary RADIUS accounting method and two backup methods (local accounting and no accounting). The device performs RADIUS accounting by default and performs local accounting when the RADIUS server is invalid. The device does not perform accounting when both of the previous methods are invalid.

Examples

In ISP domain **test**, perform local accounting for LAN users.

```
<Switch> system-view
[Switch] domain test
[Switch-isp-test] accounting lan-access local
```

In ISP domain **test**, perform RADIUS accounting for LAN users based on scheme **rd** and use local accounting as the backup.

```
<Switch> system-view
[Switch] domain test
[Switch-isp-test] accounting lan-access radius-scheme rd local
```

Related commands

accounting default

local-user

radius scheme

1.1.4. accounting login

Use **accounting login** to specify accounting methods for login users.

Use **undo accounting login** to restore the default.

Syntax

accounting login { **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo accounting login

Default

The default accounting methods of the ISP domain are used for login users.

Views

ISP domain view

Predefined user roles

network-admin

Parameters

local: Performs local accounting.

none: Does not perform accounting.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

Accounting is not supported for FTP, SFTP, and SCP users.

You can specify one primary accounting method and multiple backup accounting methods.

When the primary method is invalid, the device attempts to use the backup methods in sequence. For example, the **accounting login radius-scheme** *radius-scheme-name* **local none** command specifies a primary default RADIUS accounting method and two backup methods (local accounting and no accounting). The device performs RADIUS accounting by default and performs local accounting when the RADIUS server is invalid. The device does not perform accounting when both of the previous methods are invalid.

Examples

In ISP domain **test**, perform local accounting for login users.

```
<Switch> system-view
[Switch] domain test
[Switch-isp-test] accounting login local
```

In ISP domain **test**, perform RADIUS accounting for login users based on scheme **rd** and use local accounting as the backup.

```
<Switch> system-view
[Switch] domain test
[Switch-isp-test] accounting login radius-scheme rd local
```

Related commands

accounting default

local-user

radius scheme

1.1.5. accounting start-fail

Use **accounting start-fail** to configure access control for users that encounter accounting-start failures.

Use **undo accounting start-fail** to restore the default.

Syntax

accounting start-fail { **offline** | **online** }

undo accounting start-fail

Default

The device allows users that encounter accounting-start failures to stay online.

Views

ISP domain view

Predefined user roles

network-admin

Parameters

offline: Logs off users that encounter accounting-start failures.

online: Allows users that encounter accounting-start failures to stay online.

Examples

In ISP domain **test**, configure the device to allow users that encounter accounting-start failures to stay online.

```
<Switch> system-view
[Switch] domain test
[Switch-isp-test] accounting start-fail online
```

1.1.6. accounting update-fail

Use **accounting update-fail** to configure access control for users that have failed all their accounting-update attempts.

Use **undo accounting update-fail** to restore the default.

Syntax

accounting update-fail { [**max-times** *max-times*] **offline** | **online** }

undo accounting update-fail

Default

The device allows users that have failed all their accounting-update attempts to stay online.

Views

ISP domain view

Predefined user roles

network-admin

Parameters

max-times *max-times*: Specifies the maximum number of consecutive accounting-update failures allowed by the device for each user. The value range for the *times* argument is 1 to 255, and the default value is 1.

offline: Logs off users that have failed all their accounting-update attempts.

online: Allows users that have failed all their accounting-update attempts to stay online.

Examples

In ISP domain **test**, configure the device to allow users that have failed all their accounting-update attempts to stay online.

```
<Switch> system-view
[Switch] domain test
[Switch-isp-test] accounting update-fail online
```

1.1.7. authentication default

Use **authentication default** to specify default authentication methods for an ISP domain.

Use **undo authentication default** to restore the default.

Syntax

authentication default { **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo authentication default

Default

The default authentication method of an ISP domain is local.

Views

ISP domain view

Predefined user roles

network-admin

Parameters

local: Performs local authentication.

none: Does not perform authentication.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

The default authentication method is used for all users that support this method and do not have an authentication method configured.

You can specify one primary default authentication method and multiple backup default authentication methods.

When the primary method is invalid, the device attempts to use the backup methods in sequence. For example, the **authentication default radius-scheme** *radius-scheme-name* **local none** command specifies a primary default RADIUS authentication method and two backup methods (local authentication and no authentication). The device performs RADIUS authentication by default and performs local authentication when the RADIUS server is invalid. The device does not perform authentication when both of the previous methods are invalid.

Examples

In ISP domain **test**, use RADIUS scheme **rd** as the primary default authentication method and use local authentication as the backup.

```
<Switch> system-view
[Switch] domain test
[Switch-isp-test] authentication default radius-scheme rd local
```

Related commands

local-user

radius scheme

1.1.8. authentication lan-access

Use **authentication lan-access** to specify authentication methods for LAN users.

Use **undo authentication lan-access** to restore the default.

Syntax

authentication lan-access { **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo authentication lan-access

Default

The default authentication methods of the ISP domain are used for LAN users.

Views

ISP domain view

Predefined user roles

network-admin

Parameters

local: Performs local authentication.

none: Does not perform authentication.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

You can specify one primary authentication method and multiple backup authentication methods.

When the primary method is invalid, the device attempts to use the backup methods in sequence. For example, the **authentication lan-access radius-scheme** *radius-scheme-name* **local none** command specifies a primary RADIUS authentication method and two backup methods (local authentication and no authentication). The device performs RADIUS authentication by default and performs local authentication when the RADIUS server is invalid. The device does not perform authentication when both of the previous methods are invalid.

Examples

In ISP domain **test**, perform local authentication for LAN users.

```
<Switch> system-view
[Switch] domain test
[Switch-isp-test] authentication lan-access local
```

In ISP domain **test**, perform RADIUS authentication for LAN users based on scheme **rd** and use local authentication as the backup.

```
<Switch> system-view
[Switch] domain test
[Switch-isp-test] authentication lan-access radius-scheme rd local
```

Related commands

authentication default

local-user

radius scheme

1.1.9. authentication login

Use **authentication login** to specify authentication methods for login users.

Use **undo authentication login** to restore the default.

Syntax

authentication login { **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo authentication login

Default

The default authentication methods of the ISP domain are used for login users.

Views

ISP domain view

Predefined user roles

network-admin

Parameters

local: Performs local authentication.

none: Does not perform authentication.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

You can specify one primary authentication method and multiple backup authentication methods.

When the primary method is invalid, the device attempts to use the backup methods in sequence. For example, the **authentication login radius-scheme** *radius-scheme-name* **local none** command specifies the default primary RADIUS authentication method and two backup methods (local authentication and no authentication). The device performs RADIUS authentication by default and performs local authentication when the RADIUS server is invalid. The device does not perform authentication when both of the previous methods are invalid.

Examples

In ISP domain **test**, perform local authentication for login users.

```
<Switch> system-view
[Switch] domain test
[Switch-isp-test] authentication login local
```

In ISP domain **test**, perform RADIUS authentication for login users based on scheme **rd** and use local authentication as the backup.

```
<Switch> system-view
[Switch] domain test
[Switch-isp-test] authentication login radius-scheme rd local
```

Related commands

authentication default

local-user

radius scheme

1.1.10. authorization command

Use **authorization command** to specify command authorization methods.

Use **undo authorization command** to restore the default.

Syntax

authorization command { **local** [**none**] | **none** }

undo authorization command

Default

The default authorization methods of the ISP domain are used for command authorization.

Views

ISP domain view

Predefined user roles

network-admin

Parameters

local: Performs local authorization.

none: Does not perform authorization. The authorization server does not verify whether the entered commands are permitted by the user role. The commands are executed successfully if the user role has permission to the commands.

Usage guidelines

Command authorization restricts login users to execute only authorized commands by employing an authorization server to verify whether each entered command is permitted.

When local command authorization is configured, the device compares each entered command with the user's configuration on the device. The command is executed only when it is permitted by the user's authorized user roles.

The commands that can be executed are controlled by both the access permission of user roles and command authorization of the authorization server. Access permission only controls whether the authorized user roles have access to the entered commands, but it does not control whether the user roles have obtained authorization to these commands. If a command is permitted by the access permission but denied by command authorization, this command cannot be executed.

You can specify one primary command authorization method and multiple backup command authorization methods.

When the default authorization method is invalid, the device attempts to use the backup authorization methods in sequence.

For example, the **authorization command local none** command specifies the default local authorization method and two backup methods (local authorization and no authorization). The device performs local authorization by default and performs no authorization when the local server is invalid.

Examples

In ISP domain **test**, configure the device to perform local command authorization.

```
<Switch> system-view
[Switch] domain test
[Switch-isp-test] authorization command local
```

Related commands

command authorization (*Fundamentals Command Reference*)

local-user

1.1.11. authorization default

Use **authorization default** to specify default authorization methods for an ISP domain.

Use **undo authorization default** to restore the default.

Syntax

authorization default { **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo authorization default

Default

The default authorization method of an ISP domain is local.

Views

ISP domain view

Predefined user roles

network-admin

Parameters

local: Performs local authorization.

none: Does not perform authorization. The following default authorization information applies after users pass authentication:

- Login users obtain the level-0 user role. Login users include the Telnet, FTP, SFTP, SCP, and terminal users. Terminal users can access the device through the console port. For more information about the level-0 user role, see RBAC configuration in *Fundamentals Configuration Guide*.
- The working directory for FTP, SFTP, and SCP login users is the root directory of the NAS. However, the users do not have permission to access the root directory.
- Non-login users can access the network.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

The default authorization method is used for all users that support this method and do not have an authorization method configured.

The RADIUS authorization configuration takes effect only when the authentication method and authorization method of the ISP domain use the same RADIUS scheme.

You can specify one primary authorization method and multiple backup authorization methods.

When the default authorization method is invalid, the device attempts to use the backup authorization methods in sequence. For example, the **authorization default radius-scheme** *radius-scheme-name* **local none** command specifies the default RADIUS authorization method and two backup methods (local authorization and no authorization). The device performs RADIUS authorization by default and performs local authorization when the RADIUS server is invalid. The device does not perform authorization when both of the previous methods are invalid.

Examples

In ISP domain **test**, use RADIUS scheme **rd** as the primary default authorization method and use local authorization as the backup.

```
<Switch> system-view
[Switch] domain test
[Switch-isp-test] authorization default radius-scheme rd local
```

Related commands

local-user

radius scheme

1.1.12. authorization lan-access

Use **authorization lan-access** to specify authorization methods for LAN users.

Use **undo authorization lan-access** to restore the default.

Syntax

authorization lan-access { **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo authorization lan-access

Default

The default authorization methods of the ISP domain are used for LAN users.

Views

ISP domain view

Predefined user roles

network-admin

Parameters

local: Performs local authorization.

none: Does not perform authorization. An authenticated LAN user directly accesses the network.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

The RADIUS authorization configuration takes effect only when authentication and authorization methods of the ISP domain use the same RADIUS scheme.

You can specify one primary authorization method and multiple backup authorization methods.

When the primary method is invalid, the device attempts to use the backup methods in sequence. For example, the **authorization lan-access radius-scheme** *radius-scheme-name* **local none** command specifies a primary RADIUS authorization method and two backup methods

(local authorization and no authorization). The device performs RADIUS authorization by default and performs local authorization when the RADIUS server is invalid. The device does not perform authorization when both of the previous methods are invalid.

Examples

In ISP domain **test**, perform local authorization for LAN users.

```
<Switch> system-view
[Switch] domain test
[Switch-isp-test] authorization lan-access local
```

In ISP domain **test**, perform RADIUS authorization for LAN users based on scheme **rd** and use local authorization as the backup.

```
<Switch> system-view
[Switch] domain test
[Switch-isp-test] authorization lan-access radius-scheme rd local
```

Related commands

authorization default

local-user

radius scheme

1.1.13. authorization login

Use **authorization login** to specify authorization methods for login users.

Use **undo authorization login** to restore the default.

Syntax

authorization login { **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo authorization login

Default

The default authorization methods of the ISP domain are used for login users.

Views

ISP domain view

Predefined user roles

network-admin

Parameters

local: Performs local authorization.

none: Does not perform authorization. The following default authorization information applies after users pass authentication:

- Login users obtain the level-0 user role. Login users include the Telnet, FTP, SFTP, SCP, and terminal users. Terminal users can access the device through the console port. For more information about the level-0 user role, see RBAC configuration in *Fundamentals Configuration Guide*.
- The working directory for FTP, SFTP, and SCP login users is the root directory of the NAS. However, the users do not have permission to access the root directory.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

The RADIUS authorization configuration takes effect only when the authentication method and authorization method of the ISP domain use the same RADIUS scheme.

You can specify one primary authorization method and multiple backup authorization methods.

When the default authorization method is invalid, the device attempts to use the backup authorization methods in sequence. For example, the **authorization login radius-scheme** *radius-scheme-name* **local none** command specifies the default RADIUS authorization method and two backup methods (local authorization and no authorization). The device performs RADIUS authorization by default and performs local authorization when the RADIUS server is invalid. The device does not perform authorization when both of the previous methods are invalid.

Examples

In ISP domain **test**, perform local authorization for login users.

```
<Switch> system-view
[Switch] domain test
[Switch-isp-test] authorization login local
```

In ISP domain **test**, perform RADIUS authorization for login users based on scheme **rd** and use local authorization as the backup.

```
<Switch> system-view
[Switch] domain test
[Switch-isp-test] authorization login radius-scheme rd local
```

Related commands

authorization default

local-user

radius scheme

1.1.14. display domain

Use **display domain** to display ISP domain configuration.

Syntax

display domain [*isp-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

isp-name: Specifies an ISP domain by its name, a case-insensitive string of 1 to 255 characters. If you do not specify an ISP domain, this command displays the configuration of all ISP domains.

Examples

Display the configuration of all ISP domains.

```
<Switch> display domain
```

```
Total 2 domains

Domain: system
  State: Active
  Default authentication scheme:  Local
  Default authorization  scheme:  Local
  Default accounting     scheme:  Local
  Accounting start failure action: Online
  Accounting update failure action: Online
  Accounting quota out policy: Offline
  Service type: HSI
  Session time: Exclude idle time
  Dual-stack accounting method: Merge
  Authorization attributes:
    Idle cut: Disabled
    IGMP access number: 4
    MLD access number:  4

Domain: dm
  State: Active
  Login   authentication scheme:  RADIUS=rad
  Login   authorization  scheme:  HWTACACS=hw
  Super   authentication scheme:  RADIUS=rad
  Command authorization  scheme:  HWTACACS=hw
  LAN access authentication scheme:  RADIUS=r4
  Portal  authentication scheme:  LDAP=ldp
  Default authentication scheme:  RADIUS=rad, Local, None
  Default authorization  scheme:  Local
  Default accounting     scheme:  None
  Accounting start failure action: Online
  Accounting update failure action: Online
  Accounting quota out policy: Offline
  Service type: HSI
  Session time: Include idle time
  Dual-stack accounting method: Merge
  Authorization attributes:
    Idle cut : Disabled
    IP pool: appy
    User profile: test
    Inbound CAR: CIR 64000 bps PIR 640000 bps
    Outbound CAR: CIR 64000 bps PIR 640000 bps
    ACL number: 3000
    User group: ugg
    IPv6 pool: ipv6pool
    URL: http://test
    IGMP access number: 4
    MLD access number: 4
```

```
Default domain name: system
```

Table 1-1 Command output

Field	Description
Domain	ISP domain name.
State	Status of the ISP domain.
Default authentication scheme	Default authentication methods.
Default authorization scheme	Default authorization methods.
Default accounting scheme	Default accounting methods.
Login authentication scheme	Authentication methods for login users.
Login authorization scheme	Authorization methods for login users.
Login accounting scheme	Accounting methods for login users.
Super authentication scheme	Authentication methods for obtaining another user role without reconnecting to the device.
Command authorization scheme	Command line authorization methods.
Command accounting scheme	Command line accounting method.
LAN access authentication scheme	Authentication methods for LAN users.
LAN access authorization scheme	Authorization methods for LAN users.
LAN access accounting scheme	Accounting methods for LAN users.
Portal authentication scheme	Authentication methods for portal users.
Portal authorization scheme	Authorization methods for portal users.
Portal accounting scheme	Accounting methods for portal users.
RADIUS	RADIUS scheme.
HWTACACS	HWTACACS scheme.
LDAP	LDAP scheme.
Local	Local scheme.
None	No authentication, no authorization, or no accounting.
Accounting start failure action	Access control for users that encounter accounting-start failures: • **Online**—Allows the users to stay online. • **Offline**—Logs off the users.
Accounting update failure max-times	Maximum number of consecutive accounting-update failures allowed by the device for each user in the domain.
Accounting update failure action	Access control for users that have failed all their accounting-update attempts: • **Online**—Allows the users to stay online. • **Offline**—Logs off the users.
Accounting quota out policy	Access control for users that have used up their data quotas: • **Online**—Allows the users to stay online. • **Offline**—Logs off the users.

Field	Description
Service type	This field is not supported in the current software version. Service type of the ISP domain, including HSI, STB, and VoIP.
Session time	Online duration sent to the server for users that went offline due to connection failure or malfunction: • **Include idle time**—The online duration includes the idle timeout period. • **Exclude idle time**—The online duration does not include the idle timeout period.
Dual-stack accounting method	This field is not supported in the current software version. Accounting method for dual-stack users: • **Merge**—Merges IPv4 data with IPv6 data for accounting. • **Separate**—Separates IPv4 data from IPv6 data for accounting.
Authorization attributes	Authorization attributes for users in the ISP domain.
Idle cut	This field is not supported in the current software version. Idle cut feature status: • **Enabled**—The feature is enabled. The device logs off users that do not meet the minimum traffic requirements in an idle timeout period. • **Disabled**—The feature is disabled. It is the default idle cut state.
IP pool	Name of the authorization IPv4 address pool.
User profile	Name of the authorization user profile.
Inbound CAR	Authorization inbound CAR: • **CIR**—Committed information rate in bps. • **PIR**—Peak information rate in bps. If no inbound CAR is authorized, this field displays **N/A**.
Outbound CAR	Authorization outbound CAR: • **CIR**—Committed information rate in bps. • **PIR**—Peak information rate in bps. If no outbound CAR is authorized, this field displays **N/A**.
ACL number	Authorization ACL for users.
User group	Authorization user group for users.
IPv6 pool	Name of the authorization IPv6 address pool for users.
URL	Authorization redirect URL for users.
IGMP max access number	Maximum number of IGMP groups that an IPv4 user is authorized to join concurrently.
MLD max access number	Maximum number of MLD groups that an IPv6 user is authorized to join concurrently.

1.1.15. domain

Use **domain** to create an ISP domain and enter its view, or enter the view of an existing ISP domain.

Use **undo domain** to delete an ISP domain.

Syntax

domain *isp-name*

undo domain *isp-name*

Default

A system-defined ISP domain exists. The domain name is **system**.

Views

System view

Predefined user roles

network-admin

Parameters

isp-name: Specifies the ISP domain name, a case-insensitive string of 1 to 255 characters. The name must meet the following requirements:

- The name cannot contain a forward slash (/), backslash (\), vertical bar (|), quotation marks ("), colon (:), asterisk (*), question mark (?), left angle bracket (<), right angle bracket (>), or at sign (@).
- The name cannot be **d**, **de**, **def**, **defa**, **defau**, **defaul**, **default**, **i**, **if**, **if-**, **if-u**, **if-un**, **if-unk**, **if-unkn**, **if-unkno**, **if-unknow**, or **if-unknown**.

Usage guidelines

All ISP domains are in active state when they are created.

You can modify settings for the system-defined ISP domain **system**, but you cannot delete this domain.

An ISP domain cannot be deleted when it is the default ISP domain. Before you use the **undo domain** command, change the domain to a non-default ISP domain by using the **undo domain default enable** command.

Use short domain names to ensure that user names containing a domain name do not exceed the maximum name length required by different types of users.

Examples

Create an ISP domain named **test** and enter ISP domain view.

```
<Switch> system-view
[Switch] domain test
[Switch-isp-test]
```

Related commands

display domain

domain default enable

state (ISP domain view)

1.1.16. domain default enable

Use **domain default enable** to specify the default ISP domain. Users without any domain name included in the usernames are considered in the default domain.

Use **undo domain default enable** to restore the default.

Syntax

domain default enable *isp-name*

undo domain default enable

Default

The default ISP domain is the system-defined ISP domain **system**.

Views

System view

Predefined user roles

network-admin

Parameters

isp-name: Specifies the ISP domain name, a case-insensitive string of 1 to 255 characters. The ISP domain must already exist.

Usage guidelines

The system has only one default ISP domain.

An ISP domain cannot be deleted when it is the default ISP domain. Before you use the **undo domain** command, change the domain to a non-default ISP domain by using the **undo domain default enable** command.

Examples

Create an ISP domain named **test**, and configure the domain as the default ISP domain.

```
<Switch> system-view
[Switch] domain test
[Switch-isp-test] quit
[Switch] domain default enable test
```

Related commands

display domain

domain

1.1.17. state (ISP domain view)

Use **state** to set the status of an ISP domain.

Use **undo state** to restore the default.

Syntax

state { **active** | **block** }

undo state

Default

An ISP domain is in active state.

Views

ISP domain view

Predefined user roles

network-admin

Parameters

active: Places the ISP domain in active state to allow the users in the ISP domain to request network services.

block: Places the ISP domain in blocked state to prevent users in the ISP domain from requesting network services.

Usage guidelines

By blocking an ISP domain, you disable offline users of the domain from requesting network services. However, the online users are not affected.

Examples

Place ISP domain **test** in blocked state.

```
<Switch> system-view
[Switch] domain test
[Switch-isp-test] state block
```

Related commands

display domain

1.2. Local user commands

1.2.1. access-limit

Use **access-limit** to set the maximum number of concurrent logins using the local user name.

Use **undo access-limit** to restore the default.

Syntax

access-limit *max-user-number*

undo access-limit

Default

The number of concurrent logins using the local user name is not limited.

Views

Local user view

Predefined user roles

network-admin

Parameters

max-user-number: Specifies the maximum number of concurrent logins, in the range of 1 to 1024.

Usage guidelines

This command takes effect only when local accounting is configured for the local user. The command does not apply to FTP, SFTP, or SCP users. These users do not support accounting.

Examples

Set the maximum number of concurrent logins to 5 for users using the local user name **abc**.

```
<Switch> system-view
[Switch] local-user abc
[Switch-luser-manage-abc] access-limit 5
```

Related commands

display local-user

1.2.2. authorization-attribute (local user view/user group view)

Use **authorization-attribute** to configure authorization attributes for a local user or user group. After the local user or a local user in the user group passes authentication, the device assigns these attributes to the user.

Use **undo authorization-attribute** to restore the default of an authorization attribute.

Syntax

authorization-attribute { **acl** *acl-number* | **idle-cut** *minutes* | **user-role** *role-name* | **vlan** *vlan-id* | **work-directory** *directory-name* } *

undo authorization-attribute { **acl** | **idle-cut** | **user-role** *role-name* | **vlan** | **work-directory** } *

Default

The working directory for FTP, SFTP, and SCP users is the root directory of the NAS. However, the users do not have permission to access the root directory.

The local users created by a network-admin or level-15 user are assigned the network-operator user role.

Views

Local user view

User group view

Predefined user roles

network-admin

Parameters

acl *acl-number*: Specifies an authorization ACL. The value range for the *acl-number* argument is 2000 to 4999. After passing authentication, a local user can access the network resources specified by this ACL.

idle-cut *minutes*: Specifies an idle timeout period in minutes. The value range for the *minutes* argument is 1 to 120. An online user is logged out if its idle period exceeds the specified idle timeout period.

user-role *role-name*: Specifies an authorized user role. The *role-name* argument is a case-sensitive string of 1 to 63 characters. A maximum of 64 user roles can be specified for a user.

For user role-related commands, see *Fundamentals Command Reference* for RBAC commands. This option is available only in local user view, and is not available in user group view.

vlan *vlan-id*: Specifies an authorized VLAN. The value range for the *vlan-id* argument is 1 to 4094. After passing authentication and being authorized a VLAN, a local user can access only the resources in this VLAN.

work-directory *directory-name*: Specifies the working directory for FTP, SFTP, or SCP users. The *directory-name* argument is a case-insensitive string of 1 to 255 characters. The directory must already exist.

Usage guidelines

Configure authorization attributes according to the application environments and purposes. Support for authorization attributes depends on the service types of users.

For LAN users, only the following authorization attributes take effect: **acl**, and **vlan**.

For SSH, Telnet, and terminal users, only authorization attributes **idle-cut** and **user-role** take effect.

For HTTP and HTTPS users, only authorization attribute **user-role** takes effect.

For FTP users, only authorization attributes **user-role** and **work-directory** take effect.

For other types of local users, no authorization attribute takes effect.

Authorization attributes configured for a user group are intended for all local users in the group. You can group local users to improve configuration and management efficiency. An authorization attribute configured in local user view takes precedence over the same attribute configured in user group view.

To make sure FTP, SFTP, and SCP users can access the directory after an IRF master/subordinate switchover, do not specify slot information for the working directory.

To make sure the user have only the user roles authorized by using this command, use the **undo authorization-attribute user-role** command to remove the default user role.

Examples

Configure the authorized VLAN of network access user **abc** as VLAN 2.

```
<Switch> system-view
[Switch] local-user abc class network
[Switch-luser-network-abc] authorization-attribute vlan 2
```

Configure the authorized VLAN of user group **abc** as VLAN 3.

```
<Switch> system-view
[Switch] user-group abc
[Switch-ugroup-abc] authorization-attribute vlan 3
```

Related commands

display local-user

display user-group

1.2.3. bind-attribute

Use **bind-attribute** to configure binding attributes for a local user.

Use **undo bind-attribute** to remove binding attributes of a local user.

Syntax

bind-attribute { **ip** *ip-address* | **location interface** *interface-type interface-number* | **mac** *mac-address* | **vlan** *vlan-id* } *

undo bind-attribute { **ip** | **location** | **mac** | **vlan** } *

Default

No binding attributes are configured for a local user.

Views

Local user view

Predefined user roles

network-admin

Parameters

ip *ip-address*: Specifies the IP address to which the user is bound. This option applies only to 802.1X users.

location interface *interface-type interface-number*: Specifies the interface to which the user is bound. The *interface-type* argument represents the interface type, and the *interface-number* argument represents the interface number. To pass authentication, the user must access the network through the bound interface. This option applies only to LAN users.

mac *mac-address*: Specifies the MAC address of the user in the format H-H-H. This option applies only to LAN users.

vlan *vlan-id*: Specifies the VLAN to which the user belongs. The *vlan-id* argument is in the range of 1 to 4094. This option applies only to LAN users.

Usage guidelines

To perform local authentication of a user, the device matches the actual user attributes with the configured binding attributes. If the user has a non-matching attribute or lacks a required attribute, the user will fail authentication.

Binding attribute check takes effect on all access services. Configure the binding attributes for a user based on the access services and make sure the device can obtain all attributes to be checked from the user's packet. For example, you can configure an IP address binding for an 802.1X user, because 802.1X authentication can include the user's IP address in the packet. However, you cannot configure IP address bindings for MAC authentication users, because MAC authentication does not use IP addresses.

The binding interface type must meet the requirements of the local user. Configure the binding interface based on the service type of the user.

- If the user is an 802.1X user, specify the 802.1X-enabled Layer 2 Ethernet interface or Layer 2 aggregate interface.
- If the user is a MAC authentication user, specify the MAC authentication-enabled Layer 2 Ethernet interface or Layer 2 aggregate interface.
- If the user is a Web authentication user, specify the Web authentication-enabled Layer 2 Ethernet interface.

Examples

Bind MAC address 11-11-11 with network access user **abc**.

```
<Switch> system-view
[Switch] local-user abc class network
[Switch-luser-network-abc] bind-attribute mac 11-11-11
```

Related commands

display local-user

1.2.4. display local-user

Use **display local-user** to display the local user configuration and online user statistics.

Syntax

display local-user [**class** { **manage** | **network** } | **idle-cut** { **disable** | **enable** } | **service-type** { **ftp** | **lan-access** | **ssh** | **telnet** | **terminal** } | **state** { **active** | **block** } | **user-name** *user-name* **class** { **manage** | **network** } | **vlan** *vlan-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

class: Specifies the local user type.

manage: Device management user.

network: Network access user.

idle-cut { **disable** | **enable** }: Specifies local users by the status of the idle cut feature.

service-type: Specifies the local users that use a specific type of service.

ftp: FTP users.

lan-access: LAN users that typically access the network through an Ethernet, such as 802.1X users.

ssh: SSH users.

telnet: Telnet users.

terminal: Terminal users that log in through console ports.

state { **active** | **block** }: Specifies local users in active or blocked state. A local user in active state can access network services, but a local user in blocked state cannot.

user-name *user-name*: Specifies all local users using the specified username. The username must be a case-sensitive string of 1 to 55 characters. The name must meet the following requirements:

- Cannot contain the domain name.
- Cannot contain any of the following characters: forward slash (/), backslash (\), vertical bar (|), colon (:), asterisk (*), question mark (?), left angle bracket (<), right angle bracket (>), and at sign (@).
- Cannot be **a**, **al**, or **all**.

vlan *vlan-id*: Specifies all local users in a VLAN. The *vlan-id* argument is in the range of 1 to 4094.

Usage guidelines

If you do not specify any parameters, this command displays information about all local users.

Examples

Display information about all local users.

```
<Switch> display local-user
Device management user root:
  State:                     Active
  Service type:              SSH/Telnet/Terminal
  Access limit:              Enabled          Max access number: 3
  Current access number:     1
  User group:                system
  Bind attributes:
  Authorization attributes:
    Work directory:          flash:
    User role list:          network-admin
  Password control configurations:
    Password aging:          3 days

Network access user jj:
  State:                      Active
  Service type:               LAN-access
  User group:                 system
  Bind attributes:
    IP address:               2.2.2.2
    Location bound:           GigabitEthernet1/0/1
    MAC address:              0001-0001-0001
    VLAN ID:                  2
  Authorization attributes:
    Idle timeout:             33 minutes
    Work directory:           flash:
    ACL number:               2000
  User profile:               pp
  User role list:             network-operator, level-0, level-3
  Description:                A network access user from company cc
  Validity period:
    Start date and time:      2016/01/01-00:01:01
    Expiration date and time: 2017/01/01-01:01:01

Total 2 local users matched.
```

Table 1-2 Command output

Field	Description
State	Status of the local user: active or blocked.
Service type	Service types that the local user can use.
Access limit	Whether the concurrent login limit is enabled.
Max access number	Maximum number of concurrent logins using the local user name.
Current access number	Current number of concurrent logins using the local user name.
User group	Group to which the local user belongs.

Field	Description
Bind attributes	Binding attributes of the local user.
IP address	IP address of the local user.
Location bound	Binding port of the local user.
MAC address	MAC address of the local user.
VLAN ID	Binding VLAN of the local user.
Authorization attributes	Authorization attributes of the local user.
Idle timeout	Idle timeout period of the user, in minutes.
Session-timeout	Session timeout timer for the user, in minutes.
Work directory	Directory that the FTP, SFTP, or SCP user can access.
ACL number	Authorization ACL of the local user.
VLAN ID	Authorized VLAN of the local user.
User profile	Authorization user profile of the local user.
User role list	Authorized roles of the local user.
IP pool	IPv4 address pool authorized to the local user.
IPv6 pool	IPv6 address pool authorized to the local user.
Password control configurations	Password control attributes that are configured for the local user.
Password aging	Password expiration time.
Password length	Minimum number of characters that a password must contain.
Password composition	Password composition policy: • Minimum number of character types that a password must contain. • Minimum number of characters from each type in a password.
Password complexity	Password complexity checking policy: • Reject a password that contains the username or the reverse of the username. • Reject a password that contains any character repeated consecutively three or more times.
Maximum login attempts	Maximum number of consecutive failed login attempts.
Action for exceeding login attempts	Action to take on the user that failed to log in after using up all login attempts.
Description	Description of the network access user.
Validity period	Validity period of the network access user.
Start date and time	Date and time from which the network access user begins to take effect.
Expiration date and time	Date and time at which the network access user expires.

1.2.5. display user-group

Use **display user-group** to display user group configuration.

Syntax

display user-group { **all** | **name** *group-name* }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

all: Specifies all user groups.

name *group-name*: Specifies a user group by its name, a case-insensitive string of 1 to 32 characters.

Examples

Display the configuration of all user groups.

```
<Switch> display user-group all
Total 2 user groups matched.

User group: system
  Authorization attributes:
    Work directory:          flash:
User group: jj
  Authorization attributes:
    Idle timeout:            2 minutes
    Work directory:          flash:/
    ACL number:              2000
    VLAN ID:                 2
    User profile:            pp
  Password control configurations:
    Password aging:          2 days
```

Table 1-3 Command output

Field	Description
User group	User group name.
Authorization attributes	Authorization attributes of the user group.
Idle timeout	Idle timeout period, in minutes.
Session-timeout	Session timeout timer, in minutes.
Work directory	Directory that FTP, SFTP, or SCP users in the group can access.
ACL number	Authorization ACL.
VLAN ID	Authorized VLAN.

Field	Description
User profile	Authorization user profile.
IP pool	IPv4 address pool authorized to the user group.
IPv6 pool	IPv6 address pool authorized to the user group.
Password control configurations	Password control attributes that are configured for the user group.
Password aging	Password expiration time.
Password length	Minimum number of characters that a password must contain.
Password composition	Password composition policy: • Minimum number of character types that a password must contain. • Minimum number of characters from each type in a password.
Password complexity	Password complexity checking policy: • Reject a password that contains the username or the reverse of the username. • Reject a password that contains any character repeated consecutively three or more times.
Maximum login attempts	Maximum number of consecutive failed login attempts.
Action for exceeding login attempts	Action to take on the user that failed to log in after using up all login attempts.

1.2.6. group

Use **group** to assign a local user to a user group.

Use **undo group** to restore the default.

Syntax

group *group-name*

undo group

Default

A local user belongs to user group **system**.

Views

Local user view

Predefined user roles

network-admin

Parameters

group-name: Specifies the user group name, a case-insensitive string of 1 to 32 characters.

Examples

Assign device management user **111** to user group **abc**.

```
<Switch> system-view
[Switch] local-user 111 class manage
```

```
[Switch-luser-manage-111] group abc
```

Related commands

display local-user

1.2.7. local-user

Use **local-user** to add a local user and enter its view, or enter the view of an existing local user.

Use **undo local-user** to delete local users.

Syntax

local-user *user-name* [**class** { **manage** | **network** }]

undo local-user { *user-name* **class** { **manage** | **network** } | **all** [**service-type** { **ftp** | **lan-access** | **ssh** | **telnet** | **terminal** } | **class** { **manage** | **network** }] }

Default

No local users exist.

Views

System view

Predefined user roles

network-admin

Parameters

user-name: Specifies the local user name, a case-sensitive string of 1 to 55 characters. The name must meet the following requirements:

- Cannot contain a domain name.
- Cannot contain any of the following characters: forward slash (/), backslash (\), vertical bar (|), colon (:), asterisk (*), question mark (?), left angle bracket (<), right angle bracket (>), and at sign (@).
- Cannot be **a**, **al**, or **all**.

class: Specifies the local user type. If you do not specify this keyword, the command adds a device management user.

manage: Device management user that can configure and monitor the device after login. Device management users can use FTP, HTTP, HTTPS, Telnet, SSH, and terminal services.

network: Network access user that accesses network resources through the device. Network access users can use LAN access services.

all: Specifies all users.

service-type: Specifies the local users that use a specific type of service.

ftp: FTP users.

lan-access: LAN users that typically access the network through an Ethernet, such as 802.1X users.

ssh: SSH users.

telnet: Telnet users.

terminal: Terminal users that log in through console ports.

Examples

Add a device management user named **user1** and enter local user view.

```
<Switch> system-view
[Switch] local-user user1 class manage
[Switch-luser-manage-user1]
```

Add a network access user named **user2** and enter local user view.

```
<Switch> system-view
[Switch] local-user user2 class network
[Switch-luser-network-user2]
```

Related commands

display local-user

service-type

1.2.8. password (device management user view)

Use **password** to configure a password for a device management user.

Use **undo password** to restore the default.

Syntax

password [{ **hash** | **simple** } *string*]

undo password

Default

A device management user does not have a password and can pass authentication after entering the correct username and passing attribute checks.

Views

Device management user view

Predefined user roles

network-admin

Parameters

hash: Specifies a password encrypted by the hash algorithm.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password string. This argument is case sensitive. The hashed form of the password is a string of 1 to 110 characters. The plaintext form of the password is a string of 1 to 63 characters.

Usage guidelines

If you do not specify any parameters, you enter the interactive mode to set a plaintext password.

A device management user for which no password is specified can pass authentication after entering the correct username and passing attribute checks. To enhance security, configure a password for each device management user.

Examples

Set the password to **123456TESTplat&!** in plaintext form for device management user **user1**.

```
<Switch> system-view
```

```
[Switch] local-user user1 class manage
[Switch-luser-manage-user1] password simple 123456TESTplat&!
```

Configure the password in interactive mode for device management user **test**.

```
<Switch> system-view
[Switch] local-user test class manage
[Switch-luser-manage-test] password
Password:
confirm :
```

Related commands

display local-user

1.2.9. password (network access user view)

Use **password** to configure a password for a network access user.

Use **undo password** to restore the default.

Syntax

password { **cipher** | **simple** } *string*

undo password

Default

A network access user does not have a password and can pass authentication after entering the correct username and passing attribute checks.

Views

Network access user view

Predefined user roles

network-admin

Parameters

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password string. Its plaintext form is a case-sensitive string of 1 to 63 characters. Its encrypted form is a case-sensitive string of 1 to 117 characters.

Usage guidelines

As a best practice to enhance security, configure a password for each network access user.

Examples

Set the password to **123456TESTuser&!** in plaintext form for network access user **user1**.

```
<Switch> system-view
[Switch] local-user user1 class network
[Switch-luser-network-user1] password simple 123456TESTuser&!
```

Related commands

display local-user

1.2.10. service-type

Use **service-type** to specify the service types that a local user can use.

Use **undo service-type** to remove service types configured for a local user.

Syntax

service-type { **ftp** | **lan-access** | { **ssh** | **telnet** | **terminal** } * }

undo service-type { **ftp** | **lan-access** | { **ssh** | **telnet** | **terminal** } * }

Default

A local user is not authorized to use any service.

Views

Local user view

Predefined user roles

network-admin

Parameters

ftp: Authorizes the user to use the FTP service. The authorized directory can be modified by using the **authorization-attribute work-directory** command.

lan-access: Authorizes the user to use the LAN access service. The users are typically Ethernet users, for example, 802.1X users.

ssh: Authorizes the user to use the SSH service.

telnet: Authorizes the user to use the Telnet service.

terminal: Authorizes the user to use the terminal service and log in from a console port.

Usage guidelines

You can assign multiple service types to a user.

Examples

Authorize device management user **user1** to use the Telnet and FTP services.

```
<Switch> system-view
[Switch] local-user user1 class manage
[Switch-luser-manage-user1] service-type telnet
[Switch-luser-manage-user1] service-type ftp
```

Related commands

display local-user

1.2.11. state (local user view)

Use **state** to set the status of a local user.

Use **undo state** to restore the default.

Syntax

state { **active** | **block** }

undo state

Default

A local user is in active state.

Views

Local user view

Predefined user roles

network-admin

Parameters

active: Places the local user in active state to allow the local user to request network services.

block: Places the local user in blocked state to prevent the local user from requesting network services.

Examples

Place device management user **user1** in blocked state.

```
<Switch> system-view
[Switch] local-user user1 class manage
[Switch-luser-manage-user1] state block
```

Related commands

display local-user

1.2.12. user-group

Use **user-group** to create a user group and enter its view, or enter the view of an existing user group.

Use **undo user-group** to delete a user group.

Syntax

user-group *group-name*

undo user-group *group-name*

Default

A system-defined user group exists. The group name is **system**.

Views

System view

Predefined user roles

network-admin

Parameters

group-name: Specifies the user group name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

A user group consists of a group of local users and has a set of local user attributes. You can configure local user attributes for a user group to implement centralized management of user attributes for the local users in the group.

A user group that has local users cannot be deleted.

You can modify settings for the system-defined user group named **system**, but you cannot delete the user group.

Examples

Create a user group named **abc** and enter user group view.

```
<Switch> system-view
[Switch] user-group abc
[Switch-ugroup-abc]
```

Related commands

display user-group

1.3. RADIUS commands

1.3.1. accounting-on enable

Use **accounting-on enable** to configure the accounting-on feature.

Use **undo accounting-on enable** to disable the accounting-on feature.

Syntax

accounting-on enable [**interval** *interval* | **send** *send-times*] *

undo accounting-on enable

Default

The accounting-on feature is disabled.

Views

RADIUS scheme view

Predefined user roles

network-admin

Parameters

interval *interval*: Specifies the time interval for retransmitting an accounting-on packet in seconds. The value range for the *interval* argument is 1 to 15, and the default setting is 3.

send *send-times*: Specifies the maximum number of accounting-on packet transmission attempts. The value range for the *send-times* argument is 1 to 255, and the default setting is 50.

Usage guidelines

The accounting-on feature enables the device to automatically send an accounting-on packet to the RADIUS server after a device reboot. Upon receiving the accounting-on packet, the RADIUS server logs out all online users so they can log in again through the device.

Execute the **save** command to ensure that the **accounting-on enable** command takes effect at the next device reboot. For information about the **save** command, see *Fundamentals Command Reference*.

Parameters set by using the **accounting-on enable** command take effect immediately.

Examples

Enable the accounting-on feature for RADIUS scheme **radius1**, and set the retransmission interval to 5 seconds and the transmission attempts to 15.

```
<Switch> system-view
[Switch] radius scheme radius1
[Switch-radius-radius1] accounting-on enable interval 5 send 15
```

Related commands

display radius scheme

1.3.2. data-flow-format (RADIUS scheme view)

Use **data-flow-format** to set the data flow and packet measurement units for traffic statistics.

Use **undo data-flow-format** to restore the default.

Syntax

data-flow-format { **data** { **byte** | **giga-byte** | **kilo-byte** | **mega-byte** } | **packet** { **giga-packet** | **kilo-packet** | **mega-packet** | **one-packet** } } *

undo data-flow-format { **data** | **packet** }

Default

Traffic is counted in bytes and packets.

Views

RADIUS scheme view

Predefined user roles

network-admin

Parameters

data: Specifies the unit for data flows.

byte: Specifies the unit as byte.

giga-byte: Specifies the unit as gigabyte.

kilo-byte: Specifies the unit as kilobyte.

mega-byte: Specifies the unit as megabyte.

packet: Specifies the unit for data packets.

giga-packet: Specifies the unit as giga-packet.

kilo-packet: Specifies the unit as kilo-packet.

mega-packet: Specifies the unit as mega-packet.

one-packet: Specifies the unit as one-packet.

Usage guidelines

The data flow and packet measurement units for traffic statistics must be the same as configured on the RADIUS accounting servers. Otherwise, accounting results might be incorrect.

Examples

In RADIUS scheme **radius1**, set the data flow and packet measurement units for traffic statistics to kilobyte and kilo-packet, respectively.

```
<Switch> system-view
[Switch] radius scheme radius1
[Switch-radius-radius1] data-flow-format data kilo-byte packet kilo-packet
```

Related commands

display radius scheme

1.3.3. display radius scheme

Use **display radius scheme** to display RADIUS scheme configuration.

Syntax

display radius scheme [*radius-scheme-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

radius-scheme-name: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters. If you do not specify a RADIUS scheme, this command displays the configuration of all RADIUS schemes.

Examples

Display the configuration of all RADIUS schemes.

```
<Switch> display radius scheme
Total 1 RADIUS schemes

------------------------------------------------------------------
RADIUS scheme name: radius1
  Index : 0
  Primary authentication server:
    Host name: Not configured
    IP   : 2.2.2.2                                Port: 1812
    VPN  : vpn1
    State: Active
    Test profile: 132
      Probe username: test
      Probe interval: 60 minutes
    Weight: 40
  Primary accounting server:
    Host name: Not configured
    IP   : 1.1.1.1                                Port: 1813
    VPN  : Not configured
    State: Active
    Weight: 40
  Second authentication server:
    Host name: Not configured
    IP   : 3.3.3.3                                Port: 1812
    VPN  : Not configured
    State: Block
    Test profile: Not configured
    Weight: 40
```

```
  Second accounting server:
    Host name: Not configured
    IP   : 3.3.3.3                                Port: 1813
    VPN  : Not configured
    State: Block (Mandatory)
    Weight: 0
  Accounting-On function                      : Enabled
    extended function                         : Disabled
    retransmission times                      : 5
    retransmission interval(seconds)          : 2
  Timeout Interval(seconds)                   : 3
  Retransmission Times                        : 3
  Retransmission Times for Accounting Update  : 5
  Server Quiet Period(minutes)                : 5
  Realtime Accounting Interval(seconds)       : 22
  Stop-accounting packets buffering           : Enabled
    Retransmission times                      : 500
  NAS IP Address                              : 1.1.1.1
  VPN                                         : Not configured
  User Name Format                            : with-domain
  Data flow unit                              : Megabyte
  Packet unit                                 : One
  Attribute 15 check-mode                     : Strict
  Attribute 25                                : CAR
  Attribute Remanent-Volume unit              : Mega
  server-load-sharing                         : Enabled
  Attribute 31 MAC format                     : hh:hh:hh:hh:hh:hh
  Stop-accounting-packet send-force           : Disabled
------------------------------------------------------------------
```

Table 1-4 Command output

Field	Description
Index	Index number of the RADIUS scheme.
Primary authentication server	Information about the primary authentication server.
Primary accounting server	Information about the primary accounting server.
Second authentication server	Information about the secondary authentication server.
Second accounting server	Information about the secondary accounting server.
Host name	Host name of the server. This field displays **Not configured** in the following situations: • The server is not configured. • The server is specified by IP address.
IP	IP address of the server. This field displays **Not configured** in the following situations: • The server is not configured.

Field	Description
	• The server is specified by hostname, and the hostname is not resolved.
Port	Service port number of the server. If no port number is specified, this field displays the default port number.
VPN	VPN instance to which the server or the RADIUS scheme belongs. If no VPN instance is specified for the server, this field displays **Not configured**.
State	Status of the server: • **Active**—The server is in active state. • **Block**—The server is changed to blocked state automatically. • **Block (Mandatory)**—The server is set to blocked state manually.
Test profile	Test profile used for RADIUS server status detection.
Probe username	Username used for RADIUS server status detection.
Probe interval	Server status detection interval, in minutes.
Weight	Weight value of the RADIUS server.
Accounting-On function	Whether the accounting-on feature is enabled.
extended function	Whether the extended accounting-on feature is enabled.
retransmission times	Number of accounting-on packet transmission attempts.
retransmission interval(seconds)	Interval at which the device retransmits accounting-on packets, in seconds.
Timeout Interval(seconds)	RADIUS server response timeout period, in seconds.
Retransmission times	Maximum number of attempts for transmitting a RADIUS packet to a single RADIUS server.
Retransmission Times for Accounting Update	Maximum number of accounting attempts.
Server Quiet Period(minutes)	Quiet period for the servers, in minutes.
Realtime Accounting Interval(seconds)	Interval for sending real-time accounting updates, in seconds.
Stop-accounting packets buffering	Whether buffering of nonresponded RADIUS stop-accounting requests is enabled.
Retransmission times	Maximum number of transmission attempts for individual RADIUS stop-accounting requests.
NAS IP Address	Source IP address for outgoing RADIUS packets.
User Name Format	Format for the usernames sent to the RADIUS server: • **with-domain**—Includes the domain name. • **without-domain**—Excludes the domain name. • **keep-original**—Forwards the username as the username is entered.
Data flow unit	Measurement unit for data flow.
Packet unit	Measurement unit for packets.
Attribute 15 check-mode	RADIUS Login-Service attribute check method for SSH, FTP,

Field	Description
	and terminal users: • **Strict**—Matches Login-Service attribute values 50, 51, and 52 for SSH, FTP, and terminal services, respectively. • **Loose**—Matches the standard Login-Service attribute value 0 for SSH, FTP, and terminal services.
Attribute 25	RADIUS attribute 25 interpretation status: • **Standard**—The attribute is not interpreted as CAR parameters. • **CAR**—The attribute is interpreted as CAR parameters.
Attribute Remanent-Volume unit	Data measurement unit for the RADIUS Remanent_Volume attribute.
server-load-sharing	Status of the RADIUS server load sharing feature: • **Disabled**—The feature is disabled. The device forwards traffic to the server selected based on primary and secondary server roles. • **Enabled**—The feature is enabled. The device distributes traffic among multiple servers for load sharing.
Attribute 31 MAC format	MAC address format for RADIUS attribute 31.
Stop-accounting-packet send-force	Whether the device is enabled to forcibly send stop-accounting packets when users for which no start-accounting packets are sent go offline.

1.3.4. display radius statistics

Use **display radius statistics** to display RADIUS packet statistics.

Syntax

display radius statistics

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display RADIUS packet statistics.

```
<Switch> display radius statistics

                          Auth.         Acct.       SessCtrl.
        Request Packet:   0             0           0
          Retry Packet:   0             0           -
        Timeout Packet:   0             0           -
     Access Challenge:    0             -           -
       Account Start:     -             0           -
      Account Update:     -             0           -
        Account Stop:     -             0           -
```

```
      Terminate Request:          -           -           0
             Set Policy:          -           -           0
   Packet With Response:          0           0           0
Packet Without Response:          0           0           -
         Access Rejects:          0           -           -
         Dropped Packet:          0           0           0
         Check Failures:          0           0           0
```

Table 1-5 Command output

Field	Description
Auth.	Authentication packets.
Acct.	Accounting packets.
SessCtrl.	Session-control packets.
Request Packet	Number of request packets.
Retry Packet	Number of retransmitted request packets.
Timeout Packet	Number of request packets timed out.
Access Challenge	Number of access challenge packets.
Account Start	Number of start-accounting packets.
Account Update	Number of accounting update packets.
Account Stop	Number of stop-accounting packets.
Terminate Request	Number of packets for logging off users forcibly.
Set Policy	Number of packets for updating user authorization information.
Packet With Response	Number of packets for which responses were received.
Packet Without Response	Number of packets for which no responses were received.
Access Rejects	Number of Access-Reject packets.
Dropped Packet	Number of discarded packets.
Check Failures	Number of packets with checksum errors.

Related commands

reset radius statistics

1.3.5. display stop-accounting-buffer (for RADIUS)

Use **display stop-accounting-buffer** to display information about buffered RADIUS stop-accounting requests to which no responses have been received.

Syntax

display stop-accounting-buffer { **radius-scheme** *radius-scheme-name* | **session-id** *session-id* | **time-range** *start-time end-time* | **user-name** *user-name* }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

session-id *session-id*: Specifies a session by its ID. The *session-id* argument is a string of 1 to 64 characters and cannot contain a letter. A session ID uniquely identifies an online user for a RADIUS scheme.

time-range *start-time end-time*: Specifies a time range. The start time and end time must be in the format of hh:mm:ss-mm/dd/yyyy or hh:mm:ss-yyyy/mm/dd.

user-name *user-name*: Specifies a user by its name, a case-sensitive string of 1 to 255 characters. Whether the *user-name* argument should include the domain name depends on the setting configured by using the **user-name-format** command for the RADIUS scheme.

Examples

Display information about nonresponded RADIUS stop-accounting requests buffered for user **abc**.

```
<Switch> display stop-accounting-buffer user-name abc
Total entries: 2
Scheme      Session ID          Username    First sending time   Attempts
rad1        1000326232325010    abc         23:27:16-08/31/2015  19
aaa         1000326232326010    abc         23:33:01-08/31/2015  20
```

Table 1-6 Command output

Field	Description
First sending time	Time when the stop-accounting request was first sent.
Attempts	Number of attempts that were made to send the stop-accounting request.

Related commands

reset stop-accounting-buffer (for RADIUS)

retry

retry stop-accounting (RADIUS scheme view)

stop-accounting-buffer enable (RADIUS scheme view)

user-name-format (RADIUS scheme view)

1.3.6. key (RADIUS scheme view)

Use **key** to set the shared key for secure RADIUS authentication or accounting communication.

Use **undo key** to delete the shared key for secure RADIUS authentication or accounting communication.

Syntax

key { **accounting** | **authentication** } { **cipher** | **simple** } *string*

undo key { **accounting** | **authentication** }

Default

No shared key is configured for secure RADIUS authentication or accounting communication.

Views

RADIUS scheme view

Predefined user roles

network-admin

Parameters

accounting: Specifies the shared key for secure RADIUS accounting communication.

authentication: Specifies the shared key for secure RADIUS authentication communication.

cipher: Specifies the key in encrypted form.

simple: Specifies the key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. This argument is case sensitive. the encrypted form of the key is a string of 1 to 117 characters. The plaintext form of the key is a string of 1 to 64 characters.

Usage guidelines

The shared keys configured by using this command apply to all servers in the scheme. Make sure the settings match the shared keys configured on the RADIUS servers.

The shared keys specified for specific RADIUS servers take precedence over the shared key specified with this command.

Examples

In RADIUS scheme **radius1**, set the shared key to **ok** in plaintext form for secure accounting communication.

```
<Switch> system-view
[Switch] radius scheme radius1
[Switch-radius-radius1] key accounting simple ok
```

Related commands

display radius scheme

1.3.7. nas-ip (RADIUS scheme view)

Use **nas-ip** to specify a source IP address for outgoing RADIUS packets.

Use **undo nas-ip** to delete the source IP address of the specified type for outgoing RADIUS packets.

Syntax

nas-ip { *ipv4-address* | **ipv6** *ipv6-address* }

undo nas-ip [**ipv6**]

Default

The source IP address of an outgoing RADIUS packet is that specified by using the **radius nas-ip** command in system view.

If the **radius nas-ip** command is not configured, the source IP address is the primary IP address of the outbound interface.

Views

RADIUS scheme view

Predefined user roles

network-admin

Parameters

ipv4-address: Specifies an IPv4 address, which must be an address of the device. The IP address cannot be 0.0.0.0, 255.255.255.255, a class D address, a class E address, or a loopback address.

ipv6 *ipv6-address*: Specifies an IPv6 address, which must be a unicast address of the device and cannot be a loopback address or a link-local address.

Usage guidelines

The source IP address of RADIUS packets that a NAS sends must match the IP address of the NAS that is configured on the RADIUS server. A RADIUS server identifies a NAS by its IP address. Upon receiving a RADIUS packet, a RADIUS server checks whether the source IP address of the packet is the IP address of a managed NAS.

- If the source IP address of the packet is the IP address of a managed NAS, the server processes the packet.
- If the source IP address of the packet is not the IP address of a managed NAS, the server drops the packet.

As a best practice, specify a loopback interface address as the source IP address for outgoing RADIUS packets to avoid RADIUS packet loss caused by physical port errors.

If you use both the **nas-ip** command and **radius nas-ip** command, the following guidelines apply:

- The setting configured by using the **nas-ip** command in RADIUS scheme view applies only to the RADIUS scheme.
- The setting configured by using the **radius nas-ip** command in system view applies to all RADIUS schemes.
- The setting in RADIUS scheme view takes precedence over the setting in system view.

A RADIUS scheme can have only one source IPv4 address and one source IPv6 address for outgoing RADIUS packets.

If you do not specify the **ipv6** keyword for the **undo nas-ip** command, the command deletes the configured source IPv4 address for outgoing RADIUS packets.

Examples

In RADIUS scheme **radius1**, specify IP address 10.1.1.1 as the source IP address for outgoing RADIUS packets.

```
<Switch> system-view
[Switch] radius scheme radius1
[Switch-radius-radius1] nas-ip 10.1.1.1
```

Related commands

display radius scheme

radius nas-ip

1.3.8. primary accounting (RADIUS scheme view)

Use **primary accounting** to specify the primary RADIUS accounting server.

Use **undo primary accounting** to restore the default.

Syntax

primary accounting { *host-name* | *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **vpn-instance** *vpn-instance-name*] *

undo primary accounting

Default

The primary RADIUS accounting server is not specified.

Views

RADIUS scheme view

Predefined user roles

network-admin

Parameters

host-name: Specifies the host name of the primary RADIUS accounting server, a case-insensitive string of 1 to 253 characters.

ipv4-address: Specifies the IPv4 address of the primary RADIUS accounting server.

ipv6 *ipv6-address*: Specifies the IPv6 address of the primary RADIUS accounting server.

port-number: Specifies the service port number of the primary RADIUS accounting server. The value range for the UDP port number is 1 to 65535. The default setting is 1813.

key: Specifies the shared key for secure communication with the primary RADIUS accounting server.

cipher: Specifies the key in encrypted form.

simple: Specifies the key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. This argument is case sensitive. the encrypted form of the key is a string of 1 to 117 characters. The plaintext form of the key is a string of 1 to 64 characters.

vpn-instance *vpn-instance-name*: Specifies a VPN instance to which the primary RADIUS accounting server belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If the server is on the public network, do not specify this option.

Usage guidelines

Make sure the port number and shared key settings of the primary RADIUS accounting server are the same as those configured on the server.

Two accounting servers specified for a scheme, primary or secondary, cannot have identical VPN instance, host name, IP address, and port number settings.

The shared key configured by using this command takes precedence over the shared key configured with the **key accounting** command.

If the specified server resides on a VPN, specify the VPN instance by using the **vpn-instance** *vpn-instance-name* option. The VPN instance specified by this command takes precedence over the VPN instance specified for the RADIUS scheme.

If you use the **primary accounting** command to modify or delete the primary accounting server to which the device is sending a start-accounting request, communication with the primary server times out.

- When the RADIUS server load sharing feature is disabled, the device tries to communicate with an active server that has the highest priority for accounting.
- When the RADIUS server load sharing feature is enabled, the device returns an accounting failure message rather than searching for another active accounting server.

If you remove an actively used accounting server, the device no longer sends users' real-time accounting requests and stop-accounting requests. It does not buffer the stop-accounting requests. The device can generate incorrect accounting results.

Examples

In RADIUS scheme **radius1**, specify the primary accounting server with IP address 10.110.1.2, UDP port number 1813, and plaintext shared key **123456TESTacct&!**.

```
<Switch> system-view
[Switch] radius scheme radius1
[Switch-radius-radius1] primary accounting 10.110.1.2 1813 key simple 123456TESTacct&!
```

Related commands

display radius scheme

key (RADIUS scheme view)

secondary accounting (RADIUS scheme view)

1.3.9. primary authentication (RADIUS scheme view)

Use **primary authentication** to specify the primary RADIUS authentication server.

Use **undo primary authentication** to restore the default.

Syntax

primary authentication { *host-name* | *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **vpn-instance** *vpn-instance-name*] *

undo primary authentication

Default

The primary RADIUS authentication server is not specified.

Views

RADIUS scheme view

Predefined user roles

network-admin

Parameters

host-name: Specifies the host name of the primary RADIUS authentication server, a case-insensitive string of 1 to 253 characters.

ipv4-address: Specifies the IPv4 address of the primary RADIUS authentication server.

ipv6 *ipv6-address*: Specifies the IPv6 address of the primary RADIUS authentication server.

port-number: Specifies the service port number of the primary RADIUS authentication server. The value range for the UDP port number is 1 to 65535. The default setting is 1812.

key: Specifies the shared key for secure communication with the primary RADIUS authentication server.

cipher: Specifies the key in encrypted form.

simple: Specifies the key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. This argument is case sensitive. The encrypted form of the key is a string of 1 to 117 characters. The plaintext form of the key is a string of 1 to 64 characters.

vpn-instance *vpn-instance-name*: Specifies a VPN instance to which the primary RADIUS authentication server belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If the server is on the public network, do not specify this option.

Usage guidelines

Make sure the service port and shared key settings of the primary RADIUS authentication server are the same as those configured on the server.

Two authentication servers specified for a scheme, primary or secondary, cannot have identical VPN instance, host name, IP address, and port number settings.

The shared key configured by this command takes precedence over the shared key configured with the **key authentication** command.

If the specified server resides on a VPN instance, specify the VPN instance by using the **vpn-instance** *vpn-instance-name* option. The VPN instance specified by this command takes precedence over the VPN instance specified for the RADIUS scheme.

If you use the **primary authentication** command to modify or delete the primary authentication server during an authentication process, communication with the primary server times out.

- When the RADIUS server load sharing feature is disabled, the device tries to communicate with an active server that has the highest priority for authentication.
- When the RADIUS server load sharing feature is enabled, the device performs the following operations:
  a. Checks the number of currently served users for each active server.
  b. Determines the most appropriate server in performance to receive an AAA request.

Examples

In RADIUS scheme **radius1**, specify the primary authentication server with IP address 10.110.1.1, UDP port number 1812, and plaintext shared key **123456TESTauth&!**.

```
<Switch> system-view
[Switch] radius scheme radius1
[Switch-radius-radius1] primary authentication 10.110.1.1 1812 key simple
123456TESTauth&!
```

Related commands

display radius scheme

key (RADIUS scheme view)

secondary authentication (RADIUS scheme view)

1.3.10. radius dscp

Use **radius dscp** to change the DSCP priority of RADIUS packets.

Use **undo radius dscp** to restore the default.

Syntax

radius [**ipv6**] **dscp** *dscp-value*

undo radius [**ipv6**] **dscp**

Default

The DSCP priority of RADIUS packets is 0.

Views

System view

Predefined user roles

network-admin

Parameters

ipv6: Specifies the IPv6 RADIUS packets. If you do not specify this keyword, the command sets the DSCP priority for the IPv4 RADIUS packets.

dscp-value: Specifies the DSCP priority of RADIUS packets, in the range of 0 to 63. A larger value represents a higher priority.

Usage guidelines

Use this command to set the DSCP priority in the ToS field of RADIUS packets for changing their transmission priority.

Examples

Set the DSCP priority of IPv4 RADIUS packets to 10.

```
<Switch> system-view
[Switch] radius dscp 10
```

1.3.11. radius nas-ip

Use **radius nas-ip** to specify a source IP address for outgoing RADIUS packets.

Use **undo radius nas-ip** to delete a source IP address for outgoing RADIUS packets.

Syntax

radius nas-ip { *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]

undo radius nas-ip { *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]

Default

The source IP address of an outgoing RADIUS packet is the primary IP address of the outbound interface.

Views

System view

Predefined user roles

network-admin

Parameters

ipv4-address: Specifies an IPv4 address, which must be an address of the device. The IP address cannot be 0.0.0.0, 255.255.255.255, a class D address, a class E address, or a loopback address.

ipv6 *ipv6-address*: Specifies an IPv6 address, which must be a unicast address of the device and cannot be a loopback address or a link-local address.

vpn-instance *vpn-instance-name*: Specifies a VPN instance to which the source IP address belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. To configure a public-network source IP address, do not specify this option.

Usage guidelines

The source IP address of RADIUS packets that a NAS sends must match the IP address of the NAS that is configured on the RADIUS server. A RADIUS server identifies a NAS by its IP address. Upon receiving a RADIUS packet, a RADIUS server checks whether the source IP address of the packet is the IP address of a managed NAS.

- If the source IP address of the packet is the IP address of a managed NAS, the server processes the packet.
- If the source IP address of the packet is not the IP address of a managed NAS, the server drops the packet.

As a best practice, specify a loopback interface address as the source IP address for outgoing RADIUS packets to avoid RADIUS packet loss caused by physical port errors.

If you use both the **nas-ip** command and **radius nas-ip** command, the following guidelines apply:

- The setting configured by using the **nas-ip** command in RADIUS scheme view applies only to the RADIUS scheme.
- The setting configured by using the **radius nas-ip** command in system view applies to all RADIUS schemes.
- The setting in RADIUS scheme view takes precedence over the setting in system view.

You can specify a maximum of 16 source IP addresses in system view, including:

- Zero or one public-network source IPv4 address.
- Zero or one public-network source IPv6 address.
- Private-network source IP addresses.

Each VPN instance can have only one private-network source IPv4 address and one private-network source IPv6 address in system view.

Examples

Specify IP address 129.10.10.1 as the source address for outgoing RADIUS packets.

```
<Switch> system-view
[Switch] radius nas-ip 129.10.10.1
```

Related commands

nas-ip (RADIUS scheme view)

1.3.12. radius scheme

Use **radius scheme** to create a RADIUS scheme and enter its view, or enter the view of an existing RADIUS scheme.

Use **undo radius scheme** to delete a RADIUS scheme.

Syntax

radius scheme *radius-scheme-name*

undo radius scheme *radius-scheme-name*

Default

No RADIUS schemes exist.

Views

System view

Predefined user roles

network-admin

Parameters

radius-scheme-name: Specifies the RADIUS scheme name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

A RADIUS scheme can be used by more than one ISP domain at the same time.

The device supports a maximum of 16 RADIUS schemes.

Examples

Create a RADIUS scheme named **radius1** and enter RADIUS scheme view.

```
<Switch> system-view
[Switch] radius scheme radius1
[Switch-radius-radius1]
```

Related commands

display radius scheme

1.3.13. reauthentication server-select

> 🕮 **memo:**
>
> **reauthentication server-select** command is being supported from software after Version 7.2.16.

Use **reauthentication server-select** to specify a RADIUS server selection mode for reauthentication.

Use **undo reauthentication server-select** to restore the default.

Syntax

reauthentication server-select { **inherit** | **reselect** }

undo reauthentication server-select

Default

The inherit mode is used.

Views

RADIUS scheme view

Predefined user roles

network-admin

Parameters

inherit: Uses the RADIUS server that performed authentication for reauthentication.

reselect: Reselects a RADIUS server for reauthentication.

Usage guidelines

Use this command to configure the RADIUS server selection mechanism in reauthentication. Use one of the following modes depending on the network condition:

- **Inherit**—The device uses the RADIUS server that performed authentication for a user to perform reauthentication for that user. This mode reduces the amount of time used in reauthentication. However, if the RADIUS server is unreachable, the reauthentication will fail.
- **Reselect**—The device searches for a reachable RADIUS server to perform reauthentication for a user. This mode requires more time than the inherit mode. However, this mode ensures that the device can find the most suitable reachable RADIUS server for reauthentication. The following factors affect the RADIUS server selection:
  - Server configuration in the RADIUS scheme, including the configuration order.
  - Enabling status of the RADIUS server load sharing feature.
  - Status of the RADIUS servers in the RADIUS scheme.

Examples

In RADIUS scheme **radius1**, set the RADIUS server selection mode to reselect for reauthentication.

```
<Switch> system-view
[Switch] radius scheme radius1
[Switch-radius-radius1] reauthentication server-select reselect
```

1.3.14. reset radius statistics

Use **reset radius statistics** to clear RADIUS statistics.

Syntax

reset radius statistics

Views

User view

Predefined user roles

network-admin

Examples

Clear RADIUS statistics.

```
<Switch> reset radius statistics
```

Related commands

display radius statistics

1.3.15. reset stop-accounting-buffer (for RADIUS)

Use **reset stop-accounting-buffer** to clear buffered RADIUS stop-accounting requests to which no responses have been received.

Syntax

reset stop-accounting-buffer { **radius-scheme** *radius-scheme-name* | **session-id** *session-id* | **time-range** *start-time end-time* | **user-name** *user-name* }

Views

User view

Predefined user roles

network-admin

Parameters

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

session-id *session-id*: Specifies a session by its ID. The *session-id* argument is a string of 1 to 64 characters and cannot contain a letter. A session ID uniquely identifies an online user for a RADIUS scheme.

time-range *start-time end-time*: Specifies a time range. The start time and end time must be in the format of hh:mm:ss-mm/dd/yyyy or hh:mm:ss-yyyy/mm/dd.

user-name *user-name*: Specifies a user by its name, a case-sensitive string of 1 to 255 characters. Whether the *user-name* argument should include the domain name depends on the setting configured by using the **user-name-format** command for the RADIUS scheme.

Examples

Clear nonresponded RADIUS stop-accounting requests buffered for user **user0001@test**.

```
<Switch> reset stop-accounting-buffer user-name user0001@test
```

Clear nonresponded RADIUS stop-accounting requests buffered from 0:0:0 to 23:59:59 on August 31, 2015.

```
<Switch> reset stop-accounting-buffer time-range 0:0:0-08/31/2015 23:59:59-08/31/2015
```

Related commands

display stop-accounting-buffer (for RADIUS)

stop-accounting-buffer enable (RADIUS scheme view)

1.3.16. retry

Use **retry** to set the maximum number of attempts for transmitting a RADIUS packet to a single RADIUS server.

Use **undo retry** to restore the default.

Syntax

retry *retries*

undo retry

Default

The maximum number of RADIUS packet transmission attempts is 3.

Views

RADIUS scheme view

Predefined user roles

network-admin

Parameters

retries: Specifies the maximum number of RADIUS packet transmission attempts, in the range of 1 to 20.

Usage guidelines

Because RADIUS uses UDP packets to transmit data, the communication is not reliable.

If the device does not receive a response to its request from the RADIUS server within the response timeout period, the device retransmits the RADIUS request. To set the response timeout period, use the **timer response-timeout** command.

If the device does not receive a response from the RADIUS server after the maximum number of transmission attempts is reached, the device considers the request a failure.

If the client times out during the authentication process, the user is immediately logged off. To avoid user logoffs, the value multiplied by the following items cannot be larger than the client timeout period defined by the access module:

- The maximum number of RADIUS packet transmission attempts.
- The RADIUS server response timeout period.
- The number of RADIUS authentication servers in the RADIUS scheme.

When the device sends a RADIUS request to a new RADIUS server, it checks the total amount of time it has taken to transmit the RADIUS packet. If the amount of time has reached 300 seconds, the device stops sending the RADIUS request to the next RADIUS server. As a best practice, consider the number of RADIUS servers when you configure the maximum number of packet transmission attempts and the RADIUS server response timeout period.

Examples

In RADIUS scheme **radius1**, set the maximum number of RADIUS packet transmission attempts to 5.

```
<Switch> system-view
[Switch] radius scheme radius1
[Switch-radius-radius1] retry 5
```

Related commands

radius scheme

timer response-timeout (RADIUS scheme view)

1.3.17. retry realtime-accounting

Use **retry realtime-accounting** to set the maximum number of accounting attempts.

Use **undo retry realtime-accounting** to restore the default.

Syntax

retry realtime-accounting *retries*

undo retry realtime-accounting

Default

The maximum number of accounting attempts is 5.

Views

RADIUS scheme view

Predefined user roles

network-admin

Parameters

retries: Specifies the maximum number of accounting attempts, in the range of 1 to 255.

Usage guidelines

Typically, a RADIUS accounting server checks whether a user is online by using a timeout timer. If the server does not receive a real-time accounting request for a user in the timeout period, it considers that a line or device failure has occurred. The server stops accounting for the user.

To work with the RADIUS server, the NAS needs to send real-time accounting requests to the server before the timer on the server expires and to keep pace with the server in disconnecting the user when a failure occurs. The NAS disconnects from a user according to the maximum number of accounting attempts and specific parameters.

For example, the following conditions exist:

- The RADIUS server response timeout period is 3 seconds (set by using the **timer response-timeout** command).
- The maximum number of RADIUS packet transmission attempts is 3 (set by using the **retry** command).
- The real-time accounting interval is 12 minutes (set by using the **timer realtime-accounting** command).
- The maximum number of accounting attempts is 5 (set by using the **retry realtime-accounting** command).

In the above case, the device generates an accounting request every 12 minutes, and retransmits the request if it sends the request but receives no response within 3 seconds. If the device receives no response after transmitting the request three times, it considers the accounting attempt a failure, and makes another accounting attempt. If five consecutive accounting attempts fail, the device cuts the user connection.

Examples

In RADIUS scheme **radius1**, set the maximum number of accounting attempts to 10.

```
<Switch> system-view
[Switch] radius scheme radius1
[Switch-radius-radius1] retry realtime-accounting 10
```

Related commands

retry

timer realtime-accounting (RADIUS scheme view)

timer response-timeout (RADIUS scheme view)

1.3.18. retry stop-accounting (RADIUS scheme view)

Use **retry stop-accounting** to set the maximum number of transmission attempts for individual RADIUS stop-accounting requests.

Use **undo retry stop-accounting** to restore the default.

Syntax

retry stop-accounting *retries*

undo retry stop-accounting

Default

The maximum number of transmission attempts is 500 for individual RADIUS stop-accounting requests.

Views

RADIUS scheme view

Predefined user roles

network-admin

Parameters

retries: Specifies the maximum number of transmission attempts. The value range is 10 to 65535.

Usage guidelines

The maximum number of stop-accounting request transmission attempts controls the transmission of stop-accounting requests together with the following parameters:

- RADIUS server response timeout timer (set by using the **timer response-timeout** command).
- Maximum number of times to transmit a RADIUS packet per round (set by using the **retry** command).

For example, the following settings exist:

- The RADIUS server response timeout timer is 3 seconds.
- The maximum number of times to transmit a RADIUS packet per round is five.
- The maximum number of stop-accounting request transmission attempts is 20.

A stop-accounting request is retransmitted if the device does not receive a response within 3 seconds. When all five transmission attempts in this round are used, the device buffers the request and starts another round of retransmission. If 20 consecutive rounds of attempts fail, the device discards the request.

Examples

Set the maximum number of stop-accounting request transmission attempts to 1000 for RADIUS scheme **radius1**.

```
<Switch> system-view
[Switch] radius scheme radius1
[Switch-radius-radius1] retry stop-accounting 1000
```

Related commands

display stop-accounting-buffer (for RADIUS)

retry

timer response-timeout (RADIUS scheme view)

1.3.19. secondary accounting (RADIUS scheme view)

Use **secondary accounting** to specify a secondary RADIUS accounting server.

Use **undo secondary accounting** to remove a secondary RADIUS accounting server.

Syntax

secondary accounting { *host-name* | *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **vpn-instance** *vpn-instance-name*] *

undo secondary accounting [{ *host-name* | *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **vpn-instance** *vpn-instance-name*] *]

Default

No secondary RADIUS accounting servers are specified.

Views

RADIUS scheme view

Predefined user roles

network-admin

Parameters

host-name: Specifies the host name of a secondary RADIUS accounting server, a case-insensitive string of 1 to 253 characters.

ipv4-address: Specifies the IPv4 address of a secondary RADIUS accounting server.

ipv6 *ipv6-address*: Specifies the IPv6 address of a secondary RADIUS accounting server.

port-number: Specifies the service port number of the secondary RADIUS accounting server. The value range for the UDP port number is 1 to 65535. The default setting is 1813.

key: Specifies the shared key for secure communication with the secondary RADIUS accounting server.

cipher: Specifies the key in encrypted form.

simple: Specifies the key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. This argument is case sensitive. The encrypted form of the key is a string of 1 to 117 characters. The plaintext form of the key is a string of 1 to 64 characters.

vpn-instance *vpn-instance-name*: Specifies a VPN instance to which the secondary RADIUS accounting server belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If the server is on the public network, do not specify this option.

Usage guidelines

Make sure the port number and shared key settings of each secondary RADIUS accounting server are the same as those configured on the corresponding server.

A RADIUS scheme supports a maximum of 16 secondary RADIUS accounting servers. If the primary server fails, the device tries to communicate with a secondary server in active state. The device connects to the secondary servers in the order they are configured.

Two accounting servers specified for a scheme, primary or secondary, cannot have identical VPN instance, host name, IP address, and port number settings.

The shared key configured by this command takes precedence over the shared key configured with the **key accounting** command.

If the specified server resides on a VPN instance, specify the VPN instance by using the **vpn-instance** *vpn-instance-name* option. The VPN instance specified by this command takes precedence over the VPN instance specified for the RADIUS scheme.

If you use the **secondary accounting** command to modify or delete a secondary accounting server to which the device is sending a start-accounting request, communication with the secondary server times out.

- When the RADIUS server load sharing feature is disabled, the device tries to communicate with an active server that has the highest priority for accounting.
- When the RADIUS server load sharing feature is enabled, the device returns an accounting failure message rather than searching for another active accounting server.

If you remove an actively used accounting server, the device no longer sends users' real-time accounting requests and stop-accounting requests. The device does not buffer the stop-accounting requests, either.

Examples

In RADIUS scheme **radius1**, specify a secondary accounting server with IP address 10.110.1.1 and UDP port 1813.

```
<Switch> system-view
[Switch] radius scheme radius1
[Switch-radius-radius1] secondary accounting 10.110.1.1 1813
```

In RADIUS scheme **radius2**, specify two secondary accounting servers with IP addresses 10.110.1.1 and 10.110.1.2 and UDP port 1813.

```
<Switch> system-view
[Switch] radius scheme radius2
[Switch-radius-radius2] secondary accounting 10.110.1.1 1813
[Switch-radius-radius2] secondary accounting 10.110.1.2 1813
```

Related commands

display radius scheme

key (RADIUS scheme view)

primary accounting (RADIUS scheme view)

1.3.20. secondary authentication (RADIUS scheme view)

Use **secondary authentication** to specify a secondary RADIUS authentication server.

Use **undo secondary authentication** to remove a secondary RADIUS authentication server.

Syntax

secondary authentication { *host-name* | *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **vpn-instance** *vpn-instance-name*] *

undo secondary authentication [{ *host-name* | *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **vpn-instance** *vpn-instance-name*] *]

Default

No secondary RADIUS authentication servers are specified.

Views

RADIUS scheme view

Predefined user roles

network-admin

Parameters

host-name: Specifies the host name of a secondary RADIUS authentication server, a case-insensitive string of 1 to 253 characters.

ipv4-address: Specifies the IPv4 address of a secondary RADIUS authentication server.

ipv6 *ipv6-address*: Specifies the IPv6 address of a secondary RADIUS authentication server.

port-number: Specifies the service port number of the secondary RADIUS authentication server. The value range for the UDP port number is 1 to 65535. The default setting is 1812.

key: Specifies the shared key for secure communication with the secondary RADIUS authentication server.

cipher: Specifies the key in encrypted form.

simple: Specifies the key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. This argument is case sensitive. The encrypted form of the key is a string of 1 to 117 characters. The plaintext form of the key is a string of 1 to 64 characters.

vpn-instance *vpn-instance-name*: Specifies a VPN instance to which the secondary RADIUS authentication server belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If the server is on the public network, do not specify this option.

Usage guidelines

Make sure the port number and shared key settings of each secondary RADIUS authentication server are the same as those configured on the corresponding server.

A RADIUS scheme supports a maximum of 16 secondary RADIUS authentication servers. If the primary server fails, the device tries to communicate with a secondary server in active state. The device connects to the secondary servers in the order they are configured.

Two authentication servers specified for a scheme, primary or secondary, cannot have identical VPN instance, host name, IP address, and port number settings.

The shared key configured by this command takes precedence over the shared key configured with the **key authentication** command.

If the specified server resides on a VPN instance, specify the VPN instance by using the **vpn-instance** *vpn-instance-name* option. The VPN instance specified by this command takes precedence over the VPN instance specified for the RADIUS scheme.

If you use the **secondary authentication** command to modify or delete a secondary authentication server during an authentication process, communication with the secondary server times out.

- When the RADIUS server load sharing feature is disabled, the device tries to communicate with an active server that has the highest priority for authentication.
- When the RADIUS server load sharing feature is enabled, the device performs the following operations:
  a. Checks the number of currently served users for each active server.
  b. Determines the most appropriate server in performance to receive an AAA request.

Examples

In RADIUS scheme **radius1**, specify a secondary authentication server with IP address 10.110.1.2 and UDP port 1812.

```
<Switch> system-view
[Switch] radius scheme radius1
[Switch-radius-radius1] secondary authentication 10.110.1.2 1812
```

In RADIUS scheme **radius2**, specify two secondary authentication servers with IP addresses 10.110.1.1 and 10.110.1.2 and UDP port 1812.

```
<Switch> system-view
[Switch] radius scheme radius2
[Switch-radius-radius2] secondary authentication 10.110.1.1 1812
[Switch-radius-radius2] secondary authentication 10.110.1.2 1812
```

Related commands

display radius scheme

key (RADIUS scheme view)

primary authentication (RADIUS scheme view)

1.3.21. snmp-agent trap enable radius

Use **snmp-agent trap enable radius** to enable SNMP notifications for RADIUS.

Use **undo snmp-agent trap enable radius** to disable SNMP notifications for RADIUS.

Syntax

snmp-agent trap enable radius [**accounting-server-down** | **accounting-server-up** | **authentication-error-threshold** | **authentication-server-down** | **authentication-server-up**] *

undo snmp-agent trap enable radius [**accounting-server-down** | **accounting-server-up** | **authentication-error-threshold** | **authentication-server-down** | **authentication-server-up**] *

Default

All RADIUS SNMP notifications are disabled.

Views

System view

Predefined user roles

network-admin

Parameters

accounting-server-down: Specifies notifications to be sent when the RADIUS accounting server becomes unreachable.

accounting-server-up: Specifies notifications to be sent when the RADIUS accounting server becomes reachable.

authentication-error-threshold: Specifies notifications to be sent when the number of authentication failures exceeds the specified threshold. The threshold is represented by the ratio of the authentication failures to the total number of authentication attempts. The value range is 1 to 100, and the default value is 30. This threshold can only be configured through the MIB.

authentication-server-down: Specifies notifications to be sent when the RADIUS authentication server becomes unreachable.

authentication-server-up: Specifies notifications to be sent when the RADIUS authentication server becomes reachable.

Usage guidelines

If you do not specify any keywords, this command enables or disables all types of notifications for RADIUS.

When SNMP notifications for RADIUS are enabled, the device supports the following notifications generated by RADIUS:

- **RADIUS server unreachable notification**—The RADIUS server cannot be reached. RADIUS generates this notification if it cannot receive any response to an accounting or authentication request within the specified RADIUS request transmission attempts.
- **RADIUS server reachable notification**—The RADIUS server can be reached. RADIUS generates this notification for a previously blocked RADIUS server after the quiet timer expires.
- **Excessive authentication failures notification**—RADIUS generates this notification when the number of authentication failures to the total number of authentication attempts exceeds the specified threshold.

Examples

Enable the device to send RADIUS accounting server unreachable notifications.

```
<Switch> system-view
[Switch] snmp-agent trap enable radius accounting-server-down
```

1.3.22. state primary

Use **state primary** to set the status of a primary RADIUS server.

Syntax

state primary { **accounting** | **authentication** } { **active** | **block** }

Default

A primary RADIUS server is in active state.

Views

RADIUS scheme view

Predefined user roles

network-admin

Parameters

accounting: Specifies the primary RADIUS accounting server.

authentication: Specifies the primary RADIUS authentication server.

active: Specifies the active state, the normal operation state.

block: Specifies the blocked state, the out-of-service state.

Usage guidelines

When the RADIUS server load sharing feature is disabled, the device first tries to communicate with the primary server if the primary server is in active state. If the primary server is unavailable, the device performs the following operations:

- Changes the status of the primary server to blocked.

- Starts a quiet timer for the server.
- Tries to communicate with a secondary server in active state.

When the quiet timer of the primary server times out, the status of the server automatically changes to active. If you set the server status to blocked before the quiet timer times out, the server status cannot change back to active unless you manually set the status to active.

When the RADIUS server load sharing feature is enabled, the device checks the number of currently served users only for servers in active state. The most appropriate active server is selected for communication.

When the primary server and all secondary servers are in blocked state, the device tries to communicate with the primary server.

Examples

In RADIUS scheme **radius1**, set the status of the primary authentication server to blocked.

```
<Switch> system-view
[Switch] radius scheme radius1
[Switch-radius-radius1] state primary authentication block
```

Related commands

display radius scheme

state secondary

1.3.23. state secondary

Use **state secondary** to set the status of a secondary RADIUS server.

Syntax

state secondary { **accounting** | **authentication** } [{ *host-name* | *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **vpn-instance** *vpn-instance-name*] *] { **active** | **block** }

Default

A secondary RADIUS server is in active state.

Views

RADIUS scheme view

Predefined user roles

network-admin

Parameters

accounting: Specifies a secondary RADIUS accounting server.

authentication: Specifies a secondary RADIUS authentication server.

host-name: Specifies the host name of the secondary RADIUS server, a case-insensitive string of 1 to 253 characters.

ipv4-address: Specifies the IPv4 address of a secondary RADIUS server.

ipv6 *ipv6-address*: Specifies the IPv6 address of a secondary RADIUS server.

port-number: Specifies the service port number of a secondary RADIUS server. The value range for the UDP port number is 1 to 65535. The default port numbers for authentication and accounting are 1812 and 1813, respectively.

vpn-instance *vpn-instance-name*: Specifies a VPN instance to which the secondary RADIUS server belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters.

active: Specifies the active state, the normal operation state.

block: Specifies the blocked state, the out-of-service state.

Usage guidelines

If you do not specify an IP address, this command changes the status of all configured secondary RADIUS servers.

If the device finds that a secondary server in active state is unreachable, the device performs the following operations:

- Changes the status of the secondary server to blocked.
- Starts a quiet timer for the server.
- Tries to communicate with another secondary server in active state.

When the quiet timer of a server times out, the status of the server automatically changes to active. If you set the server status to blocked before the quiet timer times out, the server status cannot change back to active unless you manually set the status to active. If all configured secondary servers are unreachable, the device considers the authentication or accounting attempt a failure.

When the RADIUS server load sharing feature is enabled, the device checks the number of currently served users only for servers in active state. The most appropriate active server is selected for communication.

Examples

In RADIUS scheme **radius1**, set the status of all the secondary authentication servers to blocked.

```
<Switch> system-view
[Switch] radius scheme radius1
[Switch-radius-radius1] state secondary authentication block
```

Related commands

display radius scheme

state primary

1.3.24. stop-accounting-buffer enable (RADIUS scheme view)

Use **stop-accounting-buffer enable** to enable buffering of RADIUS stop-accounting requests to which no responses have been received.

Use **undo stop-accounting-buffer enable** to disable the buffering feature.

Syntax

stop-accounting-buffer enable

undo stop-accounting-buffer enable

Default

The device buffers the RADIUS stop-accounting requests to which no responses have been received.

Views

RADIUS scheme view

Predefined user roles

network-admin

Usage guidelines

This command enables the device to buffer a RADIUS stop-accounting request that has no response after the maximum transmission attempts (set by using the **retry** command) have been made. The device resends the buffered request until it receives a server response or when the number of stop-accounting request transmission attempts reaches the upper limit. If no more attempts are available, the device discards the request. However, if you have removed an accounting server, stop-accounting requests destined for the server are not buffered.

Examples

Enable buffering of RADIUS stop-accounting requests to which no responses have been received.

```
<Switch> system-view
[Switch] radius scheme radius1
[Switch-radius-radius1] stop-accounting-buffer enable
```

Related commands

display stop-accounting-buffer (for RADIUS)

reset stop-accounting-buffer (for RADIUS)

1.3.25. timer quiet (RADIUS scheme view)

Use **timer quiet** to set the quiet timer for the servers specified in a RADIUS scheme.

Use **undo timer quiet** to restore the default.

Syntax

timer quiet *minutes*

undo timer quiet

Default

The server quiet timer period is 5 minutes in a RADIUS scheme.

Views

RADIUS scheme view

Predefined user roles

network-admin

Parameters

minutes: Specifies the server quiet period in minutes, in the range of 1 to 255.

Usage guidelines

Make sure the server quiet timer is set correctly.

A timer that is too short might result in frequent authentication or accounting failures. This is because the device will continue to attempt to communicate with an unreachable server that is in active state.

A timer that is too long might temporarily block a reachable server that has recovered from a failure. This is because the server will remain in blocked state until the timer expires.

Examples

In RADIUS scheme **radius1**, set the quiet timer to 10 minutes for the servers.

```
<Switch> system-view
[Switch] radius scheme radius1
[Switch-radius-radius1] timer quiet 10
```

Related commands

display radius scheme

1.3.26. timer realtime-accounting (RADIUS scheme view)

Use **timer realtime-accounting** to set the real-time accounting interval.

Use **undo timer realtime-accounting** to restore the default.

Syntax

timer realtime-accounting *interval*

undo timer realtime-accounting

Default

The real-time accounting interval is 12 minutes.

Views

RADIUS scheme view

Predefined user roles

network-admin

Parameters

interval: Specifies the real-time accounting interval in the range of 0 to 71582.

Usage guidelines

When the real-time accounting interval on the device is not zero, the device sends online user accounting information to the RADIUS accounting server at the configured interval.

When the real-time accounting interval on the device is zero, the device sends online user accounting information to the RADIUS accounting server at the real-time accounting interval configured on the server. If the real-time accounting interval is not configured on the server, the device does not send online user accounting information.

A short interval helps improve accounting precision but requires many system resources.

Table 1-7 Recommended real-time accounting intervals

Number of users	Real-time accounting interval
1 to 99	3 minutes
100 to 499	6 minutes
500 to 999	12 minutes
1000 or more	15 minutes or longer

Examples

In RADIUS scheme **radius1**, set the real-time accounting interval to 51 minutes.

```
<Switch> system-view
[Switch] radius scheme radius1
[Switch-radius-radius1] timer realtime-accounting 51
```

Related commands

retry realtime-accounting

1.3.27. timer response-timeout (RADIUS scheme view)

Use **timer response-timeout** to set the RADIUS server response timeout timer.

Use **undo timer response-timeout** to restore the default.

Syntax

timer response-timeout *seconds*

undo timer response-timeout

Default

The RADIUS server response timeout period is 3 seconds.

Views

RADIUS scheme view

Predefined user roles

network-admin

Parameters

seconds: Specifies the RADIUS server response timeout period, in the range of 1 to 10 seconds.

Usage guidelines

If a NAS receives no response from the RADIUS server in a period of time after sending a RADIUS request, it resends the request so that the user has more opportunity to obtain the RADIUS service. The NAS uses the RADIUS server response timeout timer to control the transmission interval.

If the client times out during the authentication process, the user is immediately logged off. To avoid user logoffs, the value multiplied by the following items cannot be larger than the client timeout period defined by the access module:

- The maximum number of RADIUS packet transmission attempts.
- The RADIUS server response timeout period.
- The number of RADIUS servers in the RADIUS scheme.

When the device sends a RADIUS request to a new RADIUS server, it checks the total amount of time it has taken to transmit the RADIUS packet. If the amount of time has reached 300 seconds, the device stops sending the RADIUS request to the next RADIUS server. As a best practice, consider the number of RADIUS servers when you configure the maximum number of packet transmission attempts and the RADIUS server response timeout period.

Examples

In RADIUS scheme **radius1**, set the RADIUS server response timeout timer to 5 seconds.

```
<Switch> system-view
[Switch] radius scheme radius1
[Switch-radius-radius1] timer response-timeout 5
```

Related commands

display radius scheme

retry

1.3.28. user-name-format (RADIUS scheme view)

Use **user-name-format** to specify the format of the username to be sent to a RADIUS server.

Use **undo user-name-format** to restore the default.

Syntax

user-name-format { **keep-original** | **with-domain** | **without-domain** }

undo user-name-format

Default

The ISP domain name is included in the usernames sent to a RADIUS server.

Views

RADIUS scheme view

Predefined user roles

network-admin

Parameters

keep-original: Sends the username to the RADIUS server as the username is entered.

with-domain: Includes the ISP domain name in the username sent to the RADIUS server.

without-domain: Excludes the ISP domain name from the username sent to the RADIUS server.

Usage guidelines

A username is generally in the *userid@isp-name* format, of which the *isp-name* argument is used by the device to determine the ISP domain to which a user belongs. Some earlier RADIUS servers, however, cannot recognize a username containing an ISP domain name. Before sending a username including a domain name to such a RADIUS server, the device must remove the domain name. This command allows you to specify whether to include a domain name in a username sent to a RADIUS server.

If a RADIUS scheme defines that the username is sent without the ISP domain name, do not apply the scheme to more than one ISP domain. Otherwise, the RADIUS server will consider two users in different ISP domains but with the same *userid* as one user.

For 802.1X users using EAP authentication, the **user-name-format** command configured for a RADIUS scheme does not take effect. The device does not change the usernames from clients before forwarding them to the RADIUS server.

Examples

In RADIUS scheme **radius1**, configure the device to remove the domain name from the usernames sent to the RADIUS servers.

```
<Switch> system-view
[Switch] radius scheme radius1
[Switch-radius-radius1] user-name-format without-domain
```

Related commands

display radius scheme

Contents

A page of this section is **9-x-x**

2. 802.1X commands 2-1
2.1. 802.1X commands 2-1
2.1.1. display dot1x 2-1
2.1.2. display dot1x connection 2-5
2.1.3. dot1x 2-8
2.1.4. dot1x access-user log enable 2-9
2.1.5. dot1x authentication-method 2-9
2.1.6. dot1x auth-fail vlan 2-11
2.1.7. dot1x guest-vlan 2-11
2.1.8. dot1x handshake 2-12
2.1.9. dot1x handshake reply enable 2-13
2.1.10. dot1x mandatory-domain 2-14
2.1.11. dot1x max-user 2-14
2.1.12. dot1x multicast-trigger 2-15
2.1.13. dot1x port-control 2-16
2.1.14. dot1x port-method 2-16
2.1.15. dot1x quiet-period 2-17
2.1.16. dot1x re-authenticate 2-18
2.1.17. dot1x retry 2-19
2.1.18. dot1x timer 2-19
2.1.19. dot1x timer reauth-period 2-21
2.1.20. dot1x unicast-trigger 2-22
2.1.21. reset dot1x guest-vlan 2-23
2.1.22. reset dot1x statistics 2-23

2. 802.1X commands

2.1. 802.1X commands

2.1.1. display dot1x

Use **display dot1x** to display information about 802.1X.

Syntax

display dot1x [**sessions** | **statistics**] [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

sessions: Displays 802.1X session information.

statistics: Displays 802.1X statistics.

interface *interface-type interface-number*: Specifies a port by its type and number.

Usage guidelines

If you do not specify the **sessions** keyword or the **statistics** keyword, this command displays all information about 802.1X, including session information, statistics, and settings.

If you do not specify the **interface** *interface-type interface-number* option, this command displays all global and port-specific 802.1X information.

Examples

Display all information about 802.1X.

```
<Switch> display dot1x
Global 802.1X parameters:
   802.1X authentication  : Enabled
   CHAP authentication    : Enabled
   Max-tx period          : 30 s
   Handshake period       : 15 s
   Quiet timer            : Disabled
         Quiet period     : 60 s
   Supp timeout           : 30 s
   Server timeout         : 100 s
   Reauth period          : 3600 s
   Max auth requests      : 2
   EAD assistant function : Disabled
       URL                : http://www.dwsoft.com
       Free IP            : 6.6.6.0         255.255.255.0
```

```
      EAD timeout        : 30 min
  Domain delimiter       : @
Online 802.1X wired users    : 1

GigabitEthernet1/0/1  is link-up
  802.1X authentication      : Enabled
  Handshake                  : Enabled
  Handshake reply            : Disabled
  Handshake security         : Disabled
  Unicast trigger            : Disabled
  Periodic reauth            : Disabled
  Port role                  : Authenticator
  Authorization mode         : Auto
  Port access control        : Port-based
  Multicast trigger          : Enabled
  Mandatory auth domain      : Not configured
  Guest VLAN                 : 3
  Auth-Fail VLAN             : Not configured
  Critical VLAN              : Not configured
  Critical voice VLAN        : Disabled
  Add Guest VLAN delay       : Disabled
  Re-auth server-unreachable : Logoff
  Max online users           : 4294967295
  User IP freezing           : Disabled
  Reauth period              : 0 s
  Send Packets Without Tag   : Disabled
  Max Attempts Fail Number   : 0
  Guest VSI                  : Not configured
  Auth-Fail VSI              : Not configured
  Critical VSI               : Not configured
  Add Guest VSI delay        : Disabled

  EAPOL packets: Tx 3, Rx 3
  Sent EAP Request/Identity packets : 1
       EAP Request/Challenge packets: 1
       EAP Success packets: 1
       EAP Failure packets: 0
  Received EAPOL Start packets : 1
           EAPOL LogOff packets: 1
           EAP Response/Identity packets : 1
           EAP Response/Challenge packets: 1
           Error packets: 0
  Online 802.1X users: 1
         MAC address         Auth state
         0001-0000-0000      Authenticated
```

Table 2-1 Command output

Field	Description
Global 802.1X parameters	Global 802.1X configuration.
802.1X authentication	Whether 802.1X is enabled globally.
CHAP authentication	Performs EAP termination and uses CHAP to communicate with the RADIUS server.
EAP authentication	Relays EAP packets and supports any of the EAP authentication methods to communicate with the RADIUS server.
PAP authentication	Performs EAP termination and uses PAP to communicate with the RADIUS server.
Max-tx period	Username request timeout timer in seconds.
Handshake period	Handshake timer in seconds.
Quiet timer	Status of the quiet timer, enabled or disabled.
Quiet period	Quiet timer in seconds.
Supp timeout	Client timeout timer in seconds.
Server timeout	Server timeout timer in seconds.
Reauth period	Periodic reauthentication timer in seconds.
Max auth requests	Maximum number of attempts for sending an authentication request to a client.
EAD assistant function	Whether EAD assistant is enabled.
URL	Redirect URL for unauthenticated users using a Web browser to access the network.
Free IP	Network segment accessible to unauthenticated users.
EAD timeout	EAD rule timer in minutes.
Domain delimiter	Domain delimiters supported by the device.
Online 802.1X wired users	Number of wired online 802.1X users, including users that have passed 802.1X authentication and users that are performing 802.1X authentication.
GigabitEthernet1/0/1 is link-up	Status of the port. In this example, GigabitEthernet 1/0/1 is up.
802.1X authentication	Whether 802.1X is enabled on the port.
Handshake	Whether the online user handshake feature is enabled on the port.
Handshake reply	Whether the online user handshake reply feature is enabled on the port.
Handshake security	Whether the online user handshake security feature is enabled on the port.
Unicast trigger	Whether the 802.1X unicast trigger is enabled on the port.
Periodic reauth	Whether 802.1X periodic reauthentication is enabled on the port.
Port role	Role of the port. The port functions only as an **Authenticator**.

Field	Description
Authorization mode	Authorization state of the port, which can be Force-Authorized, Auto, or Force-Unauthorized.
Port access control	Access control method of the port: • **MAC-based**—MAC-based access control. • **Port-based**—Port-based access control.
Multicast trigger	Whether the 802.1X multicast trigger feature is enabled.
Mandatory auth domain	Mandatory authentication domain on the port.
Guest VLAN	802.1X guest VLAN configured on the port. If no 802.1X guest VLAN is configured on the port, this field displays **Not configured**.
Auth-Fail VLAN	802.1X Auth-Fail VLAN configured on the port. If no 802.1X Auth-Fail VLAN is configured on the port, this field displays **Not configured**.
Critical VLAN	802.1X critical VLAN configured on the port. If no 802.1X critical VLAN is configured on the port, this field displays **Not configured**.
Critical voice VLAN	Whether the 802.1X critical voice VLAN feature is enabled on the port.
Add Guest VLAN delay	Status and mode of the 802.1X guest VLAN assignment delay feature on a port: • **EAPOL**—EAPOL-triggered 802.1X guest VLAN assignment delay is enabled. • **NewMac**—New MAC-triggered 802.1X guest VLAN assignment delay is enabled. • **ALL**—Both EAPOL-triggered and new MAC-triggered 802.1X guest VLAN assignment delays are enabled. • **Disabled**—802.1X guest VLAN assignment delay is disabled.
Re-auth server-unreachable	Whether to log off online 802.1X users or keep them online when no server is reachable for 802.1X reauthentication.
Max online users	Maximum number of concurrent 802.1X users on the port.
User IP freezing	Whether user IP freezing is enabled on the port.
Reauth period	Periodic reauthentication timer in seconds on the port.
Send Packets Without Tag	Whether to remove the VLAN tags of all 802.1X protocol packets sent out of the port to 802.1X clients.
Max Attempts Fail Number	Maximum number of 802.1X authentication attempts for MAC authenticated users.
Guest VSI	802.1X guest VSI configured on the port. If no 802.1X guest VSI is configured on the port, this field displays **Not configured**.
Auth-Fail VSI	802.1X Auth-Fail VSI configured on the port. If no 802.1X Auth-Fail VSI is configured on the port, this field displays **Not configured**.
Critical VSI	802.1X critical VSI configured on the port. If no 802.1X critical VSI is configured on the port, this field

Field	Description
	displays **Not configured**.
Add Guest VSI delay	Status and mode of the 802.1X guest VSI assignment delay feature on a port: • **EAPOL only**—EAPOL-triggered 802.1X guest VSI assignment delay is enabled. • **NewMAC only**—New MAC-triggered 802.1X guest VSI assignment delay is enabled. • **EAPOL or NewMAC**—Both EAPOL-triggered and new MAC-triggered 802.1X guest VSI assignment delays are enabled. • **Disabled**—802.1X guest VSI assignment delay is disabled.
EAPOL packets	Number of sent (Tx) and received (Rx) EAPOL packets.
Sent EAP Request/Identity packets	Number of sent EAP-Request/Identity packets.
EAP Request/Challenge packets	Number of sent EAP-Request/MD5-Challenge packets.
EAP Success packets	Number of sent EAP-Success packets.
EAP Failure packets	Number of sent EAP-Failure packets.
Received EAPOL Start packets	Number of received EAPOL-Start packets.
EAPOL LogOff packets	Number of received EAPOL-LogOff packets.
EAP Response/Identity packets	Number of received EAP-Response/Identity packets.
EAP Response/Challenge packets	Number of received EAP-Response/MD5-Challenge packets.
Error packets	Number of received error packets.
Online 802.1X users	Number of online 802.1X users on the port, including users that have passed 802.1X authentication and users that are performing 802.1X authentication.
MAC address	MAC addresses of the online 802.1X users.
Auth state	Authentication status of the online 802.1X users.

2.1.2. display dot1x connection

Use **display dot1x connection** to display information about online 802.1X users.

Syntax

display dot1x connection [**interface** *interface-type interface-number* | **slot** *slot-number* | **user-mac** *mac-address* | **user-name** *name-string*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number. If you do not specify a port, this command displays online 802.1X user information for all ports.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays online 802.1X user information for all member devices.

user-mac *mac-address*: Specifies an 802.1X user by MAC address. The *mac-address* argument represents the MAC address of the user, in the form of H-H-H. If you do not specify an 802.1X user, this command displays all online 802.1X user information.

user-name *name-string*: Specifies an 802.1X user by its name. The *name-string* argument represents the username, a case-sensitive string of 1 to 253 characters. If you do not specify an 802.1X user, this command displays all online 802.1X user information.

Examples

Display information about all online 802.1X users.

```
<Switch> display dot1x connection
Total connections: 1

Slot ID: 1
User MAC address: 0015-e9a6-7cfe
Access interface: GigabitEthernet1/0/1
Username: ias
User access state: Successful
Authentication domain: nec
IPv4 address: 192.168.1.1
IPv6 address: 2000:0:0:0:1:2345:6789:abcd
Authentication method: CHAP
Initial VLAN: 1
Authorization untagged VLAN: 6
Authorization tagged VLAN list: 1 to 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 29 31 33
                                35 37 40 to 100
Authorization VSI: N/A
Authorization ACL ID: 3001
Authorization user profile: N/A
Authorization CAR:
  Average input rate: 102400
  Peak input rate: 204800
  Average output rate: 102400
  Peak output rate: 204800
Termination action: Default
Session timeout period: 2 s
Online from: 2013/03/02  13:14:15
Online duration: 0h 2m 15s
```

Table 2-2 Command output

Field	Description
Total connections	Number of online 802.1X users.
User MAC address	MAC address of the user.

Field	Description
Access interface	Interface through which the user access the device.
User access state	Access state of the user. • **Successful**—The user passes 802.1X authentication and comes online. • **Open**—The user uses a nonexistent username or an incorrect password to come online in open authentication mode.
Authentication domain	ISP domain used for 802.1X authentication.
IPv4 address	IPv4 address of the user. If the device does not get the IPv4 address of the user, this field is not available.
IPv6 address	IPv6 address of the user. If the device does not get the IPv6 address of the user, this field is not available.
Authentication method	EAP message handling method: • **CHAP**—Performs EAP termination and uses CHAP to communicate with the RADIUS server. • **EAP**—Relays EAP packets and supports any of the EAP authentication methods to communicate with the RADIUS server. • **PAP**—Performs EAP termination and uses PAP to communicate with the RADIUS server.
Initial VLAN	VLAN to which the user belongs before 802.1X authentication.
Authorization untagged VLAN	Untagged VLAN authorized to the user.
Authorization tagged VLAN list	Tagged VLANs authorized to the user.
Authorization VSI	VSIs authorized to the user.
Authorization ACL ID	ACL authorized to the user. If the ACL authorization fails, this field displays **(Not effective)** after the ACL ID.
Authorization user profile	User profile authorized to the user.
Authorization CAR	Authorization CAR attributes assigned by the server. • **Average input rate**—Average rate of inbound traffic in bps. • **Peak input rate**—Peak rate of inbound traffic in bps. • **Average output rate**—Average rate of outbound traffic in bps. • **Peak output rate**—Peak rate of outbound traffic in bps. If the server does not assign the peak rates, the peak rates by default are the same as the assigned average rates. In the current software version, the device does not support exclusive assignment of peak rates from the server. If no authorization CAR attributes are assigned, this field displays **N/A**.
Termination action	Action attribute assigned by the server to terminate the user session: • **Default**—Logs off the online authenticated 802.1X user

Field	Description
	when the session timeout timer expires. This attribute does not take effect when 802.1X periodic reauthentication is enabled and the periodic reauthentication timer is shorter than the session timeout timer. • **Radius-request**—Reauthenticates the online user when the session timeout timer expires, regardless of whether the 802.1X periodic reauthentication feature is enabled or not. If the device performs local authentication, this field displays **Default**.
Session timeout period	Session timeout timer assigned by the server.
Online from	Time from which the 802.1X user came online.
Online duration	Online duration of the 802.1X user.

2.1.3. dot1x

Use **dot1x** to enable 802.1X globally or on a port.

Use **undo dot1x** to disable 802.1X globally or on a port.

Syntax

dot1x

undo dot1x

Default

802.1X is neither enabled globally nor enabled for any port.

Views

System view

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

For the 802.1X feature to take effect on a port, you must enable the feature both globally and on the port.

Examples

Enable 802.1X globally.

```
<Switch> system-view
[Switch] dot1x
```

Enable 802.1X on GigabitEthernet 1/0/1.

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] dot1x
[Switch-GigabitEthernet1/0/1] quit
```

Related commands

display dot1x

NOTE:
QX-S5600G series can be certified up to 100PPS.

2.1.4. dot1x access-user log enable

Use **dot1x access-user log enable** to enable logging for 802.1X users.

Use **undo dot1x access-user log enable** to disable logging for 802.1X users.

Syntax

dot1x access-user log enable [**abnormal-logoff** | **failed-login** | **normal-logoff** | **successful-login**] *

undo dot1x access-user log enable [**abnormal-logoff** | **failed-login** | **normal-logoff** | **successful-login**] *

Default

Logging for 802.1X users is enabled.

Views

System view

Predefined user roles

network-admin

Parameters

abnormal-logoff: Specifies logs generated for exceptional logoffs of 802.1X users, such as logoffs caused by realtime accounting failures and reauthentication failures.

failed-login: Specifies logs generated for login failures of 802.1X users.

normal-logoff: Specifies logs generated for logoffs requested by 802.1X users.

successful-login: Specifies logs generated for successful logins of 802.1X users.

Usage guidelines

As a best practice, disable this feature to prevent excessive output of logs for 802.1X users.

If you do not specify any parameters, this command enables all logging functions for 802.1X users.

Examples

Enable logging for login failures of 802.1X users.

```
<Switch> system-view
[Switch] dot1x access-user log enable failed-login
```

Related commands

info-center source dot1x logfile deny (*Network Management and Monitoring Command Reference*)

2.1.5. dot1x authentication-method

Use **dot1x authentication-method** to specify an EAP message handling method.

Use **undo dot1x authentication-method** to restore the default.

Syntax

dot1x authentication-method { **chap** | **eap** | **pap** }

undo dot1x authentication-method

Default

The access device performs EAP termination and uses CHAP to communicate with the RADIUS server.

Views

System view

Predefined user roles

network-admin

Parameters

chap: Configures the access device to perform Extensible Authentication Protocol (EAP) termination and use the Challenge Handshake Authentication Protocol (CHAP) to communicate with the RADIUS server.

eap: Configures the access device to relay EAP packets, and supports any of the EAP authentication methods to communicate with the RADIUS server.

pap: Configures the access device to perform EAP termination and use the Password Authentication Protocol (PAP) to communicate with the RADIUS server.

Usage guidelines

The access device terminates or relays EAP packets.

- **In EAP termination mode**—The access device re-encapsulates and sends the authentication data from the client in standard RADIUS packets to the RADIUS server. The device performs either CHAP or PAP authentication with the RADIUS server. In this mode, the RADIUS server supports only MD5-Challenge EAP authentication and the username and password EAP authentication initiated by an iNode client.
  - PAP transports usernames and passwords in plain text. The authentication method applies to scenarios that do not require high security. To use PAP, the client can be an iNode 802.1X client.
  - CHAP transports usernames in plain text and passwords in encrypted form over the network. CHAP is more secure than PAP.
- **In EAP relay mode**—The access device relays EAP messages between the client and the RADIUS server. The EAP relay mode supports multiple EAP authentication methods, such as MD5-Challenge, EAP-TLS, and PEAP. To use this mode, make sure the RADIUS server meets the following requirements:
  - Supports the EAP-Message and Message-Authenticator attributes.
  - Uses the same EAP authentication method as the client.

  If this mode is used, the **user-name-format** command configured in RADIUS scheme view does not take effect. For more information about the **user-name-format** command, see "RADIUS commands."

If RADIUS authentication is used, you must configure the access device to use the same authentication method (PAP, CHAP, or EAP) as the RADIUS server.

Examples

Enable the access device to terminate EAP packets and perform PAP authentication with the RADIUS server.

```
<Switch> system-view
```

```
[Switch] dot1x authentication-method pap
```

Related commands

display dot1x

2.1.6. dot1x auth-fail vlan

Use **dot1x auth-fail vlan** to configure an 802.1X Auth-Fail VLAN on a port.

Use **undo dot1x auth-fail vlan** to restore the default.

Syntax

dot1x auth-fail vlan *authfail-vlan-id*

undo dot1x auth-fail vlan

Default

No 802.1X Auth-Fail VLAN exists on a port.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

authfail-vlan-id: Specifies the ID of the 802.1X Auth-Fail VLAN on the port. The value range for the VLAN ID is 1 to 4094. Make sure the VLAN has been created.

Usage guidelines

An 802.1X Auth-Fail VLAN accommodates users that have failed 802.1X authentication for any reason other than unreachable servers. Users in the Auth-Fail VLAN can access a limited set of network resources.

To delete a VLAN that has been configured as an 802.1X Auth-Fail VLAN, you must first use the **undo dot1x auth-fail vlan** command.

Examples

Configure VLAN 100 as the Auth-Fail VLAN on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] dot1x auth-fail vlan 100
```

Related commands

display dot1x

2.1.7. dot1x guest-vlan

Use **dot1x guest-vlan** to configure an 802.1X guest VLAN on a port.

Use **undo dot1x guest-vlan** to restore the default.

Syntax

dot1x guest-vlan *guest-vlan-id*

undo dot1x guest-vlan

Default

No 802.1X guest VLAN exists on a port.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

guest-vlan-id: Specifies the ID of the 802.1X guest VLAN. The value range for the VLAN ID is 1 to 4094. Make sure the VLAN has been created.

Usage guidelines

An 802.1X guest VLAN accommodates users that have not performed 802.1X authentication. In the guest VLAN, users can access a limited set of network resources, such as a software server, to download anti-virus software and system patches.

To delete a VLAN that has been configured as a guest VLAN, you must use the **undo dot1x guest-vlan** command first.

Examples

Specify VLAN 100 as the 802.1X guest VLAN on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] dot1x guest-vlan 100
```

Related commands

display dot1x

2.1.8. dot1x handshake

Use **dot1x handshake** to enable the online user handshake feature.

Use **undo dot1x handshake** to disable the online user handshake feature.

Syntax

dot1x handshake

undo dot1x handshake

Default

The online user handshake feature is enabled.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

The online user handshake feature enables the device to periodically send EAP-Request/Identity packets to the client for verifying the connectivity status of online 802.1X users. The device sets a user to the offline state if it does not receive an EAP-Response/Identity packet from the user after making the maximum attempts before the handshake timer expires. To set the handshake timer, use

the **dot1x timer handshake-period** command. To set the maximum handshake attempts, use the **dot1x retry** command.

Examples

Enable the online user handshake feature on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] dot1x handshake
```

Related commands

display dot1x

dot1x timer handshake-period

dot1x retry

2.1.9. dot1x handshake reply enable

Use **dot1x handshake reply enable** to enable the 802.1X online user handshake reply feature.

Use **undo dot1x handshake reply enable** to disable the 802.1X online user handshake reply feature.

Syntax

dot1x handshake reply enable

undo dot1x handshake reply enable

Default

The 802.1X online user handshake reply feature is disabled.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

This command enables the device to reply to 802.1X clients' EAP-Response/Identity packets with EAP-Success packets during the online handshake process.

Use this command only if 802.1X clients will go offline without receiving EAP-Success packets from the device.

Examples

Enable the 802.1X online user handshake reply feature on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] dot1x handshake reply enable
```

Related commands

dot1x handshake

2.1.10. dot1x mandatory-domain

Use **dot1x mandatory-domain** to specify a mandatory 802.1X authentication domain on a port.

Use **undo dot1x mandatory-domain** to restore the default.

Syntax

dot1x mandatory-domain *domain-name*

undo dot1x mandatory-domain

Default

No mandatory 802.1X authentication domain is specified on a port.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

domain-name: Specifies the ISP domain name, a case-insensitive string of 1 to 255 characters.

Usage guidelines

When the system authenticates an 802.1X user trying to access a port, it selects an authentication domain in the following order:

1. Mandatory domain.
2. ISP domain specified in the username.
3. Default ISP domain.

Examples

Specify **my-domain** as the mandatory authentication domain for 802.1X users on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] dot1x mandatory-domain my-domain
```

Related commands

display dot1x

2.1.11. dot1x max-user

Use **dot1x max-user** to set the maximum number of concurrent 802.1X users on a port.

Use **undo dot1x max-user** to restore the default.

Syntax

dot1x max-user *max-number*

undo dot1x max-user

Default

The maximum number of the configurable setting is 4294967295, but the number which can be used actually will be 2048.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

max-number: Specifies the maximum number of concurrent 802.1X users on a port. The value range is 1 to 4294967295.

Usage guidelines

Set the maximum number of concurrent 802.1X users on a port to prevent the system resources from being overused. When the maximum number is reached, the port denies subsequent 802.1X users.

Examples

Set the maximum number of concurrent 802.1X users to 32 on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] dot1x max-user 32
```

Related commands

display dot1x

2.1.12. dot1x multicast-trigger

Use **dot1x multicast-trigger** to enable the 802.1X multicast trigger feature.

Use **undo dot1x multicast-trigger** to disable the 802.1X multicast trigger feature.

Syntax

dot1x multicast-trigger

undo dot1x multicast-trigger

Default

The 802.1X multicast trigger feature is enabled.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

The multicast trigger feature enables the device to act as the initiator. The device periodically multicasts EAP-Request/Identity packets out of a port to detect 802.1X clients and trigger authentication. You can use the **dot1x timer tx-period** command to set the interval for sending multicast EAP-Request/Identity packets.

Examples

Enable the multicast trigger feature on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] dot1x multicast-trigger
```

Related commands

display dot1x

dot1x timer tx-period

dot1x unicast-trigger

2.1.13. dot1x port-control

Use **dot1x port-control** to set the authorization state for the port.

Use **undo dot1x port-control** to restore the default.

Syntax

dot1x port-control { **authorized-force** | **auto** | **unauthorized-force** }

undo dot1x port-control

Default

The default port authorization state is **auto**.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

authorized-force: Places the port in authorized state, enabling users on the port to access the network without authentication.

auto: Places the port initially in unauthorized state to allow only EAPOL packets to pass, and places the port in authorized state after a user passes authentication. You can use this option in most scenarios.

unauthorized-force: Places the port in unauthorized state, denying any access requests from users on the port.

Usage guidelines

You can use this command to set the port authorization state to determine whether a client is granted access to the network.

Examples

Set the authorization state of GigabitEthernet 1/0/1 to **unauthorized-force**.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] dot1x port-control unauthorized-force
```

Related commands

display dot1x

2.1.14. dot1x port-method

Use **dot1x port-method** to specify an access control method for the port.

Use **undo dot1x port-method** to restore the default.

Syntax

dot1x port-method { **macbased** | **portbased** }

undo dot1x port-method

Default

MAC-based access control applies.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

macbased: Uses MAC-based access control on the port to separately authenticate each user attempting to access the network. Using this method, when an authenticated user logs off, no other online users are affected.

portbased: Uses port-based access control on the port. Using this method, once an 802.1X user passes authentication on the port, any subsequent user can access the network through the port without authentication. When the authenticated user logs off, all other users are logged off.

Examples

Configure GigabitEthernet 1/0/1 to implement port-based access control.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] dot1x port-method portbased
```

Related commands

display dot1x

2.1.15. dot1x quiet-period

Use **dot1x quiet-period** to enable the quiet timer.

Use **undo dot1x quiet-period** to disable the quiet timer.

Syntax

dot1x quiet-period

undo dot1x quiet-period

Default

The quiet timer is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

When a client fails 802.1X authentication, the device must wait a period of time before it can process authentication requests from the client. You can use the **dot1x timer quiet-period** command to set the quiet timer.

Examples

Enable the quiet timer and set the quiet timer to 100 seconds.

```
<Switch> system-view
[Switch] dot1x quiet-period
[Switch] dot1x timer quiet-period 100
```

Related commands

display dot1x

dot1x timer

2.1.16. dot1x re-authenticate

Use **dot1x re-authenticate** to enable the 802.1X periodic reauthentication feature.

Use **undo dot1x re-authenticate** to disable the 802.1X periodic reauthentication feature.

Syntax

dot1x re-authenticate

undo dot1x re-authenticate

Default

The 802.1X periodic reauthentication feature is disabled.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

Periodic reauthentication enables the access device to periodically authenticate online 802.1X users on a port. This feature tracks the connection status of online users and updates the authorization attributes assigned by the server, such as the ACL and VLAN.

You can use the **dot1x timer reauth-period** command to configure the interval for reauthentication.

Examples

Enable the 802.1X periodic reauthentication feature on GigabitEthernet 1/0/1, and set the periodic reauthentication interval to 1800 seconds.

```
<Switch> system-view
[Switch] dot1x timer reauth-period 1800
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] dot1x re-authenticate
```

Related commands

display dot1x

dot1x timer

2.1.17. dot1x retry

Use **dot1x retry** to set the maximum number of attempts for sending an authentication request to a client.

Use **undo dot1x retry** to restore the default.

Syntax

dot1x retry *retries*

undo dot1x retry

Default

A maximum of two attempts are made to send an authentication request to a client.

Views

System view

Predefined user roles

network-admin

Parameters

retries: Specifies the maximum number of attempts for sending an authentication request to a client. The value range is 1 to 10.

Usage guidelines

The access device retransmits an authentication request to a client in any of the following situations:

- The device does not receive any responses from the client within the username request timeout interval. The timer is set by using the **dot1x timer tx-period** *tx-period-value* command for the EAP-Request/Identity packet.
- The device does not receive any responses from the client within the client timeout interval. The timer is set by using the **dot1x timer supp-timeout** *supp-timeout-value* command for the EAP-Request/MD5-Challenge packet.

The access device stops retransmitting the request, if it has made the maximum number of request transmission attempts but still received no response.

Examples

Set the maximum number of attempts to 9 for sending an authentication request to a client.

```
<Switch> system-view
[Switch] dot1x retry 9
```

Related commands

display dot1x

dot1x timer

2.1.18. dot1x timer

Use **dot1x timer** to set an 802.1X timer.

Use **undo dot1x timer** to restore the default of an 802.1X timer.

Syntax

dot1x timer { **handshake-period** *handshake-period-value* | **quiet-period** *quiet-period-value* | **reauth-period** *reauth-period-value* | **server-timeout**

server-timeout-value | **supp-timeout** *supp-timeout-value* | **tx-period** *tx-period-value* }

undo dot1x timer { **handshake-period** | **quiet-period** | **reauth-period** | **server-timeout** | **supp-timeout** | **tx-period** }

Default

The following 802.1X timers apply:

- Handshake timer: 15 seconds.
- Quiet timer: 60 seconds.
- Periodic reauthentication timer: 3600 seconds.
- Server timeout timer: 100 seconds.
- Client timeout timer: 30 seconds.
- Username request timeout timer: 30 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

handshake-period *handshake-period-value*: Specifies the handshake timer in seconds. The value range for the *handshake-period-value* argument is 5 to 1024.

quiet-period *quiet-period-value*: Specifies the quiet timer in seconds. The value range for the *quiet-period-value* argument is 10 to 120.

reauth-period *reauth-period-value*: Specifies the periodic reauthentication timer in seconds. The value range for the *reauth-period-value* argument is 60 to 7200.

server-timeout *server-timeout-value*: Specifies the server timeout timer in seconds. The value range for the *server-timeout-value* argument is 100 to 300.

supp-timeout *supp-timeout-value*: Specifies the client timeout timer in seconds. The value range for the *supp-timeout-value* argument is 1 to 120.

tx-period *tx-period-value*: Specifies the username request timeout timer in seconds. The value range for the *tx-period-value* argument is 1 to 120.

Usage guidelines

In most cases, the default settings are sufficient. You can edit the timers, depending on the network conditions.

- In a low-speed network, increase the client timeout timer.
- In a vulnerable network, set the quiet timer to a high value.
- In a high-performance network with quick authentication response, set the quiet timer to a low value.
- In a network with authentication servers of different performance, adjust the server timeout timer.

The network device uses the following 802.1X timers:

- **Handshake timer (handshake-period)**—Sets the interval at which the access device sends client handshake requests to check the online status of a client that has passed authentication. If the device does not receive a response after sending the maximum number of handshake requests, it considers that the client has logged off.

- **Quiet timer (`quiet-period`)**—Starts when a client fails authentication. The access device must wait the time period before it can process the authentication attempts from the client.
- **Periodic reauthentication timer (`reauth-period`)**—Sets the interval at which the network device periodically reauthenticates online 802.1X users. To enable 802.1X periodic reauthentication on a port, use the **`dot1x re-authenticate`** command.
- **Server timeout timer (`server-timeout`)**—Starts when the access device sends a RADIUS Access-Request packet to the authentication server. If no response is received when this timer expires, the 802.1X authentication fails.
- **Client timeout timer (`supp-timeout`)**—Starts when the access device sends an EAP-Request/MD5-Challenge packet to a client. If no response is received when this timer expires, the access device retransmits the request to the client.
- **Username request timeout timer (`tx-period`)**—Starts when the device sends an EAP-Request/Identity packet to a client in response to an authentication request. If the device does not receive a response before this timer expires, it retransmits the request. The timer also sets the interval at which the network device sends multicast EAP-Request/Identity packets to detect clients that cannot actively request authentication.

The change to the periodic reauthentication timer applies to the users that have been online only after the old timer expires. Other timer changes take effect immediately on the device.

Examples

Set the server timeout timer to 150 seconds.

```
<Switch> system-view
[Switch] dot1x timer server-timeout 150
```

Related commands

`display dot1x`

2.1.19. dot1x timer reauth-period

Use **`dot1x timer reauth-period`** to set the 802.1X periodic reauthentication timer on a port.

Use **`undo dot1x timer reauth-period`** to restore the default.

Syntax

`dot1x timer reauth-period` *`reauth-period-value`*

`undo dot1x timer reauth-period`

Default

No 802.1X periodic reauthentication timer is configured on a port. The port uses the global 802.1X periodic reauthentication timer.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

`reauth-period-value`: Specifies the 802.1X periodic reauthentication timer in seconds. The value range for the *`reauth-period-value`* argument is 60 to 7200.

Usage guidelines

The device reauthenticates online 802.1X users on a port at the specified periodic reauthentication interval when the port is enabled with periodic reauthentication. To enable periodic reauthentication on a port, use the **dot1x re-authenticate** command.

A change to the periodic reauthentication timer applies to online users only after the old timer expires.

The device selects a periodic reauthentication timer for 802.1X reauthentication in the following order:

1. Server-assigned reauthentication timer.
2. Port-specific reauthentication timer.
3. Global reauthentication timer.
4. Default reauthentication timer.

Examples

Set the 802.1X periodic reauthentication timer to 60 seconds on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] dot1x timer reauth-period 60
```

Related commands

dot1x timer

2.1.20. dot1x unicast-trigger

Use **dot1x unicast-trigger** to enable the 802.1X unicast trigger feature.

Use **undo dot1x unicast-trigger** to disable the 802.1X unicast trigger feature.

Syntax

dot1x unicast-trigger

undo dot1x unicast-trigger

Default

The 802.1X unicast trigger feature is disabled.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

The unicast trigger feature enables the access device to initiate 802.1X authentication when the device receives a data frame from an unknown source MAC address. The device sends a unicast EAP-Request/Identity packet to the unknown source MAC address. It will retransmit the packet if it does not receive any responses within a period of time (set by using the **dot1x timer tx-period** command). This process continues until the maximum number of request attempts (set by using the **dot1x retry** command) is reached.

Examples

Enable the unicast trigger feature on GigabitEthernet 1/0/1.

```
<Switch> system-view
```

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] dot1x unicast-trigger
```

Related commands

display dot1x

dot1x multicast-trigger

dot1x retry

dot1x timer

2.1.21. reset dot1x guest-vlan

Use **reset dot1x guest-vlan** to remove users from the 802.1X guest VLAN on a port.

Syntax

reset dot1x guest-vlan interface *interface-type interface-number* [**mac-address** *mac-address*]

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number.

mac-address *mac-address*: Specifies the MAC address of an 802.1X user in the guest VLAN. If you do not specify this option, the command removes all 802.1X users from the 802.1X guest VLAN on the port.

Examples

Remove the 802.1X user with MAC address 1-1-1 from the 802.1X guest VLAN on GigabitEthernet 1/0/1.

```
<Switch> reset dot1x guest-vlan interface gigabitethernet 1/0/1 mac-address 1-1-1
```

Related commands

dot1x guest-vlan

2.1.22. reset dot1x statistics

Use **reset dot1x statistics** to clear 802.1X statistics.

Syntax

reset dot1x statistics [**interface** *interface-type interface-number*]

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number. If you do not specify a port, this command clears 802.1X statistics on all ports.

Examples

Clear 802.1X statistics on GigabitEthernet 1/0/1.

```
<Switch> reset dot1x statistics interface gigabitethernet 1/0/1
```

Related commands

display dot1x

Contents

A page of this section is **9-x-x**

3. MAC authentication commands 3-1
3.1. MAC authentication commands 3-1
3.1.1. display mac-authentication 3-1
3.1.2. display mac-authentication connection 3-5
3.1.3. mac-authentication 3-7
3.1.4. mac-authentication access-user log enable 3-8
3.1.5. mac-authentication domain 3-9
3.1.6. mac-authentication guest-vlan 3-10
3.1.7. mac-authentication guest-vlan auth-period 3-10
3.1.8. mac-authentication max-user 3-11
3.1.9. mac-authentication parallel-with-dot1x 3-12
3.1.10. mac-authentication timer 3-13
3.1.11. mac-authentication timer auth-delay 3-14
3.1.12. mac-authentication user-name-format 3-15
3.1.13. reset mac-authentication guest-vlan 3-16
3.1.14. reset mac-authentication statistics 3-17

3. MAC authentication commands

3.1. MAC authentication commands

3.1.1. display mac-authentication

Use **display mac-authentication** to display MAC authentication settings and statistics.

Syntax

display mac-authentication [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number. If the specified port is not enabled with MAC authentication, this command displays only global MAC authentication information.

Usage guidelines

If you do not specify any parameters, this command displays all MAC authentication information including the global settings, port-specific settings, MAC authentication statistics, and online user statistics.

Examples

Display all MAC authentication settings and statistics.

```
<Switch> display mac-authentication
Global MAC authentication parameters:
   MAC authentication     : Enabled
   Username format        : MAC address in lowercase(xxxxxxxxxxxx)
           Username       : mac
           Password       : Not configured
   Offline detect period  : 300 s
   Quiet period           : 60 s
   Server timeout         : 100 s
   Reauth period          : 3600 s
   Authentication domain  : Not configured, use default domain
 Online MAC-auth wired users    : 1

 Silent MAC users:
          MAC address       VLAN ID  From port               Port index
          0001-0000-0001    100      GE1/0/2                21

 GigabitEthernet1/0/1  is link-up
```

```
MAC authentication         : Enabled
Carry User-IP              : Disabled
Authentication domain      : Not configured
Auth-delay timer           : Enabled
Auth-delay period          : 60 s
Periodic reauth            : Enabled
    Reauth period          : 120 s
Re-auth server-unreachable : Logoff
Guest VLAN                 : 100
Guest VLAN auth-period     : 150 s
Critical VLAN              : Not configured
Critical voice VLAN        : Disabled
Host mode                  : Multiple VLAN
Offline detection          : Enabled
Authentication order       : Parallel
Guest VSI                  : Not configured
Guest VSI auth-period      : 30 s
Critical VSI               : Not configured
Auto-tag feature           : Disabled
VLAN tag configuration ignoring : Disabled
Max online users           : 4294967295
Authentication attempts    : successful 2, failed 3
Current online users       : 1
       MAC address       Auth state
       0001-0000-0000    Authenticated
       0001-0000-0001    Unauthenticated
```

Table 3-1 Command output

Field	Description
MAC authentication	Whether MAC authentication is enabled globally.
Username format	User account type: MAC-based or shared. • If MAC-based accounts are used, this field displays the format settings for the username. For example, **MAC address in lowercase(xxxxxxxxxxxx)** indicates that the MAC address is in the hexadecimal notation without hyphens, and letters are in lower case. • If a shared account is used, this field displays **Fixed account**.
Username	Username for MAC authentication. • If MAC-based accounts are used, this field displays **mac**. The device uses the MAC address of each user as the username and password for MAC authentication. • If a shared account is used, this field displays the username of the shared account for MAC authentication users. By default, the username is **mac**.
Password	Password for MAC authentication.

Field	Description
	• If MAC-based accounts are used or if a shared account is used but no password is configured, this field displays **Not configured**. • If a shared account is used and a password is configured, this field displays a string of asterisks (******).
Offline detect period	Offline detect timer.
Quiet period	Quiet timer.
Server timeout	Server timeout timer.
Reauth period	Periodic MAC reauthentication timer in seconds.
Authentication domain	MAC authentication domain specified in system view. If no authentication domain is specified in system view, this field displays **Not configured, use default domain**.
Online MAC-auth wired users	Number of wired online MAC authentication users, including users that have passed MAC authentication and users that are performing MAC authentication.
Silent MAC users	Information about silent MAC addresses, including MAC addresses that have failed MAC authentication and MAC addresses that have been assigned the blackhole MAC attribute from the RADIUS server.
MAC address	Silent MAC address.
VLAN ID	ID of the VLAN to which the silent MAC address belongs.
From port	Name of the port that marks the MAC address as a silent MAC address.
Port index	Index of the port that marks the MAC address as a silent MAC address.
GigabitEthernet1/0/1 is link-up	Status of the link on GigabitEthernet 1/0/1. In this example, the link is up.
MAC authentication	Whether MAC authentication is enabled on the port.
Carry User-IP	Whether user IP addresses are included in MAC authentication requests.
Authentication domain	MAC authentication domain specified for the port.
Auth-delay timer	Whether MAC authentication delay is enabled on the port.
Auth-delay period	MAC authentication delay timer.
Periodic reauth	Whether periodic MAC reauthentication is enabled on the port.
Reauth period	Periodic MAC reauthentication timer on the port.
Re-auth server-unreachable	Action taken when no server is reachable for MAC reauthentication: • **Logoff**—Logs off online MAC authentication users. • **Online**—Keeps MAC authenticated users online.
Guest VLAN	MAC authentication guest VLAN configured on the port. If no MAC authentication guest VLAN is configured, this field displays **Not configured**.

Field	Description
Guest VLAN auth-period	Authentication interval for users in the MAC authentication guest VLAN on the port.
Critical VLAN	MAC authentication critical VLAN configured on the port. If no MAC authentication critical VLAN is configured, this field displays **Not configured**.
Critical voice VLAN	Whether the MAC authentication critical voice VLAN feature is enabled on the port.
Host mode	• If multi-VLAN mode is disabled, this field displays **Single VLAN**. • If multi-VLAN mode is enabled, this field displays **Multiple VLAN**.
Offline detection	Status of MAC authentication offline detection: • **Enabled**. • **Disabled**.
Authentication order	If parallel processing of MAC authentication and 802.1X authentication is disabled, this field displays **Default**. If parallel processing of MAC authentication and 802.1X authentication is enabled, this field displays **Parallel**.
Guest VSI	MAC authentication guest VSI configured on the port. If no MAC authentication guest VSI is configured, this field displays **Not configured**.
Guest VSI auth-period	Authentication interval for users in the MAC authentication guest VSI on the port.
Critical VSI	MAC authentication critical VSI configured on the port. If no MAC authentication critical VSI is configured, this field displays **Not configured**.
Auto-tag feature	This field is not supported in the current software version. Status of the authorization VLAN auto-tag feature: • **Enabled**. • **Disabled**.
VLAN tag configuration ignoring	This field is not supported in the current software version. Status of the ignore-config mode: • **Enabled**. • **Disabled**.
Max online users	Maximum number of concurrent online users allowed on the port.
Authentication attempts: successful 1, failed 0	MAC authentication statistics, including the number of successful and unsuccessful authentication attempts.
MAC address	MAC address of the online user.
Auth state	User status: • **Authenticated**—The user has passed MAC authentication. • **Unauthenticated**—The user failed MAC authentication.

3.1.2. display mac-authentication connection

Use **display mac-authentication connection** to display information about online MAC authentication users.

Syntax

display mac-authentication connection [**interface** *interface-type interface-number* | **slot** *slot-number* | **user-mac** *mac-address* | **user-name** *user-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number. If you do not specify a port, this command displays information about online MAC authentication users for all ports.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information about online MAC authentication users for all member devices.

user-mac *mac-address*: Specifies an online MAC authentication user by its MAC address. The *mac-address* argument represents the MAC address of the user, in the form of H-H-H. If you do not specify an online MAC authentication user, this command displays all online MAC authentication user information.

user-name *user-name*: Specifies an online MAC authentication user by its username. The user name is a case-sensitive string of 1 to 55 characters, and it can include the domain name. If you do not specify an online MAC authentication user, this command displays all online MAC authentication user information.

Examples

Display information about all online MAC authentication users.

```
<Switch> display mac-authentication connection
Total connections: 1

Slot ID: 1
User MAC address: 0015-e9a6-7cfe
Access interface: GigabitEthernet1/0/1
Username: ias
User access state: Successful
Authentication domain: macusers
IPv4 address: 192.168.1.1
IPv6 address: 2000:0:0:0:1:2345:6789:abcd
Initial VLAN: 1
Authorization untagged VLAN: 100
Authorization tagged VLAN: N/A
Authorization VSI: N/A
```

```
Authorization ACL ID: 3001
Authorization user profile: N/A
Authorization CAR: N/A
Termination action: Radius-request
Session timeout period: 2 s
Online from: 2013/03/02  13:14:15
Online duration: 0h 2m 15s
```

Table 3-2 Command output

Field	Description
Total connections	Total number of online MAC authentication users.
User MAC address	MAC address of the user.
Access interface	Interface through which the user accesses the device.
User access state	Access state of the user: • **Successful**—The user passes MAC authentication and comes online. • **Open**—The user uses a nonexistent username or an incorrect password to come online in open authentication mode.
Authentication domain	MAC authentication domain to which the user belongs.
IPv4 address	IPv4 address of the user. If no user IPv4 address is available, this field is not displayed.
IPv6 address	IPv6 address of the user. If no user IPv6 address is available, this field is not displayed.
Initial VLAN	VLAN that holds the user before MAC authentication.
Authorization untagged VLAN	Untagged VLAN authorized to the user.
Authorization tagged VLAN	Tagged VLAN authorized to the user.
Authorization VSI	VSI authorized to the user.
Authorization ACL ID	ACL authorized to the user. If the ACL authorization fails, this field displays **(Not effective)** after the ACL ID.
Authorization user profile	User profile authorized to the user.
Authorization CAR	Authorization CAR attributes assigned by the server. • **Average input rate**—Average rate of inbound traffic in bps. • **Peak input rate**—Peak rate of inbound traffic in bps. • **Average output rate**—Average rate of outbound traffic in bps. • **Peak output rate**—Peak rate of outbound traffic in bps. If the server does not assign the peak rates, the peak rates by default are the same as the assigned average rates. In the current software version, the device does not support exclusive assignment of peak rates from the server. If no authorization CAR attributes are assigned, this field displays **N/A**.

Field	Description
Termination action	Action attribute assigned by the server to terminate the user session: • **Default**—Logs off the online authenticated user when the session timeout timer expires. This attribute does not take effect when periodic MAC reauthentication is enabled and the periodic reauthentication timer is shorter than the session timeout timer. • **Radius-request**—Reauthenticates the online user when the session timeout timer expires, regardless of whether the periodic MAC reauthentication feature is enabled or not. If the device performs local authentication, this field displays **N/A**.
Session timeout period	Session timeout timer assigned by the server.
Online from	Time from which the MAC authentication user came online.
Online duration	Online duration of the MAC authentication user.

3.1.3. mac-authentication

Use **mac-authentication** to enable MAC authentication globally or on a port.

Use **undo mac-authentication** to disable MAC authentication globally or on a port.

Syntax

mac-authentication

undo mac-authentication

Default

MAC authentication is disabled globally or on any port.

Views

System view

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

To use MAC authentication on a port, you must enable the feature both globally and on the port.

Examples

Enable MAC authentication globally.

```
<Switch> system-view
[Switch] mac-authentication
```

Enable MAC authentication on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] mac-authentication
```

Related commands

display mac-authentication

> **NOTE:**
> QX-S5600G series can be certified up to 100PPS.

3.1.4. mac-authentication access-user log enable

Use **mac-authentication access-user log enable** to enable logging for MAC authentication users.

Use **undo mac-authentication access-user log enable** to disable logging for MAC authentication users.

Syntax

mac-authentication access-user log enable [**failed-login** | **ip-change** | **logoff** | **successful-login**] *

undo mac-authentication access-user log enable [**failed-login** | **ip-change** | **logoff** | **successful-login**] *

Default

Logging for MAC authentication users is enabled.

Views

System view

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

failed-login: Specifies logs generated for login failures of MAC authentication users.

ip-change: Logs user IP address changes.

logoff: Specifies logs generated for logoffs of MAC authentication users.

successful-login: Specifies logs generated for successful logins of MAC authentication users.

Usage guidelines

As a best practice, disable this feature to prevent excessive output of logs for MAC authentication users.

If you do not specify any parameters, this command enables all logging functions for MAC authentication users.

This feature takes effect on an interface only if you enable it both globally and on that interface.

Examples

Disable all types of MAC authentication user logging on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
```

```
[Switch-GigabitEthernet1/0/1] undo mac-authentication access-user log enable
```

Related commands

info-center source maca logfile deny (*Network Management and Monitoring Command Reference*)

3.1.5. mac-authentication domain

Use **mac-authentication domain** to specify a global or port-specific authentication domain.

Use **undo mac-authentication domain** to restore the default.

Syntax

mac-authentication domain *domain-name*

undo mac-authentication domain

Default

The system default authentication domain is used. For more information about the default authentication domain, see the **domain default enable** command in "*AAA commands*."

Views

System view

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

domain-name: Specifies the name of an ISP domain, a case-insensitive string of 1 to 255 characters.

Usage guidelines

The global authentication domain applies to all MAC authentication-enabled ports. An authentication domain specified in Layer 2 Ethernet interface view or Layer 2 aggregate interface view applies only to the port. You can specify different authentication domains on different ports.

A port chooses an authentication domain for MAC authentication users in the following order:

1. Authentication domain specified on the port.
2. Global authentication domain specified in system view.
3. Default authentication domain.

Examples

Specify ISP domain **domain1** as the global MAC authentication domain.

```
<Switch> system-view
[Switch] mac-authentication domain domain1
```

Specify ISP domain **aabbcc** as the MAC authentication domain on GigabitEthernet 1/0/1.

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] mac-authentication domain aabbcc
```

Related commands

display mac-authentication

domain default enable

3.1.6. mac-authentication guest-vlan

Use **mac-authentication guest-vlan** to configure a MAC authentication guest VLAN on a port.

Use **undo mac-authentication guest-vlan** to restore the default.

Syntax

mac-authentication guest-vlan *guest-vlan-id*

undo mac-authentication guest-vlan

Default

No MAC authentication guest VLAN exists on a port.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

guest-vlan-id: Specifies a VLAN as the MAC authentication guest VLAN. The value range for the VLAN ID is 1 to 4094. Make sure the VLAN has been created.

Usage guidelines

The MAC authentication guest VLAN accommodates users that have failed MAC authentication for any reason other than server unreachable. For example, the VLAN accommodates users for which incorrect passwords are entered. You can deploy a limited set of network resources in the MAC authentication guest VLAN. For example, a software server for downloading software and system patches.

You cannot specify a VLAN as both a super VLAN and a MAC authentication guest VLAN on a port. For more information about super VLANs, see *Layer 2—LAN Switching Configuration Guide*.

Before you delete a VLAN that has been set as a MAC authentication guest VLAN, use the **undo mac-authentication guest-vlan** command to remove the guest VLAN configuration.

Examples

Configure VLAN 100 as the MAC authentication guest VLAN on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] mac-authentication guest-vlan 100
```

Related commands

display mac-authentication

reset mac-authentication guest-vlan

3.1.7. mac-authentication guest-vlan auth-period

Use **mac-authentication guest-vlan auth-period** to set the interval at which the device authenticates users in the MAC authentication guest VLAN.

Use **undo mac-authentication guest-vlan auth-period** to restore the default.

Syntax

mac-authentication guest-vlan auth-period *period-value*

undo mac-authentication guest-vlan auth-period

Default

The device authenticates users in the MAC authentication guest VLAN every 30 seconds.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

period-value: Sets the authentication interval for users in the MAC authentication guest VLAN. The value range is 1 to 3600, in seconds.

Usage guidelines

For this command to take effect, you must use the **mac-authentication guest-vlan re-authenticate** command to enable guest VLAN reauthentication in MAC authentication.

As a best practice, set the reauthentication interval to a value greater than 30 seconds if the number of concurrent MAC authentication users on a port is likely to exceed 300.

Examples

Set the authentication interval to 150 seconds for users in the MAC authentication guest VLAN on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] mac-authentication guest-vlan auth-period 150
```

Related commands

display mac-authentication

mac-authentication guest-vlan

3.1.8. mac-authentication max-user

Use **mac-authentication max-user** to set the maximum number of concurrent MAC authentication users on a port.

Use **undo mac-authentication max-user** to restore the default.

Syntax

mac-authentication max-user *max-number*

undo mac-authentication max-user

Default

The maximum number of the configurable setting is 4294967295, but the number which can be used actually will be 2048.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

max-number: Specifies the maximum number of concurrent MAC authentication users on the port. The value range for this argument is 1 to 4294967295.

Usage guidelines

Set the maximum number of concurrent MAC authentication users on a port to prevent the system resources from being overused. When the maximum number is reached, the port denies subsequent MAC authentication users.

Examples

Configure GigabitEthernet 1/0/1 to support a maximum of 32 concurrent MAC authentication users.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] mac-authentication max-user 32
```

Related commands

display mac-authentication

3.1.9. mac-authentication parallel-with-dot1x

Use **mac-authentication parallel-with-dot1x** to enable parallel processing of MAC authentication and 802.1X authentication on a port.

Use **undo mac-authentication parallel-with-dot1x** to restore the default.

Syntax

mac-authentication parallel-with-dot1x

undo mac-authentication parallel-with-dot1x

Default

Parallel processing of MAC authentication and 802.1X authentication is disabled on a port.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

When you configure this command on a port, follow these restrictions and guidelines:

- Make sure the port meets the following requirements:
  - The port is configured with both 802.1X authentication and MAC authentication and performs MAC-based access control for 802.1X authentication.
  - The port is enabled with the 802.1X unicast trigger.
- For the port to perform MAC authentication before it is assigned to the 802.1X guest VLAN or guest VSI, use the **dot1x guest-vlan-delay new-mac** or **dot1x guest-vsi-delay new-mac** command to delay assigning the port to the 802.1X guest VLAN or guest VSI.

- Do not enable MAC authentication delay on the port. This operation will delay MAC authentication after 802.1X authentication is triggered.
- To configure both 802.1X authentication and MAC authentication on the port, use one of the following methods:
  - Enable the 802.1X and MAC authentication features separately on the port.
  - Enable port security on the port. The port security mode must be **userlogin-secure-or-mac** or **userlogin-secure-or-mac-ext**.

    For information about port security mode configuration, see port security in *Security Configuration Guide*.

Examples

Enable parallel processing of MAC authentication and 802.1X authentication on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] mac-authentication parallel-with-dot1x
```

Related commands

display mac-authentication

3.1.10. mac-authentication timer

Use **mac-authentication timer** to configure a MAC authentication timer.

Use **undo mac-authentication timer** to restore the default of a MAC authentication timer.

Syntax

mac-authentication timer { **offline-detect** *offline-detect-value* | **quiet** *quiet-value* | **reauth-period** *reauth-period-value* | **server-timeout** *server-timeout-value* }

undo mac-authentication timer { **offline-detect** | **quiet** | **reauth-period** | **server-timeout** }

Default

The following MAC authentication timers apply:

- The offline detect timer is 300 seconds.
- The quiet timer is 60 seconds.
- The global periodic MAC reauthentication timer is 3600 seconds.
- The server timeout timer is 100 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

offline-detect *offline-detect-value*: Specifies the offline detect timer in the range of 60 to 2147483647, in seconds.

quiet *quiet-value*: Specifies the quiet timer in the range of 1 to 3600, in seconds.

reauth-period *reauth-period-value*: Specifies the global periodic MAC reauthentication timer in the range of 60 to 7200, in seconds.

server-timeout *server-timeout-value*: Specifies the server timeout timer in the range of 100 to 300, in seconds.

Usage guidelines

MAC authentication uses the following timers:

- **Offline detect timer**—Sets the interval that the device waits for traffic from a user before the device regards the user as idle. The device logs off the user and requests to stop accounting for the user after the timer expires. This timer takes effect only when the MAC authentication offline detection feature is enabled.
- **Quiet timer**—Sets the interval that the device must wait before the device can perform MAC authentication for a user that has failed MAC authentication. All packets from the MAC address are dropped during the quiet time. This quiet mechanism prevents repeated authentication from affecting system performance.
- **Periodic MAC reauthentication timer**—Sets the interval at which the device reauthenticates online MAC authentication users on a port if the port is enabled with periodic MAC reauthentication. A change to the global periodic reauthentication timer applies to online users only after the old timer expires.
- **Server timeout timer**—Sets the interval that the device waits for a response from a RADIUS server before the device regards the RADIUS server unavailable. If the timer expires during MAC authentication, the user cannot access the network.

Examples

Set the server timeout timer to 150 seconds.

```
<Switch> system-view
[Switch] mac-authentication timer server-timeout 150
```

Related commands

display mac-authentication

3.1.11. mac-authentication timer auth-delay

Use **mac-authentication timer auth-delay** to configure a MAC authentication timer on a port.

Use **undo mac-authentication timer auth-delay** to restore the default of a MAC authentication timer.

Syntax

mac-authentication timer auth-delay *auth-delay-time*

undo mac-authentication timer auth-delay

Default

No MAC authentication delay timer is set on a port. MAC authentication delay is disabled. MAC authentication starts immediately after it is triggered by a user packet.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

auth-delay *auth-delay-time*: Specifies the delay time for MAC authentication in seconds. The value range is 1 to 180.

Usage guidelines

When both 802.1X authentication and MAC authentication are enabled on a port, you can delay MAC authentication so that 802.1X authentication is preferentially triggered. If no 802.1X authentication is triggered or if 802.1X authentication fails within the delay period, the port continues to process MAC authentication.

Do not set the port security mode to **mac-else-userlogin-secure** or **mac-else-userlogin-secure-ext** when you want to use MAC authentication delay. The delay does not take effect on a port in either of the two modes. For more information about port security modes, see "*Port security commands*".

Examples

Enable MAC authentication delay on GigabitEthernet 1/0/1 and set the delay time to 10 seconds.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] mac-authentication timer auth-delay 10
```

Related commands

display mac-authentication

port-security port-mode

3.1.12. mac-authentication user-name-format

Use **mac-authentication user-name-format** to configure the type of user accounts for MAC authentication users.

Use **undo mac-authentication user-name-format** to restore the default.

Syntax

mac-authentication user-name-format { **fixed** [**account** *name*] [**password** { **cipher** | **simple** } *string*] | **mac-address** [{ **with-hyphen** | **without-hyphen** } [**lowercase** | **uppercase**]] }

undo mac-authentication user-name-format

Default

Each user's MAC address is used as the username and password for MAC authentication. A MAC address is in the hexadecimal notation without hyphens, and letters are in lower case.

Views

System view

Predefined user roles

network-admin

Parameters

fixed: Uses a shared account for all MAC authentication users.

account *name*: Specifies the username for the shared account. The name is a case-sensitive string of 1 to 55 characters, excluding the at sign (@). If you do not specify a username, the default name **mac** applies.

password: Specifies the password for the shared user account.

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 63 characters. Its encrypted form is a case-sensitive string of 1 to 117 characters.

mac-address: Uses MAC-based user accounts for MAC authentication users. You can also specify the format of username and password by using the following keywords:

- **with-hyphen**: Includes hyphens in the MAC address, for example xx-xx-xx-xx-xx-xx.
- **without-hyphen**: Excludes hyphens from the MAC address, for example, xxxxxxxxxxxx.
- **lowercase**: Enters letters in lower case.
- **uppercase**: Enters letters in upper case.

Usage guidelines

If you specify the MAC-based user account, the device uses the MAC address of a user as the username and password for MAC authentication of the user. This user account type ensures high authentication security. However, you must create on the authentication server a user account for each user, using the MAC address of the user as both the username and password.

If you specify a shared user account, the device uses the specified username and password for MAC authentication of all users. Because all MAC authentication users use a single account for authentication, you only need to create one account on the authentication server. This user account type is suitable for trusted networks.

Examples

Configure a shared account for MAC authentication users, and set the username to **abc** and password to plaintext string of **xyz**.

```
<Switch> system-view
[Switch] mac-authentication user-name-format fixed account abc password simple xyz
```

Use MAC-based user accounts for MAC authentication users. Each MAC address must be in the hexadecimal notation with hyphens, and letters are in upper case.

```
<Switch> system-view
[Switch] mac-authentication user-name-format mac-address with-hyphen uppercase
```

Related commands

display mac-authentication

3.1.13. reset mac-authentication guest-vlan

Use **reset mac-authentication guest-vlan** to remove users from the MAC authentication guest VLAN on a port.

Syntax

reset mac-authentication guest-vlan interface *interface-type interface-number* [**mac-address** *mac-address*]

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number.

mac-address *mac-address*: Specifies a user by its MAC address. If you do not specify this option, the command removes all users from the MAC authentication guest VLAN on the port.

Examples

Remove the user with MAC address **1-1-1** from the MAC authentication guest VLAN on GigabitEthernet 1/0/1.

```
<Switch> reset mac-authentication guest-vlan interface gigabitethernet 1/0/1 mac-address
1-1-1
```

Related commands

display mac-authentication

mac-authentication guest-vlan

3.1.14. reset mac-authentication statistics

Use **reset mac-authentication statistics** to clear MAC authentication statistics.

Syntax

reset mac-authentication statistics [**interface** *interface-type interface-number*]

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number. If you do not specify a port, this command clears both global and port-specific MAC authentication statistics.

Examples

Clear MAC authentication statistics on GigabitEthernet 1/0/1.

```
<Switch> reset mac-authentication statistics interface gigabitethernet 1/0/1
```

Related commands

display mac-authentication

Contents

A page of this section is **9-x-x**

4. Web authentication commands ····· 4-1
4.1. Web authentication commands ····· 4-1
4.1.1. display web-auth ····· 4-1
4.1.2. display web-auth free-ip ····· 4-2
4.1.3. display web-auth server ····· 4-2
4.1.4. display web-auth user ····· 4-3
4.1.5. ip ····· 4-4
4.1.6. url ····· 4-5
4.1.7. web-auth auth-fail vlan ····· 4-6
4.1.8. web-auth domain ····· 4-7
4.1.9. web-auth enable ····· 4-8
4.1.10. web-auth free-ip ····· 4-8
4.1.11. web-auth max-user ····· 4-9
4.1.12. web-auth offline-detect ····· 4-10
4.1.13. web-auth proxy port ····· 4-11
4.1.14. web-auth server ····· 4-12

4. Web authentication commands

4.1. Web authentication commands

4.1.1. display web-auth

Use **display web-auth** to display Web authentication configuration and running status on interfaces.

Syntax

display web-auth [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays Web authentication configuration for all interfaces.

Examples

Display Web authentication configuration on GigabitEthernet 1/0/1.

```
<Switch> display web-auth interface gigabitethernet 1/0/1
 Global Web-auth parameters  :
  Proxy Port Numbers         : Not configured
  Total online web-auth users: 1
 GigabitEthernet1/0/1  is link-up
   Port role                 : Authenticator
   Web-auth domain           : my-domain
   Auth-Fail VLAN            : Not configured
   Offline-detect            : Not configured
   Max online users          : 1024
   Web-auth enable           : Enabled


  Total online web-auth users: 1
```

Table 4-1 Command output

Field	Description
Global Web-auth parameters	Global Web authentication configuration.
Proxy Port Numbers	Port numbers of the Web proxy servers.
Total online web-auth users	Total number of online Web authentication users on the device.
GigabitEthernet1/0/1 is	State of the interface:

Field	Description
link-up	• **link-up**—The interface is both administratively and physically up. • **link-down**—The interface is down.
Port role	Role of the port. The port functions only as an **Authenticator**.
Web-auth domain	ISP domain used by Web authentication.
Auth-fail VLAN	Auth-Fail VLAN for Web authentication. This field displays **Not configured** if no Auth-Fail VLAN is configured.
Offline-detect	Interval of Web authentication user detection. This field displays **Not configured** if online detection for Web authentication users is disabled.
Max online users	Maximum number of Web authentication users allowed on the interface.
Web-auth enable	State of Web authentication: • Enabled. • Disabled.
Total online web-auth users	Total number of online Web authentication users on the interface.

4.1.2. display web-auth free-ip

Use **display web-auth free-ip** to display Web authentication-free subnets.

Syntax

display web-auth free-ip

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display Web authentication-free subnets.

```
<Switch> display web-auth free-ip
       Free IP
                          : 1.1.0.0          255.255.0.0
                          : 1.2.0.0          255.255.0.0
```

Related commands

web-auth free-ip

4.1.3. display web-auth server

Use **display web-auth server** to display Web authentication server information.

Syntax

display web-auth server [*server-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

server-name: Specifies a Web authentication server name, a case-sensitive string of 1 to 32 characters. If you do not specify a Web authentication server, this command displays information about all Web authentication servers.

Examples

Display information about Web authentication server **aaa**.

```
<Switch> display web-auth server aaa
Web-auth server: aaa
  IP                       : 8.8.8.8
  Port                     : 80
  URL                      : http://8.8.8.8/portal/
  Redirect-wait-time     : 5
  URL parameters          : Not configured
```

Table 4-2 Command output

Field	Description
Web-auth server	Name of the Web authentication server.
IP	IP address of the Web authentication server.
Port	Port number of the Web authentication server.
URL	Redirection URL of the Web authentication server.
Redirect-wait-time	Time before redirecting an authenticated user to the webpage requested by the user.
URL parameters	Parameters in the redirection URL.

4.1.4. display web-auth user

Use **display web-auth user** to display information about online Web authentication users on interfaces.

Syntax

display web-auth user [**interface** *interface-type interface-number* | **slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays information about online Web authentication users on all interfaces.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays online Web authentication user information for all member devices.

Examples

Display information about online Web authentication users on GigabitEthernet 1/0/1.

```
<Switch> display web-auth user interface gigabitethernet 1/0/1
  Total online web-auth users: 1

User name: user1
  MAC address: 0000-2700-b076
  Access interface: GigabitEthernet 1/0/1
  Initial VLAN: 1
  Authorization VLAN: N/A
  Authorization ACL ID: N/A
  Authorization user profile: N/A
```

Table 4-3 Command output

Field	Description
Total online web-auth users	Total number of online Web authentication users.
User Name	Name of the online Web authentication user.
MAC address	MAC address of the online Web authentication user.
Access interface	Access interface of the online Web authentication user.
Initial VLAN	Initial VLAN of the user before the user passes Web authentication.
Authorization VLAN	Authorization VLAN ID of the online Web authentication user.
Authorization ACL ID	Authorization ACL number of the online Web authentication user.
Authorization user profile	Status of user profile of the online Web authentication user: • **N/A**—No user profile is authorized. • **Active**—The authorized user profile is applied to the user access interface successfully. • **Inactive**—The authorized user profile is not applied to the user access interface or the user profile does not exist on the device.

4.1.5. ip

Use **ip** to specify the IP address and port number for a Web authentication server.

Use **undo ip** to restore the default.

Syntax

ip *ipv4-address* **port** *port-number*

undo ip

Default

No IP address or port number is specified for a Web authentication server.

Views

Web authentication server view

Predefined user roles

network-admin

Parameters

ipv4-address: Specifies the IPv4 address of the Web authentication server. This IP address is that of a Layer 3 interface on the access device and must be routable to and from the Web authentication user.

port *port-number*: Specifies the port number of the Web authentication server, in the range of 1 to 65535.

User guidelines

As a best practice, use the IP address of a loopback interface as the IP address of the Web authentication server. A loopback interface has the following advantages:

- The status of a loopback interface is stable. This can avoid authentication page access failures caused by interface failures.
- A loopback interface does not forward received packets. This can avoid impacting system performance when there are many network access requests.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Enter the view of Web authentication server **wbs**.

```
<Switch> system-view
[Switch] web-auth server wbs
```

Specify 192.168.1.1 as the IP address and 8080 as the port number for Web authentication server **wbs**.

```
[Switch-web-auth-server-wbs] ip 192.168.1.1 port 8080
```

Related commands

url

tcp-port

4.1.6. url

Use **url** to specify the redirection URL for a Web authentication server.

Use **undo url** to restore the default.

Syntax

url *url-string*

undo url

Default

No redirection URL is specified for a Web authentication server.

Views

Web authentication server view

Predefined user roles

network-admin

Parameters

url-string: Specifies the redirection URL for the Web authentication server, a case-sensitive string of 1 to 256 characters.

Usage guidelines

The redirection URL is a URL that can be accessed through standard HTTP or HTTPS. The redirection URL should start with http:// or https://. If the redirection URL does not start with http:// or https://, the system determines that the URL begins with http://.

The IP address and port number in the URL must be the same as the IP address and port number of the Web authentication server.

Examples

Specify http://192.168.1.1/portal/ as the redirection URL for Web authentication server **wbs**.

```
<Switch> system-view
[Switch] web-auth server wbs
[Switch-web-auth-server-wbs] url http://192.168.1.1:80/portal/
```

Related commands

ip

tcp-port

4.1.7. web-auth auth-fail vlan

Use **web-auth auth-fail vlan** to specify an Auth-Fail VLAN for Web authentication.

Use **undo web-auth auth-fail vlan** to restore the default.

Syntax

web-auth auth-fail vlan *authfail-vlan-id*

undo web-auth auth-fail vlan

Default

No Auth-Fail VLAN is specified for Web authentication.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

authfail-vlan-id: Specifies the Auth-Fail VLAN ID in a range of 1 to 4094. The specified VLAN must already exist.

User guidelines

After you configure this command on an interface, users who failed Web authentication on the interface can access resources in the Auth-Fail VLAN. You must also configure the IP address of the server that provides the resources as an authentication-free IP address.

To make the Auth-Fail VLAN take effect, you must also enable MAC-based VLAN on the interface, and set the subnet of the Auth-Fail VLAN as the Web authentication-free subnet.

Because MAC-based VLAN takes effect only on Hybrid ports, Auth-Fail VLAN also takes effect only on Hybrid ports.

If a user fails Web authentication, the device maps the MAC address of the user to the Auth-Fail VLAN.

You cannot delete the VLAN that has been configured as an Auth-Fail VLAN. To delete this VLAN, first cancel the Auth-Fail VLAN configuration by using **undo web-auth auth-fail vlan** command.

If a VLAN is specified as the super VLAN, do not configure this VLAN as an Auth-Fail VLAN of an interface. If a VLAN is specified as an Auth-Fail VLAN of an interface, do not configure this VLAN as a super VLAN.

Examples

Specify VLAN 5 as Web authentication Auth-Fail VLAN on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type hybrid
[Switch-GigabitEthernet1/0/1] mac-vlan enable
[Switch-GigabitEthernet1/0/1] web-auth auth-fail vlan 5
```

Related commands

display web-auth

4.1.8. web-auth domain

Use **web-auth domain** to specify an authentication domain for Web authentication users on an interface.

Use **undo web-auth domain** to restore the default.

Syntax

web-auth domain *domain-name*

undo web-auth domain

Default

No authentication domain is specified for Web authentication users on an interface.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

domain-name: Specifies an ISP authentication domain name, a case-insensitive string of 1 to 255 characters.

User guidelines

After you configure this command, the device uses the authentication domain for authentication, authorization and accounting (AAA) of the Web authentication users on the interface.

Examples

Specify domain **my-domain** as the authentication domain of Web authentication users on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] web-auth domain my-domain
```

4.1.9. web-auth enable

Use **web-auth enable** to enable Web authentication.

Use **undo web-auth enable** to disable Web authentication.

Syntax

web-auth enable apply server *server-name*

undo web-auth enable

Default

Web authentication is disabled.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

server-name: Specifies the Web authentication server name, a case-sensitive string of 1 to 32 characters.

User guidelines

Use this command to enable Web authentication on an interface and specify a Web authentication server.

For Web authentication to operate correctly, do not enable port security or configure the port security mode on the Layer 2 Ethernet interface enabled with Web authentication.

Examples

Enable Web authentication and specify Web authentication server **wbs** on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] web-auth enable apply server wbs
```

Related commands

web-auth server

4.1.10. web-auth free-ip

Use **web-auth free-ip** to specify a Web authentication-free subnet.

Use **undo web-auth free-ip** to restore the default.

Syntax

web-auth free-ip *ip-address* { *mask-length* | *mask* }

undo web-auth free-ip { *ip-address* { *mask-length* | *mask* } | **all** }

Default

No Web-authentication-free subnets exist.

Views

System view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the Web authentication-free subnet address.

mask-length: Specifies the mask length of the Web authentication-free subnet address, in the range of 1 to 32.

mask: Specifies a mask for the Web authentication-free subnet in dotted decimal notation.

all: Specifies all Web authentication-free subnets.

User guidelines

Web authentication users can access resources in Web authentication-free subnets without being authenticated.

You can repeat this command to configure multiple Web authentication-free subnets.

Examples

Configure subnet 192.168.0.0/24 as a Web authentication-free subnet.

```
<Switch> system-view
[Switch] web-auth free-ip 192.168.0.0 24
```

4.1.11. web-auth max-user

Use **web-auth max-user** to set the maximum number of Web authentication users allowed on an interface.

Use **undo web-auth max-user** to restore the default.

Syntax

web-auth max-user *max-number*

undo web-auth max number

Default

The maximum number of Web authentication users on an interface is 1024.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

max-number: Specifies the maximum number of Web authentication users allowed on an interface. The value range for this argument is 1 to 2048.

User guidelines

If the specified maximum number is smaller than the number of current online Web authentication users on the interface, the limit can be set successfully. The limit does not impact the online Web authentication users. However, the device does not allow new Web authentication users to log in from the interface until the number drops down below the limit.

This command specifies the maximum number of only IPv4 Web authentication users.

Examples

On GigabitEthernet 1/0/1, set the maximum number of Web authentication users to 32.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] web-auth max-user 32
```

Related commands

display web-auth

4.1.12. web-auth offline-detect

Use **web-auth offline-detect** to enable online detection of Web authentication users.

Use **undo web-auth max-user** to disable online detection of Web authentication users.

Syntax

web-auth offline-detect interval *interval*

undo web-auth offline-detect interval

Default

Online detection of Web authentication users is disabled.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

interval: Specifies the Web authentication user detection interval, in the range of 60 to 65535 seconds.

User guidelines

This feature enables the device to detect packets of an online user at the specified detection interval. If no packet from the user is received within the interval, the device logs out the user and notifies the RADIUS server to stop accounting for the user.

To prevent the device from mistakenly logging out users, set the detection interval to be the same as the aging time of MAC address entries.

Examples

On GigabitEthernet 1/0/1, enable online detection of Web authentication users and set the detection interval to 3600 seconds.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] web-auth offline-detect interval 3600
```

4.1.13. web-auth proxy port

Use **web-auth proxy port** to add the port number of a Web proxy server, so that HTTP requests forwarded by the Web proxy server trigger Web authentication.

Use **undo web-auth proxy port** to delete one or all Web proxy server port numbers.

Syntax

web-auth proxy port *port number*

undo web-auth proxy port { *port-number* | **all** }

Default

No Web proxy server port numbers are configured on the device.

Views

System view

Predefined user roles

network-admin

Parameters

port number: Specifies a Web proxy server TCP port number, in the range of 1 to 65535.

all: Specifies all Web proxy server TCP port numbers.

User guidelines

By default, proxied HTTP requests cannot trigger Web authentication but are silently dropped. To allow such HTTP requests to trigger Web authentication, specify the port numbers of the Web proxy servers on the device.

You can repeat this command to add the port numbers of multiple Web proxy servers.

If a user's browser uses the Web Proxy Auto-Discovery (WPAD) protocol to discover Web proxy servers, you must perform the following tasks:

- Add the port numbers of the Web proxy servers on the device.
- Configure authentication-free rules to allow user packets destined for the IP address of the WPAD server to pass without authentication.
- For Web authentication to support Web proxy:
- You must add the port numbers of the Web proxy servers on the device.
- Users must make sure their browsers that use a Web proxy server do not use the proxy server for the listening IP address of the local portal Web service. Then, HTTP packets that the Web authentication user sends to the local portal Web service are not sent to the Web proxy server.

Examples

Add the Web proxy server TCP port number of 7777 for Web authentication.

```
<Switch> system-view
[Switch] web-auth proxy port 7777
```

4.1.14. web-auth server

Use **web-auth server** to create a Web authentication server and enter its view, or enter the view of an existing Web authentication server.

Use **undo web-auth server** to delete a Web authentication server.

Syntax

web-auth server *server-name*

undo web-auth server *server-name*

Default

No Web authentication servers exist.

Views

System view

Predefined user roles

network-admin

Parameters

server-name: Specifies a Web authentication server name, a case-sensitive string of 1 to 32 characters.

User guidelines

In Web authentication server view, you can configure the following parameters and features for the Web authentication server:

- IP address of the server.
- Redirection URL.
- Parameters to be carried in the redirection URL.

Examples

Create a Web authentication server named **wbs** and enter its view.

```
<Switch> system-view
[Switch] web-auth server wbs
[Switch-web-auth-server-wbs]
```

Related commands

web-auth enable apply server

Contents

A page of this section is **9-x-x**

5. Port security commands 5-1
5.1. Port security commands 5-1
5.1.1. display port-security 5-1
5.1.2. display port-security mac-address block 5-4
5.1.3. display port-security mac-address security 5-5
5.1.4. port-security access-user log enable 5-6
5.1.5. port-security authorization ignore 5-7
5.1.6. port-security enable 5-8
5.1.7. port-security intrusion-mode 5-8
5.1.8. port-security mac-address security 5-9
5.1.9. port-security mac-move permit 5-11
5.1.10. port-security max-mac-count 5-12
5.1.11. port-security ntk-mode 5-13
5.1.12. port-security oui 5-14
5.1.13. port-security port-mode 5-14
5.1.14. port-security timer autolearn aging 5-17
5.1.15. port-security timer disableport 5-18
5.1.16. snmp-agent trap enable port-security 5-19

5. Port security commands

5.1. Port security commands

5.1.1. display port-security

Use **display port-security** to display port security configuration, operation information, and statistics for ports.

Syntax

display port-security [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number. If you do not specify a port, this command displays port security information for all ports.

Examples

Display port security information for all ports.

```
<Switch> display port-security
Global port security parameters:
   Port security          : Enabled
   AutoLearn aging time   : 0 min
   Disableport timeout    : 20 s
   MAC move               : Denied
   Authorization fail     : Online
   NAS-ID profile         : Not configured
   Dot1x-failure trap     : Disabled
   Dot1x-logon trap       : Disabled
   Dot1x-logoff trap      : Enabled
   Intrusion trap         : Disabled
   Address-learned trap   : Enabled
   Mac-auth-failure trap  : Disabled
   Mac-auth-logon trap    : Enabled
   Mac-auth-logoff trap   : Disabled
   Open authentication    : Disabled
   OUI value list         :
    Index :  1           Value : 123401

 GigabitEthernet1/0/1 is link-up
   Port mode                     : userLogin
```

```
NeedToKnow mode                : Disabled
Intrusion protection mode      : NoAction
Security MAC address attribute
    Learning mode              : Sticky
    Aging type                 : Periodical
Max secure MAC addresses       : 32
Current secure MAC addresses   : 0
Authorization                  : Permitted
NAS-ID profile                 : Not configured
Free VLANs                     : Not configured
Open authentication           : Disabled
```

Table 5-1 Command output

Field	Description
Port security	Whether the port security feature is enabled.
AutoLearn aging time	Sticky MAC address aging timer, in minutes or seconds.
Disableport timeout	Silence period (in seconds) of the port that receives illegal packets.
MAC move	Status of MAC move: • If the feature is enabled, this field displays **Permitted**. • If the feature is disabled, this field displays **Denied**.
Authorization fail	Action to be taken for users that fail authorization: • **Online**—Allows the users to go online. • **Offline**—Logs off the users.
NAS-ID profile	NAS-ID profile applied globally.
Dot1x-failure trap	Whether SNMP notifications for 802.1X authentication failures are enabled.
Dot1x-logon trap	Whether SNMP notifications for 802.1X authentication successes are enabled.
Dot1x-logoff trap	Whether SNMP notifications for 802.1X authenticated user logoffs are enabled.
Intrusion trap	Whether SNMP notifications for intrusion protection are enabled. If they are enabled, the device sends SNMP notifications after illegal packets are detected.
Address-learned trap	Whether SNMP notifications for MAC address learning are enabled. If they are enabled, the device sends SNMP notifications after it learns a new MAC address.
Mac-auth-failure trap	Whether SNMP notifications for MAC authentication failures are enabled.
Mac-auth-logon trap	Whether SNMP notifications for MAC authentication successes are enabled.
Mac-auth-logoff trap	Whether SNMP notifications for MAC authentication user logoffs are enabled.
Open authentication	Whether global open authentication mode is enabled.
OUI value list	List of OUI values allowed for authentication.
Port mode	Port security mode:

Field	Description
	• noRestrictions. • autoLearn. • macAddressWithRadius. • macAddressElseUserLoginSecure. • macAddressElseUserLoginSecureExt. • secure. • userLogin. • userLoginSecure. • userLoginSecureExt. • macAddressOrUserLoginSecure. • macAddressOrUserLoginSecureExt. • userLoginWithOUI. For more information about port security modes, see *Security Configuration Guide*.
NeedToKnow mode	Need to know (NTK) mode: • **NeedToKnowOnly**—Allows only unicast packets with authenticated destination MAC addresses. • **NeedToKnowWithBroadcast**—Allows only unicast packets and broadcasts with authenticated destination MAC addresses. • **NeedToKnowWithMulticast**—Allows unicast packets, multicasts, and broadcasts with authenticated destination MAC addresses. • **Disabled**—NTK is disabled.
Intrusion protection mode	Intrusion protection action: • **BlockMacAddress**—Adds the source MAC address of the illegal packet to the blocked MAC address list. • **DisablePort**—Shuts down the port that receives illegal packets permanently. • **DisablePortTemporarily**—Shuts down the port that receives illegal packets for some time. • **NoAction**—Does not perform intrusion protection.
Learning mode	Secure MAC address learning mode: • **Dynamic**. • **Sticky**.
Aging type	Secure MAC address aging type: • **Periodical**—Timer aging only. • **Inactivity**—Inactivity aging feature together with the aging timer. QX-S5600G series does not support the inactivity aging.
Max secure MAC addresses	Maximum number of secure MAC addresses (or online users) that port security allows on the port.
Current secure MAC addresses	Number of secure MAC addresses stored.
Authorization	Whether the authorization information from the authentication server (RADIUS server or local device) is ignored: • **Permitted**—Authorization information from the authentication server takes effect. • **Ignored**—Authorization information from the

Field	Description
	authentication server does not take effect.
NAS-ID profile	NAS-ID profile applied to the port.
Free VLANs	VLANs in which packets will not trigger authentication. If you do not configure free VLANs, this field displays **Not configured**.
Open authentication	Whether open authentication mode is enabled on the port.

5.1.2. display port-security mac-address block

Use **display port-security mac-address block** to display information about blocked MAC addresses.

Syntax

display port-security mac-address block [**interface** *interface-type interface-number*] [**vlan** *vlan-id*] [**count**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number.

vlan *vlan-id*: Specifies a VLAN by its ID. The value range is 1 to 4094.

count: Displays only the count of the blocked MAC addresses.

Usage guidelines

If you do not specify any parameters, this command displays information about all blocked MAC addresses.

Examples

Display information about all blocked MAC addresses.

```
<Switch> display port-security mac-address block
 MAC ADDR              Port                        VLAN ID
 000f-3d80-0d2d        GE1/0/1                     30

 --- On slot 1, 1 MAC address(es) found ---

 --- 1 mac address(es) found ---
```

Display the count of all blocked MAC addresses.

```
<Switch> display port-security mac-address block count

--- On slot 1, 1 MAC address(es) found ---

--- 1 mac address(es) found ---
```

Table 5-2 Command output

Field	Description
MAC ADDR	Blocked MAC address.
Port	Port having received frames with the blocked MAC address being the source address.
VLAN ID	ID of the VLAN to which the port belongs.
number mac address(es) found	Number of blocked MAC addresses.

Related commands

port-security intrusion-mode

5.1.3. display port-security mac-address security

Use **display port-security mac-address security** to display information about secure MAC addresses.

Syntax

display port-security mac-address security [**interface** *interface-type interface-number*] [**vlan** *vlan-id*] [**count**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number.

vlan *vlan-id*: Specifies a VLAN by its ID. The value range is 1 to 4094.

count: Displays only the count of the secure MAC addresses.

Usage guidelines

Secure MAC addresses are those that are automatically learned by the port in autoLearn mode or configured by the **port-security mac-address security** command.

If you do not specify any parameters, this command displays information about all secure MAC addresses.

Examples

Display information about all secure MAC addresses.

```
<Switch> display port-security mac-address security
 MAC ADDR          VLAN ID  STATE          PORT INDEX                    AGING TIME
 0002-0002-0002    1        Security       GE1/0/1                        Not aged

 --- Number of secure MAC addresses: 1 ---
```

Display only the count of the secure MAC addresses.

```
<Switch> display port-security mac-address security count
```

```
--- Number of secure MAC addresses: 1 ---
```

Table 5-3 Command output

Field	Description
MAC ADDR	Secure MAC address.
VLAN ID	ID of the VLAN to which the port belongs.
STATE	Type of the MAC address. This field displays **Security** for a secure MAC address.
PORT INDEX	Port to which the secure MAC address belongs.
AGING TIME	Period of time before the secure MAC address ages out. • If the secure MAC address is a static MAC address, this field displays **Not aged**. • If the secure MAC address is a sticky MAC address, this field displays the remaining lifetime. If the remaining lifetime is less than 60 seconds, the lifetime is counted in seconds. If the lifetime is not less than 60 seconds, the lifetime is counted in minutes. By default, sticky MAC addresses do not age out, and this field displays **Not aged**.
Number of secure MAC addresses	Number of secure MAC addresses stored.

Related commands

port-security mac-address security

5.1.4. port-security access-user log enable

Use **port-security access-user log enable** to enable logging for port security users.

Use **undo port-security access-user log enable** to disable logging for port security users.

Syntax

port-security access-user log enable [**failed-authorization** | **mac-learning** | **violation**] *

undo port-security access-user log enable [**failed-authorization** | **mac-learning** | **violation**] *

Default

Logging is enabled for port security users.

Views

System view

Predefined user roles

network-admin

Parameters

failed-authorization: Specifies logs generated for authorization failures of 802.1X or MAC authentication users.

mac-learning: Specifies logs generated for new MAC address learning.

violation: Specifies logs generated when intrusion protection is triggered.

Usage guidelines

As a best practice, disable this feature to prevent excessive output of logs for port security users.

If you do not specify any parameters, this command enables all logging functions for port security users.

Examples

Enable logging for intrusion protection.

```
<Switch> system-view
[Switch] port-security access-user log enable violation
```

Related commands

info-center source portsec logfile deny (*Network Management and Monitoring Command Reference*)

5.1.5. port-security authorization ignore

Use **port-security authorization ignore** to configure a port to ignore the authorization information received from the authentication server (a RADIUS server or the local device).

Use **undo port-security authorization ignore** to restore the default.

Syntax

port-security authorization ignore

undo port-security authorization ignore

Default

A port uses the authorization information from the server.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

After a user passes RADIUS or local authentication, the server performs authorization based on the authorization attributes configured for the user account. For example, the server can assign a VLAN. If you do not want the port to use such authorization attributes for users, use this command to ignore the authorization information from the server.

Examples

Configure GigabitEthernet 1/0/1 to ignore the authorization information from the authentication server.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port-security authorization ignore
```

Related commands

display port-security

5.1.6. port-security enable

Use **port-security enable** to enable port security.

Use **undo port-security enable** to disable port security.

Syntax

port-security enable

undo port-security enable

Default

Port security is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

You must disable global 802.1X and MAC authentication before you enable port security on a port.

Enabling or disabling port security resets the following security settings to the default:

- 802.1X access control mode is MAC-based.
- Port authorization state is auto.

When online users are present on a port, disabling port security logs off the online users.

Examples

Enable port security.

```
<Switch> system-view
[Switch] port-security enable
```

Related commands

display port-security

dot1x

dot1x port-control

dot1x port-method

mac-authentication

5.1.7. port-security intrusion-mode

Use **port-security intrusion-mode** to configure the intrusion protection feature so the port takes the predefined actions when intrusion protection detects illegal frames on the port.

Use **undo port-security intrusion-mode** to restore the default.

Syntax

port-security intrusion-mode { **blockmac** | **disableport** | **disableport-temporarily** }

undo port-security intrusion-mode

Default

Intrusion protection is disabled.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

blockmac: Adds the source MAC addresses of illegal frames to the blocked MAC address list and discards frames with blocked source MAC addresses. This action implements illegal traffic filtering on the port. A blocked MAC address is restored to normal after being blocked for 3 minutes, which is not user configurable. To display the blocked MAC address list, use the **display port-security mac-address block** command.

disableport: Disables the port permanently upon detecting an illegal frame received on the port.

disableport-temporarily: Disables the port for a period of time whenever it receives an illegal frame. You can use the **port-security timer disableport** command to set the period.

Usage guidelines

To restore the connection of the port disabled by the intrusion protection feature, use the **undo shutdown** command.

Examples

Configure GigabitEthernet 1/0/1 to block the source MAC addresses of illegal frames after intrusion protection detects the illegal frames.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port-security intrusion-mode blockmac
```

Related commands

display port-security

display port-security mac-address block

port-security timer disableport

5.1.8. port-security mac-address security

Use **port-security mac-address security** to add a secure MAC address.

Use **undo port-security mac-address security** to remove a secure MAC address.

Syntax

In Layer 2 Ethernet interface view:

port-security mac-address security [**sticky**] *mac-address* **vlan** *vlan-id*

undo port-security mac-address security [**sticky**] *mac-address* **vlan** *vlan-id*

In system view:

port-security mac-address security [**sticky**] *mac-address* **interface** *interface-type interface-number* **vlan** *vlan-id*

undo port-security mac-address security [[*mac-address* [**interface** *interface-type interface-number*]] **vlan** *vlan-id*]

Default

No manually configured secure MAC address entries exist.

Views

System view

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

sticky: Specifies the MAC address type as sticky. If you do not specify this keyword, the command configures a static secure MAC address.

mac-address: Specifies a MAC address, in H-H-H format.

interface *interface-type interface-number*: Specifies a port by its type and number.

vlan *vlan-id*: Specifies the VLAN to which the secure MAC address belongs. The value range for the *vlan-id* argument is 1 to 4094.

Usage guidelines

Secure MAC addresses are MAC addresses configured or learned in autoLearn mode, and if saved, can survive a device reboot. You can bind a secure MAC address only to one port in a VLAN.

You can add important or frequently used MAC addresses as sticky or static secure MAC addresses to avoid the secure MAC address limit causing authentication failure. To successfully add secure MAC addresses on a port, first complete the following tasks:

- Enable port security on the port.
- Set the port security mode to autoLearn.
- Configure the port to permit packets of the specified VLAN to pass or add the port to the VLAN. Make sure the VLAN already exists.

Sticky MAC addresses can be manually configured or automatically learned in autoLearn mode. Sticky MAC addresses do not age out by default. You can use the **port-security timer autolearn aging** command to set an aging timer for the sticky MAC addresses. When the timer expires, the sticky MAC addresses are removed.

Static secure MAC addresses never age out unless you perform the following operations:

- Remove these MAC addresses by using the **undo port-security mac-address security** command.
- Change the port security mode.
- Disable the port security feature.

You cannot change the type of a secure address entry that has been added or add two entries that are identical except for their entry type. For example, you cannot add the **port-security mac-address security sticky 1-1-1 vlan 10** entry when a **port-security mac-address security 1-1-1 vlan 10** entry exists. To add the new entry, you must delete the old entry.

Examples

Enable port security, set GigabitEthernet 1/0/1 to operate in autoLearn mode, and configure the port to support a maximum number of 100 secure MAC addresses.

```
<Switch> system-view
```

```
[Switch] port-security enable
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port-security max-mac-count 100
[Switch-GigabitEthernet1/0/1] port-security port-mode autolearn
```

Specify MAC address 0001-0002-0003 in VLAN 4 as a sticky MAC address.

```
[Switch-GigabitEthernet1/0/1] port-security mac-address security sticky 0001-0002-0003
vlan 4
[Switch-GigabitEthernet1/0/1] quit
```

In system view, specify MAC address 0001-0001-0002 in VLAN 10 as a secure MAC address for GigabitEthernet 1/0/1.

```
[Switch] port-security mac-address security 0001-0001-0002 interface gigabitethernet
1/0/1 vlan 10
```

Related commands

display port-security

port-security timer autolearn aging

5.1.9. port-security mac-move permit

Use **port-security mac-move permit** to enable MAC move on the device.

Use **undo port-security mac-move permit** to disable MAC move on the device.

Syntax

port-security mac-move permit

undo port-security mac-move permit

Default

MAC move is enabled on the device.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command takes effect on both 802.1X and MAC authentication users.

MAC move allows 802.1X or MAC authenticated users to move between ports on a device. For example, if an 802.1X-authenticated user moves to another 802.1X-enabled port on the device, the authentication session is deleted from the first port. The user is reauthenticated on the new port.

If MAC move is disabled, 802.1X or MAC users authenticated on one port cannot pass authentication after they move to another port.

802.1X or MAC authenticated users cannot move between ports on a device if the number of online users on the authentication server (local or remote) has reached the upper limit.

Examples

Enable MAC move.

```
<Switch> system-view
[Switch] port-security mac-move permit
```

Related commands

display port-security

5.1.10. port-security max-mac-count

Use **port-security max-mac-count** to set the maximum number of secure MAC addresses that port security allows on a port.

Use **undo port-security max-mac-count** to restore the default.

Syntax

port-security max-mac-count *max-count* [**vlan** [*vlan-id-list*]]

undo port-security max-mac-count [**vlan** [*vlan-id-list*]]

Default

Port security does not limit the number of secure MAC addresses on a port.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

max-count: Specifies the maximum number of secure MAC addresses that port security allows on the port. The value range is 1 to 2147483647. The maximum number of the configurable setting is 2147483647, but the number which can be used actually will be 2048.

vlan [*vlan-id-list*]: Specifies a space-separated list of up to 10 VLAN items. Each VLAN item specifies a VLAN ID or a range of VLAN IDs in the form of *start-vlan-id* **to** *end-vlan-id*. The end VLAN ID cannot be smaller than the start VLAN ID. The value range for VLAN IDs is 1 to 4094. If you do not specify the **vlan** keyword, this command sets the maximum number of secure MAC addresses that port security allows on a port. If you do not specify the *vlan-id-list* argument, this command sets the maximum number of secure MAC addresses for each VLAN on the port. This option takes effect only on a port that operates in autoLearn mode.

Usage guidelines

For autoLearn mode, this command sets the maximum number of secure MAC addresses (both configured and automatically learned) on the port.

In any other mode that enables 802.1X, MAC authentication, or both, this command sets the maximum number of authenticated MAC addresses on the port. The actual maximum number of concurrent users that the port accepts equals the smaller of the following values:

- The value set by using this command.
- The maximum number of concurrent users allowed by the authentication mode in use.

For example, in userLoginSecureExt mode, if 802.1X allows more concurrent users than port security's limit on the number of MAC addresses, port security's limit takes effect.

When you configure this command, follow these guidelines and restrictions:

- Make sure the maximum number of secure MAC addresses for a VLAN is not less than the number of MAC addresses currently saved for the VLAN.
- If you execute this command multiple times to set the maximum number of secure MAC addresses for the same VLAN, the most recent configuration takes effect.

- You cannot change port security's limit on the number of MAC addresses when the port is operating in autoLearn mode.

Examples

Set the maximum number of secure MAC address port security allows on GigabitEthernet 1/0/1 to 100.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port-security max-mac-count 100
```

Related commands

display port-security

5.1.11. port-security ntk-mode

Use **port-security ntk-mode** to configure the NTK feature.

Use **undo port-security ntk-mode** to restore the default.

Syntax

port-security ntk-mode { **ntk-withbroadcasts** | **ntk-withmulticasts** | **ntkonly** }

undo port-security ntk-mode

Default

The NTK feature is not configured on a port and all frames are allowed to be sent.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

ntk-withbroadcasts: Forwards only broadcast frames and unicast frames with authenticated destination MAC addresses.

ntk-withmulticasts: Forwards only broadcast frames, multicast frames, and unicast frames with authenticated destination MAC addresses.

ntkonly: Forwards only unicast frames with authenticated destination MAC addresses.

Usage guidelines

The NTK feature checks the destination MAC addresses in outbound frames. This feature allows frames to be sent only to devices passing authentication, preventing illegal devices from intercepting network traffic.

Examples

Set the NTK mode of GigabitEthernet 1/0/1 to **ntkonly**, allowing the port to forward received packets only to devices passing authentication.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port-security ntk-mode ntkonly
```

Related commands

display port-security

5.1.12. port-security oui

Use **port-security oui** to configure an OUI value for user authentication.

Use **undo port-security oui** to delete the OUI value with the specified OUI index.

Syntax

port-security oui index *index-value* **mac-address** *oui-value*

undo port-security oui index *index-value*

Default

No OUI values are configured.

Views

System view

Predefined user roles

network-admin

Parameters

index-value: Specifies the OUI index, in the range of 1 to 16.

oui-value: Specifies an OUI string, a 48-bit MAC address in the H-H-H format. The system uses only the 24 high-order bits as the OUI value.

Usage guidelines

You can configure multiple OUI values.

An OUI, the first 24 binary bits of a MAC address, is assigned by IEEE to uniquely identify a device vendor. Use this command to allow devices of specific vendors to access the network without being authenticated. For example, you can specify the OUIs of IP phones and printers.

The OUI values configured by this command apply only to the ports operating in userLoginWithOUI mode. In userLoginWithOUI mode, a port allows only one 802.1X user and one user whose MAC address matches one of the configured OUI values.

Examples

Configure an OUI value of 000d2a, and set the index to 4.

```
<Switch> system-view
[Switch] port-security oui index 4 mac-address 000d-2a10-0033
```

Related commands

display port-security

5.1.13. port-security port-mode

Use **port-security port-mode** to set the port security mode of a port.

Use **undo port-security port-mode** to restore the default.

Syntax

```
port-security port-mode { autolearn | mac-authentication |
mac-else-userlogin-secure | mac-else-userlogin-secure-ext | secure |
userlogin | userlogin-secure | userlogin-secure-ext |
userlogin-secure-or-mac | userlogin-secure-or-mac-ext |
userlogin-withoui }

undo port-security port-mode
```

Default

A port operates in noRestrictions mode, where port security does not take effect.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

Keyword	Security mode	Description
autolearn	autoLearn	A port in this mode can learn MAC addresses. The automatically learned MAC addresses are not added to the MAC address table as dynamic MAC address. Instead, the MAC addresses are added to the secure MAC address table as secure MAC addresses. You can also configure secure MAC addresses by using the **port-security mac-address security** command. A port in autoLearn mode allows frames sourced from the following MAC addresses to pass: • Secure MAC addresses. • MAC addresses configured by using the **mac-address dynamic** and **mac-address static** commands. When the number of secure MAC addresses reaches the upper limit set by the **port-security max-mac-count** command, the port changes to **secure** mode.
mac-authentication	macAddressWithRadius	In this mode, a port performs MAC authentication for users and services multiple users.
mac-else-userlogin-secure	macAddressElseUserLoginSecure	This mode is the combination of the macAddressWithRadius and userLoginSecure modes, with MAC authentication having a higher priority. In this mode, the port allows one 802.1X authentication user and multiple MAC authentication users to log in. • Upon receiving a non-802.1X frame, a port in this mode performs only MAC authentication. • Upon receiving an 802.1X frame, the port performs MAC authentication and then, if MAC authentication fails, 802.1X authentication.

Keyword	Security mode	Description
mac-else-userlogin-secure-ext	macAddressElseUserLoginSecureExt	Same as the macAddressElseUserLoginSecure mode except that a port in this mode supports multiple 802.1X and MAC authentication users.
secure	secure	In this mode, MAC address learning is disabled on the port and you can configure MAC addresses by using the **mac-address static** and **mac-address dynamic** commands. The port permits only frames sourced from the following MAC addresses to pass: • Secure MAC addresses. • MAC addresses configured by using the **mac-address static** and **mac-address dynamic** commands.
userlogin	userLogin	In this mode, a port performs 802.1X authentication and implements port-based access control. If one 802.1X user passes authentication, all the other 802.1X users of the port can access the network without authentication.
userlogin-secure	userLoginSecure	In this mode, a port performs 802.1X authentication and implements MAC-based access control. The port services only one user passing 802.1X authentication.
userlogin-secure-ext	userLoginSecureExt	Same as the userLoginSecure mode, except that this mode supports multiple online 802.1X users.
userlogin-secure-or-mac	macAddressOrUserLoginSecure	This mode is the combination of the userLoginSecure and macAddressWithRadius modes. In this mode, the port allows one 802.1X authentication user and multiple MAC authentication users to log in. In this mode, the port performs 802.1X authentication first. By default, if 802.1X authentication fails, MAC authentication is performed. However, the port in this mode processes authentication differently when the following conditions exist: • The port is enabled with parallel processing of MAC authentication and 802.1X authentication. • The port is enabled with the 802.1X unicast trigger. • The port receives a packet from an unknown MAC address. Under such conditions, the port sends a unicast EAP-Request/Identity packet to the MAC address to initiate 802.1X authentication. After that, the port immediately processes MAC authentication without waiting for the 802.1X authentication result.
userlogin-se	macAddressOrUs	Same as the macAddressOrUserLoginSecure

Keyword	Security mode	Description
cure-or-mac-ext	erLoginSecureExt	mode, except that a port in this mode supports multiple 802.1X and MAC authentication users.
userlogin-withoui	userLoginWithOUI	Similar to the userLoginSecure mode. In addition, a port in this mode also permits frames from a user whose MAC address contains a specific OUI. In this mode, the port performs OUI check at first. If the OUI check fails, the port performs 802.1X authentication. The port permits frames that pass OUI check or 802.1X authentication.

Usage guidelines

To change the security mode for a port security enabled port, you must set the port in noRestrictions mode first. Do not change port security mode when the port has online users.

IMPORTANT:

If you are configuring the autoLearn mode, first set port security's limit on the number of secure MAC addresses by using the **port-security max-mac-count** command. You cannot change the setting when the port is operating in autoLearn mode.

When port security is enabled, you cannot enable 802.1X or MAC authentication, or change the access control mode or port authorization state. The port security automatically modifies these settings in different security modes.

As a best practice, do not enable the **mac-else-userlogin-secure** or **mac-else-userlogin-secure-ext** mode on the port where MAC authentication delay is enabled. The two modes are mutually exclusive with the MAC authentication delay feature. For more information about MAC authentication delay, see "*MAC authentication commands*".

Examples

Enable port security, and set GigabitEthernet 1/0/1 to operate in secure mode.

```
<Switch> system-view
[Switch] port-security enable
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port-security port-mode secure
```

Change the port security mode of GigabitEthernet 1/0/1 to userLogin.

```
[Switch-GigabitEthernet1/0/1] undo port-security port-mode
[Switch-GigabitEthernet1/0/1] port-security port-mode userlogin
```

Related commands

display port-security

port-security max-mac-count

5.1.14. port-security timer autolearn aging

Use **port-security timer autolearn aging** to set the secure MAC aging timer.

Use **undo port-security timer autolearn aging** to restore the default.

Syntax

port-security timer autolearn aging second *time-value*

undo port-security timer autolearn aging

Default

Secure MAC addresses do not age out.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

second *time-value*: Specifies the secure MAC aging timer. The value range for the time-value argument is 10 to 7776000 in seconds.

Usage guidelines

The timer applies to all sticky secure MAC addresses and those automatically learned by a port.

The effective aging timer varies by the aging timer setting:

- If the aging timer is set in seconds, the effective aging timer can be either of the following values:
  - The nearest multiple of 30 seconds to the configured aging timer if the configured timer is not less than 60 seconds. The effective aging timer is not less than the configured aging timer. For example, if you set the aging timer to 80 seconds, the actual aging timer that takes effect is 90 seconds.
  - The configured aging timer if the configured timer is less than 60 seconds..

A short aging time improves port access security and port resource utility but affects online user stability. Set an appropriate secure MAC address aging timer according to your device performance and the network environment.

When a short aging time (less than 60 seconds) works with inactivity aging, do not assign a large value to the maximum number of secure MAC addresses on a port. A large value in this case might affect device performance. QX-S5600G series does not support the inactivity aging.

When you configure the secure MAC address aging timer in both interface view and system view, the configuration in interface view takes priority. The actual aging timer that takes effect uses the value set in interface view.

Examples

Set the secure MAC address aging timer to 50 seconds on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port-security timer autolearn aging second 50
```

Related commands

display port-security

port-security mac-address security

5.1.15. port-security timer disableport

Use **port-security timer disableport** to set the silence period during which the port remains disabled.

Use **undo port-security timer disableport** to restore the default.

Syntax

port-security timer disableport *time-value*

undo port-security timer disableport

Default

The port silence period is 20 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

time-value: Specifies the silence period in seconds during which the port remains disabled. The value is in the range of 20 to 300.

Usage guidelines

If you configure the intrusion protection action as disabling the port temporarily, use this command to set the silence period.

Examples

Configure the intrusion protection action on GigabitEthernet 1/0/1 as disabling the port temporarily, and set the port silence period to 30 seconds.

```
<Switch> system-view
[Switch] port-security timer disableport 30
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port-security intrusion-mode disableport-temporarily
```

Related commands

display port-security

port-security intrusion-mode

5.1.16. snmp-agent trap enable port-security

Use **snmp-agent trap enable port-security** to enable SNMP notifications for port security.

Use **undo snmp-agent trap enable port-security** to disable SNMP notifications for port security.

Syntax

snmp-agent trap enable port-security [**address-learned** | **dot1x-failure** | **dot1x-logoff** | **dot1x-logon** | **intrusion** | **mac-auth-failure** | **mac-auth-logoff** | **mac-auth-logon**] *

undo snmp-agent trap enable port-security [**address-learned** | **dot1x-failure** | **dot1x-logoff** | **dot1x-logon** | **intrusion** | **mac-auth-failure** | **mac-auth-logoff** | **mac-auth-logon**] *

Default

All port security SNMP notifications are disabled.

Views

System view

Predefined user roles

network-admin

Parameters

address-learned: Specifies notifications about MAC address learning.

dot1x-failure: Specifies notifications about 802.1X authentication failures.

dot1x-logoff: Specifies notifications about 802.1X user logoffs.

dot1x-logon: Specifies notifications about 802.1X authentication successes.

intrusion: Specifies notifications about illegal frame detection.

mac-auth-failure: Specifies notifications about MAC authentication failures.

mac-auth-logoff: Specifies notifications about MAC authentication user logoffs.

mac-auth-logon: Specifies notifications about MAC authentication successes.

Usage guidelines

To report critical port security events to an NMS, enable SNMP notifications for port security. For port security event notifications to be sent correctly, you must also configure SNMP on the device. For more information about SNMP configuration, see *Network Management and Monitoring Configuration Guide*.

If you do not specify a notification, this command enables all SNMP notifications for port security.

For this command to take effect, make sure the intrusion protection feature is configured.

Examples

Enable SNMP notifications about MAC address learning.

```
<Switch> system-view
[Switch] snmp-agent trap enable port-security address-learned
```

Related commands

display port-security

port-security enable

Contents

A page of this section is **9-x-x**

6. Password control commands 6-1
6.1. Password control commands 6-1
6.1.1. display password-control 6-1
6.1.2. display password-control blacklist 6-2
6.1.3. password-control { aging | composition | history | length } enable 6-4
6.1.4. password-control aging 6-5
6.1.5. password-control alert-before-expire 6-6
6.1.6. password-control complexity 6-7
6.1.7. password-control composition 6-11
6.1.8. password-control enable 6-12
6.1.9. password-control expired-user-login 6-13
6.1.10. password-control history 6-13
6.1.11. password-control length 6-14
6.1.12. password-control login idle-time 6-16
6.1.13. password-control login-attempt 6-16
6.1.14. password-control super aging 6-18
6.1.15. password-control super composition 6-19
6.1.16. password-control super length 6-20
6.1.17. password-control update-interval 6-20
6.1.18. reset password-control blacklist 6-21
6.1.19. reset password-control history-record 6-22

6. Password control commands

6.1. Password control commands

6.1.1. display password-control

Use **display password-control** to display password control configuration.

Syntax

display password-control [**super**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

super: Displays the password control information for the super passwords. If you do not specify this keyword, the command displays the global password control configuration.

Examples

Display the global password control configuration.

```
<Switch> display password-control
 Global password control configurations:
 Password control:                       Disabled
 Password aging:                         Enabled (90 days)
 Password length:                        Enabled (10 characters)
 Password composition:                   Enabled (1 types, 1 characters per type)
 Password history:                       Enabled (max history records:4)
 Early notice on password expiration:  7 days
 Maximum login attempts:                 3
 Action for exceeding login attempts:  Lock user for 1 minutes
 Minimum interval between two updates: 24 hours
 User account idle time:                 90 days
 Logins with aged password:              3 times in 30 days
 Password complexity:                    Disabled (username checking)
                                         Disabled (repeated characters checking)
 Password change:                       Enabled (first login)
                                         Enabled (mandatory weak password change)
 All line:                               Disabled (all line blacklist)
```

Display the password control configuration for super passwords.

```
<Switch> display password-control super
 Super password control configurations:
 Password aging:                         Enabled (90 days)
 Password length:                        Enabled (10 characters)
```

```
Password composition:                Enabled (1 types, 1 characters per type)
```

Table 6-1 Command output

Field	Description
Password control	Whether the password control feature is enabled.
Password aging	Whether password expiration is enabled and, if enabled, the aging time.
Password length	Whether the minimum password length restriction feature is enabled and, if enabled, the setting.
Password composition	Whether the password composition restriction feature is enabled and, if enabled, the settings.
Password history	Whether the password history feature is enabled and, if enabled, the setting.
Early notice on password expiration	Number of days during which the user is notified of the pending password expiration.
Maximum login attempts	Allowed maximum number of consecutive failed login attempts for FTP and VTY users.
Action for exceeding login attempts	Action to be taken after a user fails to log in after the specified number of attempts.
Minimum interval between two updates	Minimum password update interval.
Logins with aged password	Number of times and maximum number of days a user can log in using an expired password.
Password complexity	Whether the following password complexity checking is enabled: • **username checking**—Checks whether a password contains the username or the reverse of the username. • **repeated characters checking**—Checks whether a password contains any character that appears consecutively three or more times.
Password change	Status of the password change at first login feature: • Enabled (first login). • Disabled (first login). • Enabled (mandatory weak password change). Disabled (mandatory weak password change). Supported from version 7.3.21 and later software.
All line	Status of the password control blacklist feature for all user line types: • Enabled (all line blacklist). Disabled (all line blacklist). Supported from version 7.3.21 and later software.

6.1.2. display password-control blacklist

Use **display password-control blacklist** to display password control blacklist information.

Syntax

display password-control blacklist [**user-name** *user-name* | **ip** *ipv4-address* | **ipv6** *ipv6-address*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

user-name *user-name*: Specifies a user by its username, a case-sensitive string of 1 to 55 characters.

ip *ipv4-address*: Specifies the IPv4 address of a user.

ipv6 *ipv6-address*: Specifies the IPv6 address of a user.

Usage guidelines

Before **Version 7.2.**18 and Version 7.2.23：

If you do not specify any parameters, this command displays information about all users in the password control blacklist.

The users' IP addresses and user accounts are added to the password control blacklist when the users fail authentication. You can use this command to view information about blacklisted FTP and virtual terminal line (VTY) users.

Users accessing the system through the console interface are not blacklisted for the following reasons:

- The system is unable to obtain the IP addresses of these users.
- These users are privileged and, therefore, relatively secure to the system.

After Version 7.3.21 :

If you do not specify any parameters, this command displays information about all users in the password control blacklist.

When the AUX or USB users fail authentication, their user accounts are added to the password control blacklist. When FTP or virtual terminal line (VTY) users fail authentication, their IP addresses and user accounts are added to the password control blacklist. You can use this command to view information about the blacklisted users.

Examples

Display password control blacklist information.

```
<Switch> display password-control blacklist
 Blacklist items matched: 2.
 Username                    IP address          Login failures   Lock flag
 abcd                        169::168:34:1       4                lock
 admin                       192.168.34.1        1                unlock
```

Table 6-2 Command output

Field	Description
Blacklist items matched	Number of blacklisted users.

Field	Description
IP address	IP address of the user.
Login failures	Number of login failures.
Lock flag	Whether the user account is locked for the user: • **unlock**—Not limited. • **lock**—Disabled temporarily or permanently, depending on the **password-control login-attempt** command.

6.1.3. password-control { aging | composition | history | length } enable

Use **password-control { aging | composition | history | length } enable** to enable the password expiration, composition restriction, history, or minimum length restriction feature.

Use **undo password-control { aging | composition | history | length } enable** to disable a password control feature.

Syntax

password-control { aging | composition | history | length } enable

undo password-control { aging | composition | history | length } enable

Default

The password control features (**aging**, **composition**, **history**, and **length**) are all enabled.

Views

System view

Predefined user roles

network-admin

Parameters

aging: Enables the password expiration feature.

composition: Enables the password composition restriction feature.

history: Enables the password history feature.

length: Enables the minimum password length restriction feature.

Usage guidelines

For a specific password control feature to take effect, make sure the global password control and the specific password control feature are both enabled. For example, if the global password control and the minimum length restriction feature are not enabled, the **password-control length** command does not take effect.

The system stops recording history passwords after you execute the **undo password-control history enable** command, but it does not delete the prior records.

If the global password control feature is enabled but the minimum password length restriction feature is disabled. A password must contain a minimum of 4 characters and a minimum of 4 characters must be different.

Examples

Enable the password control feature globally.

```
<Switch> system-view
[Switch] password-control enable
```

Enable the password composition restriction feature.

```
[Switch] password-control composition enable
```

Enable the password expiration feature.

```
[Switch] password-control aging enable
```

Enable the minimum password length restriction feature.

```
[Switch] password-control length enable
```

Enable the password history feature.

```
[Switch] password-control history enable
```

Related commands

display password-control

password-control enable

6.1.4. password-control aging

Use **password-control aging** to set the password aging time.

Use **undo password-control aging** to restore the default.

Syntax

password-control aging *aging-time*

undo password-control aging

Default

A password expires after 90 days. The password aging time for a user group equals the global setting. The password aging time for a local user equals that of the user group to which the local user belongs.

Views

System view

User group view

Local user view

Predefined user roles

network-admin

Parameters

aging-time: Specifies the password aging time in days, in the range of 1 to 365.

Usage guidelines

The aging time depends on the view:

- The time in system view has global significance and applies to all user groups.
- The time in user group view applies to all local users in the user group.
- The time in local user view applies only to the local user.

A password aging time with a smaller application scope has higher priority. The system prefers to use the password aging time in local user view for a local user.

- If no password aging time is configured for the local user, the system uses the password aging time for the user group to which the local user belongs.
- If no password aging time is configured for the user group, the system uses the global password aging time.

Examples

Globally set the passwords to expire after 80 days.

```
<Switch> system-view
[Switch] password-control aging 80
```

Set the passwords for user group **test** to expire after 90 days.

```
[Switch] user-group test
[Switch-ugroup-test] password-control aging 90
[Switch-ugroup-test] quit
```

Set the password for device management user **abc** to expire after 100 days.

```
[Switch] local-user abc class manage
[Switch-luser-manage-abc] password-control aging 100
```

Related commands

display local-user

display password-control

display user-group

password-control aging enable

6.1.5. password-control alert-before-expire

Use **password-control alert-before-expire** to set the number of days before a user's password expires during which the user is notified of the pending password expiration.

Use **undo password-control alert-before-expire** to restore the default.

Syntax

password-control alert-before-expire *alert-time*

undo password-control alert-before-expire

Default

The default is 7 days.

Views

System view

Predefined user roles

network-admin

Parameters

alert-time: Specifies the number of days before a user password expires during which the user is notified of the pending password expiration. The value range is 1 to 30.

Usage guidelines

This command is effective only for non-FTP users. FTP users can only have their passwords changed by the administrator.

Examples

Configure the device to notify a user about pending password expiration 10 days before the user's password expires.

```
<Switch> system-view
[Switch] password-control alert-before-expire 10
```

Related commands

display password-control

6.1.6. password-control blacklist all-line

> 🕮 **MEMO:**
>
> **password-control blacklist all-line** command is supported from later software, including Version 7.3.21.

Use **password-control blacklist all-line** to enable the password control blacklist feature for all user line types.

Use **undo password-control blacklist all-line** to disable the password control blacklist feature for all user line types.

Syntax

password-control blacklist all-line

undo password-control blacklist all-line

Default

The password control blacklist feature is disabled for all user line types.

Views

System view

Predefined user roles

network-admin

Usage guidelines

By default, the password control blacklist feature is enabled only for FTP and VTY users when you enable the global password control feature. To enable the password control blacklist feature for login users on all user lines (AUX, VTY, and USB lines), you must also execute this command. For more information about user lines, see login management configuration in in *Fundamentals Configuration Guide*.

With this feature enabled, the number of consecutive login failures on the same user account is accumulated for users on AUX and USB lines. If the number reaches the limit for console, AUX, TTY, and USB users, the system adds the user account to the blacklist and takes corresponding action.

Use **password-control login-attempt** to configure the maximum number of consecutive login failures and the action to be taken when the maximum number is reached.

Examples

Enable the password control blacklist feature for all user line types.

```
<Sysname> system-view
[Sysname] password-control blacklist all-line
```

Related commands

display password-control

display password-control blacklist

password-control enable

password-control login-attempt

6.1.7. password-control change-password first-login enable

> 🕮 **MEMO:**
>
> **password-control change-password first-login enable** command is supported from later software, including Version 7.3.21.

Use **password-control change-password first-login enable** to enable the password change at first login feature.

Use **undo password-control change-password first-login enable** to disable the password change at first login feature.

Syntax

password-control change-password first-login enable

undo password-control change-password first-login enable

Default

The password change at first login feature is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

For the password change at first login feature to take effect, make sure the global password control and password change features are both enabled.

In FIPS mode, the password change at first login feature cannot be disabled.

Examples

Enable password change at first login.

```
<Sysname> system-view
[Sysname] password-control change-password first-login enable
```

Related commands

display password-control

password-control enable

6.1.8. password-control change-password weak-password enable

> 🕮 **MEMO:**
>
> **password-control change-password weak-password enable** command is supported from later software, including Version 7.3.21.

Use **password-control change-password weak-password enable** to enable mandatory weak password change.

Use **undo password-control change-password weak-password enable** to disable mandatory weak password change.

Syntax

password-control change-password weak-password enable

undo password-control change-password weak-password enable

Default

The mandatory weak password change feature is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

The system checks for weak login passwords for Telnet, SSH, HTTP, or HTTPS device management users. A password is weak if it does not meet the following requirements:

- Password composition restriction.
- Minimum password length restriction.
- Cannot contain the username or the reverse letters of the username.

By default, the system displays a message about a weak password but does not force the user to change it. To improve the device security, you can enable the mandatory weak password change feature, which forces the users to change the identified weak passwords. The users can log in to the device only after their passwords meet the password requirements.

To view the password composition restriction and the minimum password length restriction, use the **display password-control** command. To change the password composition restriction and minimum password length, use the **password-control composition** and **password-control length** commands, respectively.

Examples

Enable the mandatory weak password change feature.

```
<Sysname> system-view
[Sysname] password-control change-password weak-password enable
```

Related commands

display password-control

password-control { **aging** | **composition** | **history** | **length** }

password-control complexity

password-control composition

password-control length

password-control enable

6.1.9. password-control complexity

Use **password-control complexity** to configure the password complexity checking policy.

Use **undo password-control complexity** to remove a password complexity checking item.

Syntax

password-control complexity { **same-character** | **user-name** } **check**

undo password-control complexity { **same-character** | **user-name** } **check**

Default

The global password complexity checking policy is that both username checking and repeated character checking are disabled. The password complexity checking policy for a user group equals the global setting. The password complexity checking policy for a local user equals that of the user group to which the local user belongs.

Views

System view

User group view

Local user view

Predefined user roles

network-admin

Parameters

same-character: Refuses a password that contains a minimum of three consecutive identical characters. For example, the password **aaabc** is not complex enough.

user-name: Refuses a password that contains the username or the reverse of the username. For example, if the username is **123**, a password such as **abc123** or **321df** is not complex enough.

Usage guidelines

The password complexity checking policy depends on the view:

- The policy in system view has global significance and applies to all user groups.
- The policy in user group view applies to all local users in the user group.
- The policy in local user view applies only to the local user.

A password complexity checking policy with a smaller application scope has higher priority. The system prefers to use the password complexity checking policy in local user view for a local user.

- If no policy is configured for the local user, the system uses the policy for the user group to which the local user belongs.
- If no policy is configured for the user group, the system uses the global policy.

You can enable both username checking and repeated character checking.

Examples

Configure the password complexity checking policy, refusing any password that contains the username or the reverse of the username.

```
<Switch> system-view
```

```
[Switch] password-control complexity user-name check
```

Related commands

display local-user

display password-control

display user-group

6.1.10. password-control composition

Use **password-control composition** to configure the password composition policy.

Use **undo password-control composition** to restore the default.

Syntax

password-control composition type-number *type-number* [**type-length** *type-length*]

undo password-control composition

Default

The password using the global composition policy must contain a minimum of one character type and a minimum of one character for each type.

The password composition policy for a user group is the same as the global policy. The password composition policy for a local user is the same as that of the user group to which the local user belongs.

Views

System view

User group view

Local user view

Predefined user roles

network-admin

Parameters

type-number *type-number*: Specifies the minimum number of character types that a password must contain. The value range for the *type-number* argument is 1 to 4.

type-length *type-length*: Specifies the minimum number of characters that are from each type in the password. The value range for the *type-length* argument is 1 to 63.

Usage guidelines

The password composition policy depends on the view:

- The policy in system view has global significance and applies to all user groups.
- The policy in user group view applies to all local users in the user group.
- The policy in local user view applies only to the local user.

A password composition policy with a smaller application scope has higher priority. The system prefers to use the password composition policy in local user view for a local user.

- If no policy is configured for the local user, the system uses the policy for the user group to which the local user belongs.
- If no policy is configured for the user group, the system uses the global policy.

The product of the minimum number of character types and minimum number of characters for each type must be smaller than the maximum length of passwords.

Examples

Specify that all passwords must each contain a minimum of four character types and a minimum of five characters for each type.

```
<Switch> system-view
[Switch] password-control composition type-number 4 type-length 5
```

Specify that passwords in user group **test** must contain a minimum of four character types and a minimum of five characters for each type.

```
[Switch] user-group test
[Switch-ugroup-test] password-control composition type-number 4 type-length 5
[Switch-ugroup-test] quit
```

Specify that the password of device management user **abc** must contain a minimum of four character types and a minimum of five characters for each type.

```
[Switch] local-user abc class manage
[Switch-luser-manage-abc] password-control composition type-number 4 type-length 5
```

Related commands

display local-user

display password-control

display user-group

password-control composition enable

6.1.11. password-control enable

Use **password-control enable** to enable the password control feature globally.

Use **undo password-control enable** to disable the password control feature globally.

Syntax

password-control enable

undo password-control enable

Default

The password control feature is disabled globally.

Views

System view

Predefined user roles

network-admin

Usage guidelines

A specific password control feature takes effect only after the global password control feature is enabled.

After the global password control feature is enabled, you cannot display the password and super password configurations for device management users by using the corresponding **display** commands. The configuration for network access user passwords can be displayed. The first password configured for device management users must contain a minimum of four different characters.

Examples

Enable the password control feature globally.

```
<Switch> system-view
[Switch] password-control enable
```

Related commands

display password-control

password-control { **aging** | **composition** | **history** | **length** } **enable**

6.1.12. password-control expired-user-login

Use **password-control expired-user-login** to set the maximum number of days and maximum number of times that a user can log in after the password expires.

Use **undo password-control expired-user-login** to restore the defaults.

Syntax

password-control expired-user-login delay *delay* **times** *times*

undo password-control expired-user-login

Default

A user can log in three times within 30 days after the password expires.

Views

System view

Predefined user roles

network-admin

Parameters

delay *delay*: Specifies the maximum number of days during which a user can log in using an expired password. The value range for the *delay* argument is 1 to 90.

times *times*: Specifies the maximum number of times a user can log in after the password expires. The value range is 0 to 10. To deny users to log in after the password expires, set the value to 0.

Usage guidelines

This command is effective only on non-FTP login users. An FTP user cannot continue to log in after its password expires.

Examples

Allow a user to log in five times within 60 days after the password expires.

```
<Switch> system-view
[Switch] password-control expired-user-login delay 60 times 5
```

Related commands

display password-control

6.1.13. password-control history

Use **password-control history** to set the maximum number of history password records for each user.

Use **undo password-control history** to restore the default.

Syntax

password-control history *max-record-number*

undo password-control history

Default

The maximum number of history password records for each user is 4.

Views

System view

Predefined user roles

network-admin

Parameters

max-record-number: Specifies the maximum number of history password records for each user. The value range is 2 to 15.

Usage guidelines

When the number of history password records reaches the maximum number, the subsequent history record overwrites the earliest one.

The system stops recording passwords after you execute the **undo password-control history enable** command, but it does not delete the prior records.

To delete the existing records, use one of the following methods:

- Use the **undo password-control enable** command to disable the password control feature globally.
- Use the **reset password-control history-record** command to clear the passwords manually.

Examples

Set the maximum number of history password records for each user to 10.

```
<Switch> system-view
[Switch] password-control history 10
```

Related commands

display password-control

password-control history enable

reset password-control blacklist

6.1.14. password-control length

Use **password-control length** to set the minimum password length.

Use **undo password-control length** to restore the default.

Syntax

password-control length *length*

undo password-control length

Default

The global minimum password length is 10 characters.

The minimum password length for a user group equals the global setting. The minimum password length for a local user equals that of the user group to which the local user belongs.

Views

System view

User group view

Local user view

Predefined user roles

network-admin

Parameters

length: Specifies the minimum password length in characters. The value range for this argument is 4 to 32.

Usage guidelines

The minimum length setting depends on the view:

- The setting in system view has global significance and applies to all user groups.
- The setting in user group view applies to all local users in the user group.
- The setting in local user view applies only to the local user.

A minimum password length with a smaller application scope has higher priority. The system prefers to use the minimum password length in local user view for a local user.

- If no minimum password length is configured for the local user, the system uses the minimum password length for the user group to which the local user belongs.
- If no minimum password length is configured for the user group, the system uses the global minimum password length.

Examples

Set the global minimum password length to 16 characters.

```
<Switch> system-view
[Switch] password-control length 16
```

Set the minimum password length to 16 characters for the user group **test**.

```
[Switch] user-group test
[Switch-ugroup-test] password-control length 16
[Switch-ugroup-test] quit
```

Set the minimum password length to 16 characters for the device management user **abc**.

```
[Switch] local-user abc class manage
[Switch-luser-manage-abc] password-control length 16
```

Related commands

display local-user

display password-control

display user-group

password-control length enable

6.1.15. password-control login idle-time

Use **password-control login idle-time** to set the maximum account idle time.

Use **undo password-control login idle-time** to restore the default.

Syntax

password-control login idle-time *idle-time*

undo password-control login idle-time

Default

The maximum account idle time is 90 days.

Views

System view

Predefined user roles

network-admin

Parameters

idle-time: Specifies the maximum account idle time in days. The value range is 0 to 365. 0 means no restriction for account idle time.

Usage guidelines

If a user account is idle for this period of time, the account becomes invalid and can no longer be used to log in to the device.

Examples

Set the maximum account idle time to 30 days.

```
<Switch> system-view
[Switch] password-control login idle-time 30
```

Related commands

display password-control

6.1.16. password-control login-attempt

Use **password-control login-attempt** to configure the login attempt limit. The settings include the maximum number of consecutive login failures and the action to be taken when the maximum number is reached.

Use **undo password-control login-attempt** to restore the default.

Syntax

password-control login-attempt *login-times* [**exceed** { **lock** | **lock-time** *time* | **unlock** }]

undo password-control login-attempt

Default

The global login-attempt settings:

- The maximum number of consecutive login failures is 3.
- The locking period is 1 minute.

The login-attempt settings for a user group equal the global settings.

The login-attempt settings for a local user equal those for the user group to which the local user belongs.

Views

System view

User group view

Local user view

Predefined user roles

network-admin

Parameters

login-times: Specifies the maximum number of consecutive login failures. The value range is 2 to 10.

exceed: Specifies an action to be taken for the user who fails to log in after making the maximum number of attempts.

- **lock**: Disables the user account permanently.
- **lock-time** *time*: Disables the user account for a period of time. The user can uses this user account when the timer expires. The value range for the *time* argument is 1 to 360 minutes.
- **unlock**: Allows the user account to continue using this account to perform login attempts.

Usage guidelines

The login-attempt policy depends on the view:

- The policy in system view has global significance and applies to all user groups.
- The policy in user group view applies to all local users in the user group.
- The policy in local user view applies only to the local user.

A login-attempt policy with a smaller application scope has higher priority. The system prefers to use the login-attempt policy in local user view for a local user.

- If no policy is configured for the local user, the system uses the policy for the user group to which the local user belongs.
- If no policy is configured for the user group, the system uses the global policy.

If an FTP or VTY user fails to log in, the system adds the user account and the user's IP address to the password control blacklist. When the maximum number of consecutive login failures is reached, the login attempt limit feature is triggered.

Whether a blacklisted user and user account are locked depends on the locking setting:

- If a user account is permanently locked for a user, the user cannot use this account unless this account is removed from the password control blacklist. To remove the user account, use the **reset password-control blacklist** command.
- To use a temporarily locked user account, the user can perform either of the following tasks:
  - Wait until the locking timer expires.
  - Remove the user account from the password control blacklist.
- If the user account and the user are blacklisted but not locked, the user can continue using this account to log in. The account and the user's IP address are removed from the password control blacklist when the user uses the account to successfully log in to the device.

NOTE:

This account is locked only for this user. Other users can still use this account, and the blacklisted user can use other user accounts.

The **password-control login-attempt** command takes effect immediately after being executed, and can affect the users already in the password control blacklist.

Examples

Allow a maximum of four consecutive login failures on a user account, and disable the user account if the limit is reached.

```
<Switch> system-view
[Switch] password-control login-attempt 4 exceed lock
```

Use the user account **test** to log in to the device, and enter incorrect password for four times.

Display the password control blacklist. The output shows that the user account is on the blacklist, and its status is **lock**.

```
[Switch] display password-control blacklist

 Username: test
    IP: 192.168.44.1        Login failures: 4      Lock flag: lock

 Blacklist items matched: 1.
```

Verify that the user at 192.168.44.1 cannot use this user account to log in.

Allow a maximum of two consecutive login failures on a user account, and disable the account for 3 minutes if the limit is reached.

```
<Switch> system-view
[Switch] password-control login-attempt 2 exceed lock-time 3
```

Use the user account **test** to log in to the device, and enter incorrect password for two attempts.

Display the password control blacklist. The output shows that the user account is on the blacklist and its status is **lock**.

```
[Switch] display password-control blacklist

 Username: test
    IP: 192.168.44.1        Login failures: 2      Lock flag: lock

 Blacklist items matched: 1.
```

Verify that after 3 minutes, the user account is removed from the password control blacklist and the user at 192.168.44.1 can use this account.

Related commands

display local-user

display password-control

display password-control blacklist

display user-group

reset password-control blacklist

6.1.17. password-control super aging

Use **password-control super aging** to set the aging time for super passwords.

Use **undo password-control super aging** to restore the default.

Syntax

password-control super aging *aging-time*

undo password-control super aging

Default

A super password expires after 90 days.

Views

System view

Predefined user roles

network-admin

Parameters

aging-time: Specifies the super password aging time in days, in the range of 1 to 365.

Examples

Set the super passwords to expire after 10 days.

```
<Switch> system-view
[Switch] password-control super aging 10
```

Related commands

display password-control

password-control aging

6.1.18. password-control super composition

Use **password-control super composition** to configure the composition policy for super passwords.

Use **undo password-control super composition** to restore the default.

Syntax

password-control super composition type-number *type-number* [**type-length** *type-length*]

undo password-control super composition

Default

A super password must contain a minimum of one character type and a minimum of one character for each type.

Views

System view

Predefined user roles

network-admin

Parameters

type-number *type-number*: Specifies the minimum number of character types that a super password must contain. The value range for the *type-number* argument is 1 to 4.

type-length *type-length*: Specifies the minimum number of characters that are from each character type. The value range for the *type-length* argument is 1 to 63.

Usage guidelines

The product of the minimum number of character types and minimum number of characters for each type must be smaller than the maximum length of the super password.

Examples

Specify that a super password must contain a minimum of four character types and a minimum of five characters for each type.

```
<Switch> system-view
[Switch] password-control super composition type-number 4 type-length 5
```

Related commands

display password-control

password-control composition

6.1.19. password-control super length

Use **password-control super length** to set the minimum length for super passwords.

Use **undo password-control super length** to restore the default.

Syntax

password-control super length *length*

undo password-control super length

Default

The minimum super password length is 10 characters.

Views

System view

Predefined user roles

network-admin

Parameters

length: Specifies the minimum length of super passwords in characters. The value range for this argument is 4 to 63.

Examples

Set the minimum length of super passwords to 16 characters.

```
<Switch> system-view
[Switch] password-control super length 16
```

Related commands

display password-control

password-control length

6.1.20. password-control update-interval

Use **password-control update-interval** to set the minimum password update interval, which is the minimum interval at which users can change their passwords.

Use **undo password-control update-interval** to restore the default.

Syntax

password-control update-interval *interval*

undo password-control update-interval

Default

The minimum password update interval is 24 hours.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the minimum password update interval in hours, in the range of 0 to 168. 0 means no requirements for password update interval.

Usage guidelines

The set minimum interval is not effective on a user who is prompted to change the password at the first login or after the password expires.

Examples

Set the minimum password update interval to 36 hours.

```
<Switch> system-view
[Switch] password-control update-interval 36
```

Related commands

display password-control

6.1.21. reset password-control blacklist

Use **reset password-control blacklist** to remove blacklisted users.

Syntax

reset password-control blacklist [**user-name** *user-name*]

Views

User view

Predefined user roles

network-admin

Parameters

user-name *user-name*: Specifies the username of a user account to be removed from the password control blacklist. The username is a case-sensitive string of 1 to 55 characters.

Usage guidelines

You can use this command to remove a user account that is blacklisted due to excessive login failures. Then the blacklisted user can use this user account to log in.

Examples

Remove the user account named **test** from the password control blacklist.

```
<Switch> reset password-control blacklist user-name test
```

```
Are you sure to delete the specified user in blacklist? [Y/N]:
```

Related commands

display password-control blacklist

6.1.22. reset password-control history-record

Use **reset password-control history-record** to delete history password records.

Syntax

reset password-control history-record [**super** [**role** *role name*] | **user-name** *user-name*]

Views

User view

Predefined user roles

network-admin

Parameters

super: Deletes the history records of the specified super password or all super passwords.

role *role name*: Specifies a user role name, a case-sensitive string of 1 to 63 characters. If you do not specify this option, the command deletes the history records of all super passwords.

user-name *user-name*: Specifies the username of the user whose password records are to be deleted. The *user-name* argument is a case-sensitive string of 1 to 55 characters.

Usage guidelines

If you do not specify any parameters, this command deletes the history password records of all local users.

Examples

Clear the history password records of all local users.

```
<Switch> reset password-control history-record
Are you sure to delete all local user's history records? [Y/N]:y
```

Related commands

password-control history

Contents

A page of this section is **9-x-x**

7. Public key management commands 7-1
7.1. Public key management commands 7-1
7.1.1. display public-key local public 7-1
7.1.2. display public-key peer 7-4
7.1.3. peer-public-key end 7-5
7.1.4. public-key local create 7-6
7.1.5. public-key local destroy 7-9
7.1.6. public-key local export dsa 7-10
7.1.7. public-key local export rsa 7-12
7.1.8. public-key peer 7-14
7.1.9. public-key peer import sshkey 7-14

7. Public key management commands

7.1. Public key management commands

7.1.1. display public-key local public

Use **display public-key local public** to display local public keys.

Syntax

display public-key local { **dsa** | **rsa** } **public** [**name** *key-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

dsa: Specifies the DSA key pair type.

rsa: Specifies the RSA key pair type.

name *key-name*: Specifies a local key pair by its name, a case-insensitive string of 1 to 64 characters. Valid characters are letters, digits, and hyphens (-). If you do not specify a key pair, this command displays the public keys of all local key pairs of the specified type.

Usage guidelines

You can copy and distribute the public key of a local key pair to peer devices.

You cannot display a host public key that has the default key pair name by specifying the **name** *key-name* option. To view a host public key that has the default key pair name, display all local public keys by using this command without specifying a key pair name.

Examples

Display all local RSA public keys.

```
<Switch> display public-key local rsa public

=============================================
Key name: hostkey (default)
Key type: RSA
Time when key pair created: 15:40:48 2011/05/12
Key code:
   30819F300D06092A864886F70D010101050003818D0030818902818100DAA4AAFEFE04C2C9
   667269BB8226E26331E30F41A8FF922C7338208097E84332610632B49F75DABF6D871B80CE
   C1BA2B75020077C74745C933E2F390DC0B39D35B88283D700A163BB309B19F8F87216A44AB
   FBF6A3D64DEB33E5CEBF2BCF26296778A26A84F4F4C5DBF8B656ACFA62CD96863474899BC1
   2DA4C04EF5AE0835090203010001
=============================================
Key name: serverkey (default)
```

```
Key type: RSA
Time when key pair created: 15:40:48 2011/05/12
Key code:
   307C300D06092A864886F70D0101010500036B003068026100CAB4CACCA16442AD5F453442
   762F03897E0D494FEDE69224F5C051A441D290976733A278C9F0C0F5A198E66143EAB54A64
   DB608269CAE844B1E7CC64AD7E808972E7CF887F3B657F056E7930FC84FBF1AD83A01CC47E
   9D85C13413996ECD093B0203010001
=============================================
Key name: rsa1
Key type: RSA
Time when key pair created: 15:42:26 2011/05/12
Key code:
   30819F300D06092A864886F70D010101050003818D003081890281810 0DEBC46F217DDF11D
   426E7095AA45CD6BF1F87343D952569AC223A01365E0D8C91D49D347C143C5D8FAADA896AA
   1A827E580F2502F1926F52197230E1DE391A64015C43DD79DC4E9E171BAEA1DEB4C71DAED7
   9A6EDFD460D8945D27D39B7C9822D56AEA5B7C2CCFF1B6BC524AD498C3B87D4BD6EB36AF03
   92D8C6D940890BF4290203010001
```

Display all local DSA public keys.

```
<Switch> display public-key local dsa public

=============================================
Key name: dsakey (default)
Key type: DSA
Time when key pair created: 15:41:37 2011/05/12
Key code:
   308201B73082012C06072A8648CE3804013082011F02818100D757262C4584C44C211F18BD
   96E5F061C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE65BE6C265854889DC1E
   DBD13EC8B274DA9F75BA26CCB987723602787E922BA84421F22C3C89CB9B06FD60FE01941D
   DD77FE6B12893DA76EEBC1D128D97F0678D7722B5341C8506F358214B16A2FAC4B36895038
   7811C7DA33021500C773218C737EC8EE993B4F2DED30F48EDACE915F0281810082269009E1
   4EC474BAF2932E69D3B1F18517AD9594184CCDFCEAE96EC4D5EF93133E84B47093C52B20CD
   35D02492B3959EC6499625BC4FA5082E22C5B374E16DD00132CE71B020217091AC717B6123
   91C76C1FB2E88317C1BD8171D41ECB83E210C03CC9B32E810561C21621C73D6DAAC028F4B1
   585DA7F42519718CC9B09EEF038184000 2818041912CE34D12BCD2157E7AB1C2F03B3EF395
   100F3DB4A9E2FDFE860C1BD663D676438F7DA40A9406D61CA9079AF13E330489F1C76785DE
   52DA649AC8BC04B6D39CD7C52CD0A14F75F7491A91D31D6AC22340B5981B27A915CDEC4F09
   887E541EC1E5302D500F68E7AC29A084463C60F9EE266985A502FC92193E1CF4D265C4BA
=============================================
Key name: dsa1
Key type: DSA
Time when key pair created: 15:35:42 2011/05/12
Key code:
   308201B83082012C06072A8648CE3804013082011F02818100D757262C4584C44C211F18BD
   96E5F061C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE65BE6C265854889DC1E
   DBD13EC8B274DA9F75BA26CCB987723602787E922BA84421F22C3C89CB9B06FD60FE01941D
   DD77FE6B12893DA76EEBC1D128D97F0678D7722B5341C8506F358214B16A2FAC4B36895038
   7811C7DA33021500C773218C737EC8EE993B4F2DED30F48EDACE915F0281810082269009E1
```

```
   4EC474BAF2932E69D3B1F18517AD9594184CCDFCEAE96EC4D5EF93133E84B47093C52B20CD
   35D02492B3959EC6499625BC4FA5082E22C5B374E16DD00132CE71B020217091AC717B6123
   91C76C1FB2E88317C1BD8171D41ECB83E210C03CC9B32E810561C21621C73D6DAAC028F4B1
   585DA7F42519718CC9B09EEF0381850002818100A1E456C8DA2AD1BB83B1BDF2A1A6B5A6E8
   3642B460402445DA7E4036715F468F76655E114D460B7112F57143EE020AEF4A5BFAD07B74
   0FBCB1C64DA8A2BCE619283421445EEC77D3CF0D11866E9656AD6511F4926F8376967B0AB7
   15F9FB7B514BC1174155DD6E073B1FCB3A2749E6C5FEA81003E16729497D0EAD9105E3E76A
```

Display the public key of the local RSA key pair **rsa1**.

```
<Switch> display public-key local rsa public name rsa1

=============================================
Key name: rsa1
Key type: RSA
Time when key pair created: 15:42:26 2011/05/12
Key code:
   30819F300D06092A864886F70D010101050003818D0030818902818100DEBC46F217DDF11D
   426E7095AA45CD6BF1F87343D952569AC223A01365E0D8C91D49D347C143C5D8FAADA896AA
   1A827E580F2502F1926F52197230E1DE391A64015C43DD79DC4E9E171BAEA1DEB4C71DAED7
   9A6EDFD460D8945D27D39B7C9822D56AEA5B7C2CCFF1B6BC524AD498C3B87D4BD6EB36AF03
   92D8C6D940890BF4290203010001
```

Display the public key of the local DSA key pair **dsa1**.

```
<Switch> display public-key local dsa public name dsa1

=============================================
Key name: dsa1
Key type: DSA
Time when key pair created: 15:35:42 2011/05/12
Key code:
   308201B83082012C06072A8648CE3804013082011F02818100D757262C4584C44C211F18BD
   96E5F061C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE65BE6C265854889DC1E
   DBD13EC8B274DA9F75BA26CCB987723602787E922BA84421F22C3C89CB9B06FD60FE01941D
   DD77FE6B12893DA76EEBC1D128D97F0678D7722B5341C8506F358214B16A2FAC4B36895038
   7811C7DA33021500C773218C737EC8EE993B4F2DED30F48EDACE915F0281810082269009E1
   4EC474BAF2932E69D3B1F18517AD9594184CCDFCEAE96EC4D5EF93133E84B47093C52B20CD
   35D02492B3959EC6499625BC4FA5082E22C5B374E16DD00132CE71B020217091AC717B6123
   91C76C1FB2E88317C1BD8171D41ECB83E210C03CC9B32E810561C21621C73D6DAAC028F4B1
   585DA7F42519718CC9B09EEF0381850002818100A1E456C8DA2AD1BB83B1BDF2A1A6B5A6E8
   3642B460402445DA7E4036715F468F76655E114D460B7112F57143EE020AEF4A5BFAD07B74
   0FBCB1C64DA8A2BCE619283421445EEC77D3CF0D11866E9656AD6511F4926F8376967B0AB7
   15F9FB7B514BC1174155DD6E073B1FCB3A2749E6C5FEA81003E16729497D0EAD9105E3E76A
```

Table 7-1 Command output

Field	Description
Key name	Name of the local key pair. If you did not specify a name when creating the key pair, the default name is used followed by the word **default** in brackets. The following is the default key pair name for each key algorithm:

Field	Description
	• **hostkey**—Default RSA host key pair name. • **serverkey**—Default RSA server key pair name. • **dsakey**—Default DSA host key pair name.
Key type	Options include: • RSA. • DSA.
Time when key pair created	Date and time when the local key pair was created.
Key code	Public key string.

Related commands

public-key local create

7.1.2. display public-key peer

Use **display public-key peer** to display information about peer host public keys.

Syntax

display public-key peer [**brief** | **name** *publickey-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

brief: Displays brief information about all peer host public keys. The brief information includes only the key type, key modulus, and key name.

name *publickey-name*: Displays detailed information about a peer host public key, including its key code. The *publickey-name* argument specifies a peer host public by its name, a case-sensitive string of 1 to 64 characters.

Usage guidelines

If you do not specify any keywords, this command displays detailed information about all peer host public keys configured on the local device.

You can use the **public-key peer** command or the **public-key peer import sshkey** command to configure a peer host public key on the local device.

Examples

Display detailed information about the peer host public key **idrsa**.

```
<Switch> display public-key peer name idrsa

=========================================
Key name: idrsa
Key type: RSA
Key modulus: 1024
```

```
Key code:
   30819F300D06092A864886F70D010101050003818D0030818902818100C5971581A78B5388
   B3C9063EC6B53D395A6704D9752B6F9B7B1F734EEB5DD509F0B050662C46FFB8D27F797E37
   918F6270C5793F1FC63638970A0E4D51A3CEF7CFF6E92BFAFD73F530E0BDE27056E81F2525
   6D0883836FD8E68031B2C272FE2EA75C87734A7B8F85B8EBEB3BD51CC26916AF3B3FDC32C3
   42C142D41BB4884FEB0203010001
```

Table 7-2 Command output

Field	Description
Key name	Name of the peer host public key.
Key type	Key type: RSA, or DSA.
Key modulus	Key modulus length in bits.
Key code	Public key string.

Display brief information about all peer host public keys.

```
<Switch> display public-key peer brief
Type  Modulus  Name
---------------------------
RSA   1024    idrsa
DSA   1024    10.1.1.1
```

Table 7-3 Command output

Field	Description
Type	Key type: RSA, or DSA.
Modulus	Key modulus length in bits.
Name	Name of the peer host public key.

Related commands

public-key peer

public-key peer import sshkey

7.1.3. peer-public-key end

Use **peer-public-key end** to exit public key view to system view and save the configured peer host public key.

Syntax

peer-public-key end

Views

Public key view

Predefined user roles

network-admin

Usage guidelines

After you type the peer host public key on the local device, use this command to exit public key view and to save the peer host public key.

The system verifies the public key before saving it. If the key is not in the correct format, the system discards the key and displays an error message. If the key is valid, for example, the key was displayed by the **display public-key local public** command, the system saves the key.

Examples

Exit public key view and save the configured peer host public key.

```
<Switch> system-view
[Switch] public-key peer key1
Enter public key view. Return to system view with "peer-public-key end" command.
[Switch-pkey-public-key-key1]30819F300D06092A864886F70D010101050003818D00308189028181
00C0EC8014F82515F6335A0A
[Switch-pkey-public-key-key1]EF8F999C01EC94E5760A079BD73E4F4D97F3500EDB308C29481B77E7
19D1643135877E13B1C531B4
[Switch-pkey-public-key-key1]FF1877A5E2E7B1FA4710DB0744F66F6600EEFE166F1B854E2371D5B9
52ADF6B80EB5F52698FCF3D6
[Switch-pkey-public-key-key1]1F0C2EAAD9813ECB16C5C7DC09812D4EE3E9A0B074276FFD4AF2050B
D4A9B1DDE675AC30CB020301
[Switch-pkey-public-key-key1]0001
[Switch-pkey-public-key-key1] peer-public-key end
[Switch]
```

Related commands

display public-key local public

display public-key peer

public-key peer

7.1.4. public-key local create

Use **public-key local create** to create local key pairs.

Syntax

public-key local create { **dsa** | **rsa** } [**name** *key-name*]

Default

No local key pairs exist.

Views

System view

Predefined user roles

network-admin

Parameters

dsa: Specifies the DSA key pair type.

rsa: Specifies the RSA key pair type.

name *key-name*: Assigns a name to the key pair. The *key-name* argument is a case-insensitive string of 1 to 64 characters. Valid characters are letters, digits, and hyphens (-). If you do not assign a name to the key pair, the key pair takes the default name.

Table 7-4 Default local key pair names

Type	Default name
RSA	• Host key pair: **hostkey** • Server key pair: **serverkey**
DSA	**dsakey**

Usage guidelines

The key algorithm must be the same as required by the security application.

When you create an RSA or DSA key pair, enter an appropriate key modulus length at the prompt. The longer the key modulus length, the higher the security, and the longer the key generation time.

See Table 7-5 for more information about key modulus lengths and key lengths.

If you do not assign the key pair a name, the system assigns the default name to the key pair and marks the key pair as **default**. You can also assign the default name to another key pair, but the system does not mark the key pair as **default**. The name of a key pair must be unique among all manually named key pairs that use the same key algorithm. If a name conflict occurs, the system asks whether you want to overwrite the existing key pair.

The key pairs are automatically saved and can survive system reboots.

Table 7-5 A comparison of different types of asymmetric key algorithms

Type	Generated key pairs	Modulus/key length
RSA	• One host key pair, if you specify a key pair name. • One server key pair and one host key pair, if you do not specify a key pair name. Both key pairs use their default names. **NOTE:** Only SSH 1.5 uses the RSA server key pair.	512 to 2048 bits, 1024 bits by default. To ensure security, use a minimum of 768 bits.
DSA	One host key pair.	512 to 2048 bits, 1024 bits by default. To ensure security, use a minimum of 768 bits.

Examples

Create local RSA key pairs with default names.

```
<Switch> system-view
[Switch] public-key local create rsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
...++++++
.++++++
..++++++++
....++++++++
```

```
Create the key pair successfully.
```

Create a local DSA key pair with the default name.

```
<Switch> system-view
[Switch] public-key local create dsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.++++++++++++++++++++++++++++++++++++++++++++++++++*
........+......+.....+.....................................+..+.............
.......+..........+............+............+...+.....+.............+..+...
...+.................+.........+...+....+.......+.....+............+.........+.
.........................+........+.........+............+.....+...+..........
..............+.........+.........+...........+........+....+..................
.....++++++++++++++++++++++++++++++++++++++++++++++++++*
Create the key pair successfully.
```

Create a local RSA key pair with the name **rsa1**.

```
<Switch> system-view
[Switch] public-key local create rsa name rsa1
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
...++++++
.............................++++++
Create the key pair successfully.
```

Create a local DSA key pair with the name **dsa1**.

```
<Switch> system-view
[Switch] public-key local create dsa name dsa1
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.++++++++++++++++++++++++++++++++++++++++++++++++++*
........+......+.....+.....................................+..+.............
.......+..........+............+............+...+.....+.............+..+...
...+.................+.........+...+....+.......+.....+............+.........+.
.........................+........+.........+............+.....+...+..........
..............+.........+.........+...........+........+....+..................
.....++++++++++++++++++++++++++++++++++++++++++++++++++*
Create the key pair successfully.
```

Related commands

display public-key local public

public-key local destroy

7.1.5. public-key local destroy

Use **public-key local destroy** to destroy local key pairs.

Syntax

public-key local destroy { **dsa** | **rsa** } [**name** *key-name*]

Views

System view

Predefined user roles

network-admin

Parameters

dsa: Specifies the DSA key pair type.

rsa: Specifies the RSA key pair type.

name *key-name*: Specifies a local key pair by its name, a case-insensitive string of 1 to 64 characters. Valid characters are letters, digits, and hyphens (-). If you do not specify a key pair, this command destroys all key pairs of the specified type.

Usage guidelines

To avoid key compromise, destroy the local key pair and generate a new pair after any of the following conditions occurs:

- An intrusion event has occurred.
- The storage media of the device is replaced.
- The local certificate has expired. For more information about local certificates, see *Security Configuration Guide*.

Examples

Destroy the local RSA key pairs with the default names.

```
<Switch> system-view
[Switch] public-key local destroy rsa
Confirm to destroy the key pair? [Y/N]:y
```

Destroy the local DSA key pair with the default name.

```
<Switch> system-view
[Switch] public-key local destroy dsa
Confirm to destroy the key pair? [Y/N] :y
```

Destroy the local RSA key pair **rsa1**.

```
<Switch> system-view
[Switch] public-key local destroy rsa name rsa1
Confirm to destroy the key pair? [Y/N]:y
```

Destroy the local DSA key pair **dsa1**.

```
<Switch> system-view
[Switch] public-key local destroy dsa name dsa1
Confirm to destroy the key pair? [Y/N] :y
```

Related commands

public-key local create

7.1.6. public-key local export dsa

Use **public-key local export dsa** to export a local DSA host public key.

Syntax

public-key local export dsa [**name** *key-name*] { **openssh** | **ssh2** } [*filename*]

Views

System view

Predefined user roles

network-admin

Parameters

name *key-name*: Specifies a local DSA key pair by its name, a case-insensitive string of 1 to 64 characters. Valid characters are letters, digits, and hyphens (-). If you do not specify a key pair, this command exports the host public key of the local DSA key pair with the default name.

openssh: Exports the host public key in OpenSSH format.

ssh2: Exports the host public key in SSH 2.0 format.

filename: Specifies the name of the file for saving the DSA host public key. The file name is a case-insensitive string of 1 to 128 characters. The name cannot be all dots (.), hostkey, serverkey, or dsakey, and cannot start with a slash (/) or contain **./** and **../**. For more information about file names, see *Fundamentals Configuration Guide*. If you do not specify a file name, this command displays the key on the monitor screen.

Usage guidelines

You can use this command to export a local DSA host public key before distributing it to a peer device.

To distribute a local DSA host public key to a peer device:

1. Save the exported local host public key to a file by using one of the following methods:
   - Use the **public-key local export dsa** [**name** *key-name*] { **openssh** | **ssh2** } command to export the local host public key, and then copy and paste the key to a file.
   - Use the **public-key local export dsa** [**name** *key-name*] { **openssh** | **ssh2** } *filename* command to export the key to a file. You cannot export the key to the folder **pkey** or its subfolders.
2. Transfer a copy of the file to the peer device, for example, by using FTP in binary mode or TFTP. For more information about FTP and TFTP, see *Fundamentals Configuration Guide*.
3. On the peer device, use the **public-key peer import sshkey** command to import the host public key from the file.

SSH 2.0 and OpenSSH are different public key formats. Choose the correct format that is supported on the device where you import the host public key.

Examples

Export the host public key of the local DSA key pair with the default name in OpenSSH format to a file named **key.pub**.

```
<Switch> system-view
[Switch] public-key local export dsa openssh key.pub
```

Display the host public key of the local DSA key pair with the default name in SSH 2.0 format.

```
<Switch> system-view
[Switch] public-key local export dsa ssh2
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "dsa-key-2011/05/12"
AAAAB3NzaC1kc3MAAACBANdXJixFhMRMIR8YvZbl8GHE8KQj9/5ra4WzTO9yzhSg06UiL+CM7OZb5sJlhUiJ3
B7b0T7IsnTan3W6Jsy5h3I2Anh+kiuoRCHyLDyJy5sG/WD+AZQd3Xf+axKJPadu68HRKNl/BnjXcitTQchQbz
WCFLFqL6xLNolQOHgRx9ozAAAAFQDHcyGMc37I7pk7Ty3tMPSO2s6RXwAAAIEAgiaQCeFOxHS68pMuadOx8YU
XrZWUGEzN/OrpbsTV75MTPoS0cJPFKyDNNdAkkrOVnsZJliW8T6UILiLFs3ThbdABMs5xsCAhcJGscXthI5HH
bB+y6IMXwb2BcdQey4PiEMA8ybMugQVhwhYhxz1tqsAo9LFYXaf0JRlxjMmwnu8AAACAQZEs400SvNIVfnqxw
vA7PvOVEA89tKni/f6GDBvWY9Z2Q499pAqUBtYcqQea8T4zBInxx2eF3lLaZJrIvAS205zXxSzQoU9190kakd
MdasIjQLWYGyepFc3sTwmIflQeweUwLVAPaOesKaCERjxg+e4maYWlAvySGT4c9NJlxLo=
---- END SSH2 PUBLIC KEY ----
```

Display the host public key of the local DSA key pair with the default name in OpenSSH format.

```
<Switch> system-view
[Switch] public-key local export dsa openssh
ssh-dss
AAAAB3NzaC1kc3MAAACBANdXJixFhMRMIR8YvZbl8GHE8KQj9/5ra4WzTO9yzhSg06UiL+CM7OZb5sJlhUiJ3
B7b0T7IsnTan3W6Jsy5h3I2Anh+kiuoRCHyLDyJy5sG/WD+AZQd3Xf+axKJPadu68HRKNl/BnjXcitTQchQbz
WCFLFqL6xLNolQOHgRx9ozAAAAFQDHcyGMc37I7pk7Ty3tMPSO2s6RXwAAAIEAgiaQCeFOxHS68pMuadOx8YU
XrZWUGEzN/OrpbsTV75MTPoS0cJPFKyDNNdAkkrOVnsZJliW8T6UILiLFs3ThbdABMs5xsCAhcJGscXthI5HH
bB+y6IMXwb2BcdQey4PiEMA8ybMugQVhwhYhxz1tqsAo9LFYXaf0JRlxjMmwnu8AAACAQZEs400SvNIVfnqxw
vA7PvOVEA89tKni/f6GDBvWY9Z2Q499pAqUBtYcqQea8T4zBInxx2eF3lLaZJrIvAS205zXxSzQoU9190kakd
MdasIjQLWYGyepFc3sTwmIflQeweUwLVAPaOesKaCERjxg+e4maYWlAvySGT4c9NJlxLo= dsa-key
```

Export the host public key of the local DSA key pair **dsa1** in OpenSSH format to the file **dsa1.pub**.

```
<Switch> system-view
[Switch] public-key local export dsa name dsa1 openssh dsa1.pub
```

Display the host public key of the local DSA key pair **dsa1** in SSH 2.0 format.

```
<Switch> system-view
[Switch] public-key local export dsa name dsa1 ssh2
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "dsa-key-2011/05/12"
AAAAB3NzaC1kc3MAAACBANdXJixFhMRMIR8YvZbl8GHE8KQj9/5ra4WzTO9yzhSg06UiL+CM7OZb5sJlhUiJ3
B7b0T7IsnTan3W6Jsy5h3I2Anh+kiuoRCHyLDyJy5sG/WD+AZQd3Xf+axKJPadu68HRKNl/BnjXcitTQchQbz
WCFLFqL6xLNolQOHgRx9ozAAAAFQDHcyGMc37I7pk7Ty3tMPSO2s6RXwAAAIEAgiaQCeFOxHS68pMuadOx8YU
XrZWUGEzN/OrpbsTV75MTPoS0cJPFKyDNNdAkkrOVnsZJliW8T6UILiLFs3ThbdABMs5xsCAhcJGscXthI5HH
bB+y6IMXwb2BcdQey4PiEMA8ybMugQVhwhYhxz1tqsAo9LFYXaf0JRlxjMmwnu8AAACBAKHkVsjaKtG7g7G98
qGmtaboNkK0YEAkRdp+QDZxX0aPdmVeEU1GC3ES9XFD7gIK70pb+tB7dA+8scZNqKK85hkoNCFEXux3088NEY
ZullatZRH0km+DdpZ7CrcV+ft7UUvBF0FV3W4HOx/LOidJ5sX+qBAD4WcpSX0OrZEF4+dq
---- END SSH2 PUBLIC KEY ----
```

Display the host public key of the local DSA key pair **dsa1** in OpenSSH format.

```
<Switch> system-view
[Switch] public-key local export dsa name dsa1 openssh
ssh-dss
AAAAB3NzaC1kc3MAAACBANdXJixFhMRMIR8YvZbl8GHE8KQj9/5ra4WzTO9yzhSg06UiL+CM7OZb5sJlhUiJ3
B7b0T7IsnTan3W6Jsy5h3I2Anh+kiuoRCHyLDyJy5sG/WD+AZQd3Xf+axKJPadu68HRKNl/BnjXcitTQchQbz
WCFLFqL6xLNolQOHgRx9ozAAAAFQDHcyGMc37I7pk7Ty3tMPSO2s6RXwAAAIEAgiaQCeFOxHS68pMuadOx8YU
XrZWUGEzN/OrpbsTV75MTPoS0cJPFKyDNNdAkkrOVnsZJliW8T6UILiLFs3ThbdABMs5xsCAhcJGscXthI5HH
bB+y6IMXwb2BcdQey4PiEMA8ybMugQVhwhYhxz1tqsAo9LFYXaf0JRlxjMmwnu8AAACBAKHkVsjaKtG7g7G98
```

```
qGmtaboNkK0YEAkRdp+QDZxX0aPdmVeEU1GC3ES9XFD7gIK70pb+tB7dA+8scZNqKK85hkoNCFEXux3088NEY
ZullatZRH0km+DdpZ7CrcV+ft7UUvBF0FV3W4HOx/LOidJ5sX+qBAD4WcpSX0OrZEF4+dq dsa-key
```

Related commands

public-key local create

public-key peer import sshkey

7.1.7. public-key local export rsa

Use **public-key local export rsa** to export a local RSA host public key.

Syntax

public-key local export rsa [**name** *key-name*] { **openssh** | **ssh1** | **ssh2** } [*filename*]

Views

System view

Predefined user roles

network-admin

Parameters

name *key-name*: Specifies a local RSA key pair by its name, a case-insensitive string of 1 to 64 characters. Valid characters are letters, digits, and hyphens (-). If you do not specify a key pair, this command exports the host public key of the local RSA key pair with the default name.

openssh: Exports the host public key in OpenSSH format.

ssh1: Exports the host public key in SSH 1.5 format.

ssh2: Exports the host public key in SSH 2.0 format.

filename: Specifies the name of the file for saving the RSA host public key. The file name is a case-insensitive string of 1 to 128 characters. The name cannot be all dots (.), hostkey, serverkey, or dsakey, and cannot start with a slash (/) or contain **./** and **../**. For more information about file names, see *Fundamentals Configuration Guide*. If you do not specify a file name, this command displays the key on the monitor screen.

Usage guidelines

You can use this command to export a local RSA host public key before distributing it to a peer device.

To distribute a local RSA host public key to a peer device:

1. Save the exported local host public key to a file by using one of the following methods:
   - Use the **public-key local export rsa** [**name** *key-name*] { **openssh** | **ssh2** } command to export the key, and then copy and paste it to a file.
   - Use the **public-key local export rsa** [**name** *key-name*] { **openssh** | **ssh2** } *filename* command to export key to a file. You cannot export the key to the folder **pkey** or its subfolders.
2. Transfer a copy of the file to the peer device, for example, by using FTP in binary mode or TFTP. For more information about FTP and TFTP, see *Fundamentals Configuration Guide*.
3. On the peer device, use the **public-key peer import sshkey** command to import the host public key from the file.

Choose the correct public key format that is supported on the device where you import the host public key.

Examples

Export the host public key of the local RSA key pair with the default name in OpenSSH format to the file **key.pub**.

```
<Switch> system-view
[Switch] public-key local export rsa openssh key.pub
```

Display the host public key of the local RSA key pair with the default name in SSH 2.0 format.

```
<Switch> system-view
[Switch] public-key local export rsa ssh2
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "rsa-key-2011/05/12"
AAAAB3NzaC1yc2EAAAADAQABAAAAgQDapKr+/gTCyWZyabuCJuJjMeMPQaj/kixzOCCAl+hDMmEGMrSfddq/b
YcbgM7Buit1AgB3x0dFyTPi85DcCznTW4goPXAKFjuzCbGfj4chakSr+/aj1k3rM+XOvyvPJilneKJqhPT0xd
v4tlas+mLNloY0dImbwS2kwE71rgg1CQ==
---- END SSH2 PUBLIC KEY ----
```

Display the host public key of the local RSA key pair with the default name in OpenSSH format.

```
<Switch> system-view
[Switch] public-key local export rsa openssh
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAAAgQDapKr+/gTCyWZyabuCJuJjMeMPQaj/kixzOCCAl+hDMmEGMrSfddq/b
YcbgM7Buit1AgB3x0dFyTPi85DcCznTW4goPXAKFjuzCbGfj4chakSr+/aj1k3rM+XOvyvPJilneKJqhPT0xd
v4tlas+mLNloY0dImbwS2kwE71rgg1CQ== rsa-key
```

Export the host public key of the local RSA key pair **rsa1** in OpenSSH format to the file **rsa1.pub**.

```
<Switch> system-view
[Switch] public-key local export rsa name rsa1 openssh rsa1.pub
```

Display the host public key of the local RSA key pair **rsa1** in SSH 2.0 format.

```
<Switch> system-view
[Switch] public-key local export rsa name rsa1 ssh2
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "rsa-key-2011/05/12"
AAAAB3NzaC1yc2EAAAADAQABAAAAgQDevEbyF93xHUJucJWqRc1r8fhzQ9lSVprCI6ATZeDYyR1J00fBQ8XY+
q2olqoagn5YDyUC8ZJvUhlyMOHeORpkAVxD3XncTp4XG66h3rTHHa7Xmm7f1GDYlF0n05t8mCLVaupbfCzP8b
a8UkrUmMO4fUvW6zavA5LYxtlAiQv0KQ==
---- END SSH2 PUBLIC KEY ----
```

Display the host public key of the local RSA key pair **rsa1** in OpenSSH format.

```
<Switch> system-view
[Switch] public-key local export rsa name rsa1 openssh
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAAAgQDevEbyF93xHUJucJWqRc1r8fhzQ9lSVprCI6ATZeDYyR1J00fBQ8XY+
q2olqoagn5YDyUC8ZJvUhlyMOHeORpkAVxD3XncTp4XG66h3rTHHa7Xmm7f1GDYlF0n05t8mCLVaupbfCzP8b
a8UkrUmMO4fUvW6zavA5LYxtlAiQv0KQ== rsa-key
```

Related commands

public-key local create

public-key peer import sshkey

7.1.8. public-key peer

Use **public-key peer** to assign a name to a peer host public key and enter public key view, or enter the view of an existing peer host public key.

Use **undo public-key peer** to delete a peer host public key.

Syntax

public-key peer *keyname*

undo public-key peer *keyname*

Default

No peer host public keys exist.

Views

System view

Predefined user roles

network-admin

Parameters

keyname: Specifies a key name, a case-sensitive string of 1 to 64 characters.

Usage guidelines

After you execute this command to enter the public key view, type the public key. Spaces and carriage returns are allowed, but are not saved.

To configure a peer host public key on the local device, first obtain the peer public key in hexadecimal notation, and then perform the following tasks on the local device:

1. Execute the **public-key peer** command to enter public key view.
2. Type the public key.
3. Execute the **peer-public-key end** command to save the public key and return to system view.

The public key you type in the public key view must be in a correct format. If the peer device is an NEC device, use the **display public-key local public** command to display and record its public key.

Examples

Assign the name **key1** to the peer host public key and enter public key view.

```
<Switch> system-view
[Switch] public-key peer key1
Enter public key view. Return to system view with "peer-public-key end" command.
[Switch-pkey-public-key-key1]
```

Related commands

display public-key local public

display public-key peer

peer-public-key end

7.1.9. public-key peer import sshkey

Use **public-key peer import sshkey** to import a peer host public key from a public key file.

Use **undo public-key peer** to remove a peer host public key.

Syntax

public-key peer *keyname* **import sshkey** *filename*

undo public-key peer *keyname*

Default

No peer host public keys exist.

Views

System view

Predefined user roles

network-admin

Parameters

keyname: Specifies a name for a peer host public key, a case-sensitive string of 1 to 64 characters.

filename: Specifies a public key file by its name, a case-insensitive string of 1 to 128 characters. The name cannot be all dots (.), hostkey, serverkey, or dsakey, and cannot start with a slash (/) or contain **./** and **../**. For more information about file names, see *Fundamentals Configuration Guide*.

Usage guidelines

After you configure this command, the system automatically transforms the host public key to the PKCS format, and saves the key.

Before you use this command, make sure you have got a copy of the public key file from the peer device through FTP in binary mode or through TFTP.

The device supports importing public keys in the format of SSH 1.5, SSH 2.0, and OpenSSH.

Examples

Import the peer host public key **key2** from the public key file **key.pub**.

```
<Switch> system-view
[Switch] public-key peer key2 import sshkey key.pub
```

Related commands

display public-key peer

public-key local export dsa

public-key local export rsa

Contents

A page of this section is **9-x-x**

8. PKI commands ····· 8-1
8.1. PKI commands ····· 8-1
8.1.1. attribute ····· 8-1
8.1.2. ca identifier ····· 8-2
8.1.3. certificate request entity ····· 8-3
8.1.4. certificate request from ····· 8-4
8.1.5. certificate request mode ····· 8-5
8.1.6. certificate request polling ····· 8-6
8.1.7. certificate request url ····· 8-7
8.1.8. common-name ····· 8-7
8.1.9. country ····· 8-8
8.1.10. crl check enable ····· 8-8
8.1.11. crl url ····· 8-9
8.1.12. display pki certificate access-control-policy ····· 8-10
8.1.13. display pki certificate attribute-group ····· 8-11
8.1.14. display pki certificate domain ····· 8-12
8.1.15. display pki certificate request-status ····· 8-15
8.1.16. display pki crl domain ····· 8-17
8.1.17. fqdn ····· 8-18
8.1.18. ip ····· 8-19
8.1.19. locality ····· 8-20
8.1.20. organization ····· 8-20
8.1.21. organization-unit ····· 8-21
8.1.22. pki abort-certificate-request ····· 8-21
8.1.23. pki certificate access-control-policy ····· 8-22
8.1.24. pki certificate attribute-group ····· 8-23
8.1.25. pki delete-certificate ····· 8-24
8.1.26. pki domain ····· 8-25
8.1.27. pki entity ····· 8-26
8.1.28. pki import ····· 8-26
8.1.29. pki request-certificate ····· 8-31
8.1.30. pki retrieve-certificate ····· 8-32
8.1.31. pki retrieve-crl ····· 8-33
8.1.32. pki storage ····· 8-34
8.1.33. pki validate-certificate ····· 8-35
8.1.34. public-key dsa ····· 8-37
8.1.35. public-key ecdsa ····· 8-38
8.1.36. public-key rsa ····· 8-39
8.1.37. root-certificate fingerprint ····· 8-41
8.1.38. state ····· 8-42

8. PKI commands

8.1. PKI commands

8.1.1. attribute

Use **attribute** to configure a rule to filter certificates based on an attribute in the certificate issuer name, subject name, or alternative subject name field.

Use **undo attribute** to remove an attribute rule.

Syntax

attribute *id* { **alt-subject-name** { **fqdn** | **ip** } | { **issuer-name** | **subject-name** } { **dn** | **fqdn** | **ip** } } { **ctn** | **equ** | **nctn** | **nequ** } *attribute-value*

undo attribute *id*

Default

No attribute rules exist.

Views

Certificate attribute group view

Predefined user roles

network-admin

Parameters

id: Specifies a rule ID in the range of 1 to 16.

alt-subject-name: Specifies the alternative subject name field.

fqdn: Specifies the FQDN attribute.

ip: Specifies the IP address attribute.

dn: Specifies the DN attribute.

issuer-name: Specifies the issuer name field.

subject-name: Specifies the subject name field.

ctn: Specifies the contain operation.

equ: Specifies the equal operation.

nctn: Specifies the not-contain operation.

nequ: Specifies the not-equal operation.

attribute-value: Sets an attribute value, a case-insensitive string of 1 to 128 characters.

Usage guidelines

Different certificate fields support different attributes.

- The subject name field and the issuer name field can contain a single DN, multiple FQDNs, and multiple IP addresses.
- The alternative subject name field can contain multiple FQDNs and IP addresses but zero DNs.

An attribute rule is a combination of an attribute-value pair with an operation keyword, as listed in Table 8-1 .

Table 8-1 Combinations of attribute-value pairs and operation keywords

Operation	DN	FQDN/IP
ctn	The DN contains the specified attribute value.	Any FQDN or IP address contains the specified attribute value.
nctn	The DN does not contain the specified attribute value.	None of the FQDNs or IP addresses contain the specified attribute value.
equ	The DN is the same as the specified attribute value.	Any FQDN or IP address is the same as the specified attribute value.
nequ	The DN is not the same as the specified attribute value.	None of the FQDNs or IP addresses are the same as the specified attribute value.

A certificate matches an attribute rule if it contains an attribute that matches the criterion defined in the rule. For example, a certificate matches the **attribute 1 subject-name dn ctn abc** rule if it meets the following conditions:

- The subject name field of the certificate contains the DN attribute.
- The DN attribute value contains the **abc** string.

A certificate matches an attribute group if it matches all attribute rules in the group.

Examples

Create a certificate attribute group and enter its view.

```
<Switch> system-view
[Switch] pki certificate attribute-group mygroup
```

Configure an attribute rule to match certificates that contain the **abc** string in the subject DN.

```
[Switch-pki-cert-attribute-group-mygroup] attribute 1 subject-name dn ctn abc
```

Configure an attribute rule to match certificates that do not contain FQDN **abc** in the issuer name field.

```
[Switch-pki-cert-attribute-group-mygroup] attribute 2 issuer-name fqdn nequ abc
```

Configure an attribute rule to match certificates that do not contain IP address **10.0.0.1** in the alternative subject name field.

```
[Switch-pki-cert-attribute-group-mygroup] attribute 3 alt-subject-name ip nequ 10.0.0.1
```

Related commands

display pki certificate attribute-group

8.1.2. ca identifier

Use **ca identifier** to specify the trusted CA.

Use **undo ca identifier** to restore the default.

Syntax

ca identifier *name*

undo ca identifier

Default

No trusted CA is specified.

Views

PKI domain view

Predefined user roles

network-admin

Parameters

name: Specifies the trusted CA by its name, a case-sensitive string of 1 to 63 characters.

Usage guidelines

To obtain a CA certificate in a PKI domain, you must specify the trusted CA name. The trusted CA name uniquely identifies the CA to be used if multiple CAs exist on the CA server specified for the PKI domain.

Make sure the specified CA name is consistent with the name of the CA that owns the CA certificate to be obtained.

Examples

Set the name of the trusted CA to **new-ca**.

```
<Switch> system-view
[Switch] pki domain aaa
[Switch-pki-domain-aaa] ca identifier new-ca
```

8.1.3. certificate request entity

Use **certificate request entity** to specify the PKI entity for certificate request.

Use **undo certificate request entity** to restore the default.

Syntax

certificate request entity *entity-name*

undo certificate request entity

Default

No PKI entity is specified for certificate request.

Views

PKI domain view

Predefined user roles

network-admin

Parameters

entity-name: Specifies a PKI entity by its name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

A PKI entity describes the identity attributes of an entity for certificate request, including the following information:

- Common name.
- Organization.
- Unit in the organization.

- Locality.
- State and country where the entity resides.
- FQDN.
- IP address.

You can specify only one PKI entity for a PKI domain. If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify PKI entity **en1** for certificate request in PKI domain **aaa**.

```
<Switch> system-view
[Switch] pki domain aaa
[Switch-pki-domain-aaa] certificate request entity en1
```

Related commands

pki entity

8.1.4. certificate request from

Use **certificate request from** to specify the type of certificate request reception authority.

Use **undo certificate request from** to restore the default.

Syntax

certificate request from { **ca** | **ra** }

undo certificate request from

Default

The type of certificate request reception authority is not specified.

Views

PKI domain view

Predefined user roles

network-admin

Parameters

ca: Sends certificate requests to the CA.

ra: Sends certificate requests to the RA.

Usage guidelines

The CA server determines whether the CA or RA accepts certificate requests. This authority setting must be consistent with the setting on the CA server.

Examples

Sends certificate requests to the RA.

```
<Switch> system-view
[Switch] pki domain aaa
[Switch-pki-domain-aaa] certificate request from ra
```

8.1.5. certificate request mode

Use **certificate request mode** to set the certificate request mode.

Use **undo certificate request mode** to restore the default.

Syntax

certificate request mode { **auto** [**password** { **cipher** | **simple** } *string*] | **manual** }

undo certificate request mode

Default

The certificate request mode is manual.

Views

PKI domain view

Predefined user roles

network-admin

Parameters

auto: Specifies the auto certificate request mode.

password: Specifies a password for certificate revocation.

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 31 characters. Its encrypted form is a case-sensitive string of 1 to 73 characters.

manual: Specifies the manual certificate request mode.

Usage guidelines

A certificate request can be submitted to a CA in offline or online mode. In online mode, a certificate request can be automatically or manually submitted:

- **Auto request mode**—A PKI entity automatically obtains the CA certificate and submits a certificate request to the CA when both of the following conditions exist:
  - An associated application (IKE, for example) performs identity authentication.
  - No certificate is available for the application on the device.

  In auto request mode, specify the password for certificate revocation as required by the CA policy.
- **Manual request mode**—You must manually obtain the CA certificate and submit certificate requests.

Examples

Set the certificate request mode to **auto**.

```
<Switch> system-view
[Switch] pki domain aaa
[Switch-pki-domain-aaa] certificate request mode auto
```

Set the certificate request mode to **auto**, and set the certificate revocation password in plain text to **123456**.

```
<Switch> system-view
```

```
[Switch] pki domain aaa
[Switch-pki-domain-aaa] certificate request mode auto password simple 123456
```

Related commands

pki request-certificate

8.1.6. certificate request polling

Use **certificate request polling** to set the polling interval and the maximum number of attempts to query certificate request status.

Use **undo certificate request polling** to restore the defaults.

Syntax

certificate request polling { **count** *count* | **interval** *interval* }

undo certificate request polling { **count** | **interval** }

Default

The polling interval is 20 minutes, and the maximum number of attempts is 50.

Views

PKI domain view

Predefined user roles

network-admin

Parameters

count *count*: Specifies the maximum number of query attempts. The value range is 1 to 100.

interval *interval*: Specifies a polling interval in minutes. The value range is 5 to 168.

Usage guidelines

After a PKI entity submits a certificate request, it might take the CA server a while to issue the certificate if the CA administrator must manually approve the certificate request. During this period, the PKI entity periodically queries the CA server for the certificate request status. The periodic query operation stops until the PKI entity obtains the certificate or the maximum number of query attempts is reached. If the maximum number of query attempts is reached, the certificate request fails.

If the CA server automatically approves certificate requests, the PKI entity can obtain the certificate immediately after it submits a certificate request. In this case, the PKI entity does not send queries to the CA server.

Examples

Set the polling interval to 15 minutes, and the maximum number of query attempts to 40.

```
<Switch> system-view
[Switch] pki domain aaa
[Switch-pki-domain-aaa] certificate request polling interval 15
[Switch-pki-domain-aaa] certificate request polling count 40
```

Related commands

display pki certificate request-status

8.1.7. certificate request url

Use **certificate request url** to specify the URL of the certificate request reception authority (CA or RA) to which the device should send SCEP certificate requests.

Use **undo certificate request url** to restore the default.

Syntax

certificate request url *url-string*

undo certificate request url

Default

The URL of the certificate request reception authority is not specified.

Views

PKI domain view

Predefined user roles

network-admin

Parameters

url-string: Specifies the URL of the certificate request reception authority, a case-sensitive string of 1 to 511 characters. The URL length is restricted by the CLI string limitation or the *url-string* parameter, whichever is smaller.

Usage guidelines

The certificate request URL contains the location of the certificate request reception authority server and the path of the application script on the server, in the format http://*server_location/cgi_script_location*.

Examples

Set the certificate request URL to **http://169.254.0.1/certsrv/mscep/mscep.dll**.

```
<Switch> system-view
[Switch] pki domain a
[Switch-pki-domain-a] certificate request url
http://169.254.0.1/certsrv/mscep/mscep.dll
```

8.1.8. common-name

Use **common-name** to set the common name for a PKI entity.

Use **undo common-name** to restore the default.

Syntax

common-name *common-name-sting*

undo common-name

Default

No common name is set for a PKI entity.

Views

PKI entity view

Predefined user roles

network-admin

Parameters

common-name-sting: Specifies a common name, a case-sensitive string of 1 to 63 characters. No comma can be included. You can set the username of the PKI entity as the common name.

Examples

Set the common name to **test** for PKI entity **en**.

```
<Switch> system-view
[Switch] pki entity en
[Switch-pki-entity-en] common-name test
```

8.1.9. country

Use **country** to set the country code of a PKI entity.

Use **undo country** to restore the default.

Syntax

country *country-code-string*

undo country

Default

No country code is set for a PKI entity.

Views

PKI entity view

Predefined user roles

network-admin

Parameters

country-code-string: Specifies a country code, a case-sensitive string of two characters. For example, JP is the country code for Japan.

Examples

Set the country code to JP for PKI entity 1.

```
<Switch> system-view
[Switch] pki entity 1
[Switch-pki-entity-1] country JP
```

8.1.10. crl check enable

Use **crl check enable** to enable CRL checking.

Use **undo crl check enable** to disable CRL checking.

Syntax

crl check enable

undo crl check enable

Default

CRL checking is enabled.

Views

PKI domain view

Predefined user roles

network-admin

Usage guidelines

A CRL is a list of revoked certificates signed and published by a CA. Revoked certificates should no longer be trusted.

Enable CRL checking to ensure that the device only accepts certificates that have not been revoked by the issuing CA.

Examples

Disable CRL checking.

```
<Switch> system-view
[Switch] pki domain aaa
[Switch-pki-domain-aaa] undo crl check enable
```

Related commands

pki import

pki retrieve-certificate

pki validate-certificate

8.1.11. crl url

Use **crl url** to specify the URL of the CRL repository.

Use **undo crl url** to restore the default.

Syntax

crl url *url-string*

undo crl url

Default

The URL of the CRL repository is not specified.

Views

PKI domain view

Predefined user roles

network-admin

Parameters

url-string: Specifies the URL of the CRL repository, a case-sensitive string of 1 to 511 characters. The URL format is ldap://*server_location* or http://*server_location*. The URL length is restricted by the CLI string limitation or the *url-string* parameter, whichever is smaller.

Usage guidelines

To use CRL checking, a CRL must be obtained from a CRL repository.

The device selects a CRL repository in the following order:

1. CRL repository specified in the PKI domain by using this command.
2. CRL repository in the certificate that is being verified.
3. CRL repository in the CA certificate or CRL repository in the upper-level CA certificate if the CA certificate is the certificate being verified.

After the previous selection process, if the CRL repository is not found, the device obtains the CRL through SCEP. In this scenario, the CA certificate and the local certificates must have been obtained.

Examples

Set the URL of the CRL repository to **http://169.254.0.30**.

```
<Switch> system-view
[Switch] pki domain aaa
[Switch-pki-domain-aaa] crl url http://169.254.0.30
```

Set the URL of the CRL repository to **ldap://169.254.0.30** in VPN instance **vpn1**.

```
<Switch> system-view
[Switch] pki domain 1
[Switch-pki-domain-1] crl url ldap://169.254.0.30 vpn-instance vpn1
```

Related commands

pki retrieve-crl

8.1.12. display pki certificate access-control-policy

Use **display pki certificate access-control-policy** to display information about certificate-based access control policies.

Syntax

display pki certificate access-control-policy [*policy-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

policy-name: Specifies a certificate-based access control policy by its name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

If you do not specify a policy name, this command displays information about all certificate-based access control policies.

Examples

Display information about certificate-based access control policy **mypolicy**.

```
<Switch> display pki certificate access-control-policy mypolicy
 Access control policy name: mypolicy
     Rule 1  deny    mygroup1
     Rule 2  permit  mygroup2
```

Display information about all certificate-based access control policies.

```
<Switch> display pki certificate access-control-policy
 Total PKI certificate access control policies: 2
 Access control policy name: mypolicy1
     Rule 1  deny    mygroup1
     Rule 2  permit  mygroup2
 Access control policy name: mypolicy2
     Rule 1  deny    mygroup3
     Rule 2  permit  mygroup4
```

Table 8-2 Command output

Field	Description
Total PKI certificate access control policies	Total number of certificate-based access control policies.
permit	Permit certificates that match the attribute group in the access control rule.
deny	Deny certificates that match the attribute group in the access control rule.

Related commands

pki certificate access-control-policy

8.1.13. display pki certificate attribute-group

Use **display pki certificate attribute-group** to display information about certificate attribute groups.

Syntax

display pki certificate attribute-group [*group-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

group-name: Specifies a certificate attribute group by its name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

If you do not specify a certificate attribute group, this command displays information about all certificate attribute groups.

Examples

Display information about certificate attribute group **mygroup**.

```
<Switch> display pki certificate attribute-group mygroup
 Attribute group name: mygroup
      Attribute  1 subject-name     dn    ctn   abc
      Attribute  2 issuer-name      fqdn  nctn  app
```

Display information about all certificate attribute groups.

```
<Switch> display pki certificate attribute-group
 Total PKI certificate attribute groups: 2.
 Attribute group name: mygroup1
      Attribute  1 subject-name     dn    ctn   abc
      Attribute  2 issuer-name      fqdn  nctn  app
Attribute group name: mygroup2
      Attribute  1 subject-name     dn    ctn   def
      Attribute  2 issuer-name      fqdn  nctn  fqd
```

Table 8-3 Command output

Field	Description
Total PKI certificate attribute groups	Total number of certificate attribute groups.
ctn	Contain operation.
nctn	Not-contain operation.
equ	Equal operation.
nequ	Not-equal operation.
Attribute 1 subject-name dn ctn abc	Attribute rule contents: • **alt-subject-name**—Alternative subject name. • **issuer-name**—Certificate issuer name. • **subject-name**—Certificate subject name. • **fqdn**—FQDN of the PKI entity. • **ip**—IP address of the PKI entity. • **dn**—DN of the PKI entity. • **ctn**—Indicates the contain operation. • **equ**—Indicates the equal operation. • **nctn**—Indicates the not-contain operation. • **nequ**—Indicates the not-equal operation.

Related commands

attribute

pki certificate attribute-group

8.1.14. display pki certificate domain

Use **display pki certificate domain** to display information about certificates.

Syntax

display pki certificate domain *domain-name* { **ca** | **local** }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

domain-name: Specifies a PKI domain by its name, a case-insensitive string of 1 to 31 characters. The domain name cannot contain the special characters listed in Table 8-4 .

Table 8-4 Special characters

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar	|	Quotation marks	"
Colon	:	Apostrophe	'

ca: Specifies the CA certificate.

local: Specifies the local certificates.

Usage guidelines

If you specify the **CA** keyword, this command displays information about all CA certificates in the domain. If the domain has RA certificates, the RA certificates are also displayed.

If you specify the **local** keyword, this command displays information about all local certificates in the domain.

Examples

Display information about the CA certificate in PKI domain **aaa**.

```
<Switch> display pki certificate domain aaa ca
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number:
            5c:72:dc:c4:a5:43:cd:f9:32:b9:c1:90:8f:dd:50:f6
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=cn, O=docm, OU=rnd, CN=rootca
        Validity
            Not Before: Jan  6 02:51:41 2011 GMT
            Not After : Dec  7 03:12:05 2013 GMT
        Subject: C=cn, O=ccc, OU=ppp, CN=rootca
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:c4:fd:97:2c:51:36:df:4c:ea:e8:c8:70:66:f0:
                    28:98:ec:5a:ee:d7:35:af:86:c4:49:76:6e:dd:40:
                    4a:9e:8d:c0:cb:d9:10:9b:61:eb:0c:e0:22:ce:f6:
                    57:7c:bb:bb:1b:1d:b6:81:ad:90:77:3d:25:21:e6:
                    7e:11:0a:d8:1d:3c:8e:a4:17:1e:8c:38:da:97:f6:
                    6d:be:09:e3:5f:21:c5:a0:6f:27:4b:e3:fb:9f:cd:
                    c1:91:18:ff:16:ee:d8:cf:8c:e3:4c:a3:1b:08:5d:
                    84:7e:11:32:5f:1a:f8:35:25:c0:7e:10:bd:aa:0f:
```

```
                52:db:7b:cd:5d:2b:66:5a:fb
            Exponent: 65537 (0x10001)
    Signature Algorithm: sha1WithRSAEncryption
        6d:b1:4e:d7:ef:bb:1d:67:53:67:d0:8f:7c:96:1d:2a:03:98:
        3b:48:41:08:a4:8f:a9:c1:98:e3:ac:7d:05:54:7c:34:d5:ee:
        09:5a:11:e3:c8:7a:ab:3b:27:d7:62:a7:bb:bc:7e:12:5e:9e:
        4c:1c:4a:9f:d7:89:ca:20:46:de:c5:b3:ce:36:ca:5e:6e:dc:
        e7:c6:fe:3f:c5:38:dd:d5:a3:36:ad:f4:3d:e6:32:7f:48:df:
        07:f0:a2:32:89:86:72:22:cd:ed:e5:0f:95:df:9c:75:71:e7:
        fe:34:c5:a0:64:1c:f0:5c:e4:8f:d3:00:bd:fa:90:b6:64:d8:
        88:a6
```

Display information about local certificates in the PKI domain **aaa**.

```
<Switch> display pki certificate domain aaa local
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            bc:05:70:1f:0e:da:0d:10:16:1e
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=CN, O=sec, OU=software, CN=abdfdc
        Validity
            Not Before: Jan  7 20:05:44 2011 GMT
            Not After : Jan  7 20:05:44 2012 GMT
        Subject: O=OpenCA Labs, OU=Users, CN=fips fips-sec
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:b2:38:ad:8c:7d:78:38:37:88:ce:cc:97:17:39:
                    52:e1:99:b3:de:73:8b:ad:a8:04:f9:a1:f9:0d:67:
                    d8:95:e2:26:a4:0b:c2:8c:63:32:5d:38:3e:fd:b7:
                    4a:83:69:0e:3e:24:e4:ab:91:6c:56:51:88:93:9e:
                    12:a4:30:ad:ae:72:57:a7:ba:fb:bc:ac:20:8a:21:
                    46:ea:e8:93:55:f3:41:49:e9:9d:cc:ec:76:13:fd:
                    a5:8d:cb:5b:45:08:b7:d1:c5:b5:58:89:47:ce:12:
                    bd:5c:ce:b6:17:2f:e0:fc:c0:3e:b7:c4:99:31:5b:
                    8a:f0:ea:02:fd:2d:44:7a:67
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Cert Type:
                SSL Client, S/MIME
            X509v3 Key Usage:
                Digital Signature, Non Repudiation, Key Encipherment
            X509v3 Extended Key Usage:
```

```
                TLS Web Client Authentication, E-mail Protection, Microsoft
Smartcardlogin
            Netscape Comment:
                User Certificate of OpenCA Labs
            X509v3 Subject Key Identifier:
                91:95:51:DD:BF:4F:55:FA:E4:C4:D0:10:C2:A1:C2:99:AF:A5:CB:30
            X509v3 Authority Key Identifier:
                keyid:DF:D2:C9:1A:06:1F:BC:61:54:39:FE:12:C4:22:64:EB:57:3B:11:9F

            X509v3 Subject Alternative Name:
                email:fips@ccc.com
            X509v3 Issuer Alternative Name:
                email:pki@openca.org
            Authority Information Access:
                CA Issuers - URI:http://titan/pki/pub/cacert/cacert.crt
                OCSP - URI:http://titan:2560/
                1.3.6.1.5.5.7.48.12 - URI:http://titan:830/

            X509v3 CRL Distribution Points:

                Full Name:
                  URI:http://titan/pki/pub/crl/cacrl.crl

    Signature Algorithm: sha256WithRSAEncryption
        94:ef:56:70:48:66:be:8f:9d:bb:77:0f:c9:f4:65:77:e3:bd:
        ea:9a:b8:24:ae:a1:38:2d:f4:ab:e8:0e:93:c2:30:33:c8:ef:
        f5:e9:eb:9d:37:04:6f:99:bd:b2:c0:e9:eb:b1:19:7e:e3:cb:
        95:cd:6c:b8:47:e2:cf:18:8d:99:f4:11:74:b1:1b:86:92:98:
        af:a2:34:f7:1b:15:ee:ea:91:ed:51:17:d0:76:ec:22:4c:56:
        da:d6:d1:3c:f2:43:31:4f:1d:20:c8:c2:c3:4d:e5:92:29:ee:
        43:c6:d7:72:92:e8:13:87:38:9a:9c:cd:54:38:b2:ad:ba:aa:
        f9:a4:68:b5:2a:df:9a:31:2f:42:80:0c:0c:d9:6d:b3:ab:0f:
        dd:a0:2c:c0:aa:16:81:aa:d9:33:ca:01:75:94:92:44:05:1a:
        65:41:fa:1e:41:b5:8a:cc:2b:09:6e:67:70:c4:ed:b4:bc:28:
        04:50:a6:33:65:6d:49:3c:fc:a8:93:88:53:94:4c:af:23:64:
        cb:af:e3:02:d1:b6:59:5f:95:52:6d:00:00:a0:cb:75:cf:b4:
        50:c5:50:00:65:f4:7d:69:cc:2d:68:a4:13:5c:ef:75:aa:8f:
        3f:ca:fa:eb:4d:d5:5d:27:db:46:c7:f4:7d:3a:b2:fb:a7:c9:
        de:18:9d:c1
```

Related commands

pki domain

pki retrieve-certificate

8.1.15. display pki certificate request-status

Use **display pki certificate request-status** to display certificate request status.

Syntax

display pki certificate request-status

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

If you do not specify a PKI domain, this command displays the certificate request status for all PKI domains.

Examples

Display certificate request statuses for all PKI domains.

```
<Switch> display pki certificate request-status
Certificate Request Transaction 1
    Domain name: domain1
    Status: Pending
    Key usage: General
    Remain polling attempts: 10
    Next polling attempt after : 1191 seconds
Certificate Request Transaction 2
    Domain name: domain2
    Status: Pending
    Key usage: Signature
    Remain polling attempts: 10
    Next polling attempt after : 188 seconds
```

Table 8-5 Command output

Field	Description
Certificate Request Transaction *number*	Certificate request transaction number, starting from 1.
Status	Certificate request status, including only the pending status.
Key usage	Certificate purposes: • **General**—Signature and encryption. • **Signature**—Signature only. • **Encryption**—Encryption only.
Remain polling attempts	Remaining number of attempts to query certificate request status.
Next polling attempt after	Remaining seconds before the next request status polling.

Related commands

certificate request polling

pki domain

pki retrieve-certificate

8.1.16. display pki crl domain

Use **display pki crl domain** to display information about the CRL saved at the local for a PKI domain.

Syntax

display pki crl domain *domain-name*

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

domain-name: Specifies a PKI domain by its name, a case-insensitive string of 1 to 31 characters. The domain name cannot contain the special characters listed in Table 8-6 .

Table 8-6 Special characters

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar	|	Quotation marks	"
Colon	:	Apostrophe	'

Usage guidelines

Use this command to determine whether a certificate has been revoked.

Examples

Display information about the CRL saved at the local for PKI domain **aaa**.

```
<Switch> display pki crl domain aaa
Certificate Revocation List (CRL):
        Version 2 (0x1)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: /C=cn/O=docm/OU=sec/CN=therootca
        Last Update: Apr 28 01:42:13 2011 GMT
        Next Update: NONE
        CRL extensions:
            X509v3 CRL Number:
                6
            X509v3 Authority Key Identifier:
                keyid:49:25:DB:07:3A:C4:8A:C2:B5:A0:64:A5:F1:54:93:69:14:51:11:EF

Revoked Certificates:
```

```
Serial Number: CDE626BF7A44A727B25F9CD81475C004
    Revocation Date: Apr 28 01:37:52 2011 GMT
    CRL entry extensions:
        Invalidity Date:
            Apr 28 01:37:49 2011 GMT
Serial Number: FCADFA81E1F56F43D3F2D3EF7EB56DE5
    Revocation Date: Apr 28 01:33:28 2011 GMT
    CRL entry extensions:
        Invalidity Date:
            Apr 28 01:33:09 2011 GMT
Signature Algorithm: sha1WithRSAEncryption
    57:ac:00:3e:1e:e2:5f:59:62:04:05:9b:c7:61:58:2a:df:a4:
    5c:e5:c0:14:af:c8:e7:de:cf:2a:0a:31:7d:32:da:be:cd:6a:
    36:b5:83:e8:95:06:bd:b4:c0:36:fe:91:7c:77:d9:00:0f:9e:
    99:03:65:9e:0c:9c:16:22:ef:4a:40:ec:59:40:60:53:4a:fc:
    8e:47:57:23:e0:75:0a:a4:1c:0e:2f:3d:e0:b2:87:4d:61:8a:
    4a:cb:cb:37:af:51:bd:53:78:76:a1:16:3d:0b:89:01:91:61:
    52:d0:6f:5c:09:59:15:be:b8:68:65:0c:5d:1b:a1:f8:42:04:
    ba:aa
```

Table 8-7 Command output

Field	Description
Version	CRL version number.
Signature Algorithm	Signature algorithm used by the CA to sign the CRL.
Issuer	Name of the CA that issued the CRL.
Last Update	Most recent CRL update time.
Next Update	Next CRL update time.
X509v3 Authority Key Identifier	X509v3 ID of the CA that issues the CRL.
keyid	Key ID. This field identifies the key pair used to sign the CRL.
Signature Algorithm:	Signature algorithm and signature data.

Related commands

pki retrieve-crl

8.1.17. fqdn

Use **fqdn** to set the FQDN of an entity.

Use **undo fqdn** to restore the default.

Syntax

fqdn *fqdn-name-string*

undo fqdn

Default

No FQDN is set for a PKI entity.

Views

PKI entity view

Predefined user roles

network-admin

Parameters

fqdn-name-string: Specifies an FQDN, a case-sensitive string of 1 to 255 characters in the format *hostname*@*domainname*.

Usage guidelines

An FQDN uniquely identifies a PKI entity on a network.

Examples

Set the FQDN to **pki.domain-name.com** for PKI entity **en**.

```
<Switch> system-view
[Switch] pki entity en
[Switch-pki-entity-en] fqdn abc@pki.domain.com
```

8.1.18. ip

Use **ip** to assign an IP address to a PKI entity.

Use **undo ip** to restore the default.

Syntax

ip { *ip-address* | **interface** *interface-type interface-number* }

undo ip

Default

No IP address is assigned to the PKI entity.

Views

PKI entity view

Predefined user roles

network-admin

Parameters

ip-address: Specifies an IPv4 address.

interface *interface-type interface-number*: Specifies an interface by its type and number. The primary IPv4 address of the interface will be used as the IP address of the PKI entity.

Usage guidelines

Use this command to assign an IP address to a PKI entity or specify an interface for the entity. The interface's primary IPv4 address will be used as the IP address of the PKI entity. If you specify an interface, make sure the interface is assigned an IP address before the PKI entity requests a certificate.

Examples

Assign IP address **192.168.0.2** to PKI entity **en**.

```
<Switch> system-view
[Switch] pki entity en
[Switch-pki-entity-en] ip 192.168.0.2
```

8.1.19. locality

Use **locality** to set the locality of a PKI entity.

Use **undo locality** to restore the default.

Syntax

locality *locality-name*

undo locality

Default

No locality is set for a PKI entity.

Views

PKI entity view

Predefined user roles

network-admin

Parameters

locality-name: Specifies a locality, a case-sensitive string of 1 to 63 characters. No comma can be included. You can set a city name as the locality.

Examples

Set the locality to **pukras** for PKI entity **en**.

```
<Switch> system-view
[Switch] pki entity en
[Switch-pki-entity-en] locality pukras
```

8.1.20. organization

Use **organization** to set an organization name for a PKI entity.

Use **undo organization** to restore the default.

Syntax

organization *org-name*

undo organization

Default

No organization name is set for a PKI entity.

Views

PKI entity view

Predefined user roles

network-admin

Parameters

org-name: Specifies an organization name, a case-sensitive string of 1 to 63 characters. No comma can be included.

Examples

Set the organization name to **abc** for PKI entity **en**.

```
<Switch> system-view
[Switch] pki entity en
[Switch-pki-entity-en] organization abc
```

8.1.21. organization-unit

Use **organization-unit** to set an organization unit name for a PKI entity.

Use **undo organization-unit** to restore the default.

Syntax

organization-unit *org-unit-name*

undo organization-unit

Default

No organization unit name is set for a PKI entity.

Views

PKI entity view

Predefined user roles

network-admin

Parameters

org-unit-name: Specifies an organization unit name, a case-sensitive string of 1 to 63 characters. No commas can be included.

Examples

Set the organization unit name to **rdtest** for PKI entity **en**.

```
<Switch> system-view
[Switch] pki entity en
[Switch-pki-entity-en] organization-unit rdtest
```

8.1.22. pki abort-certificate-request

Use **pki abort-certificate-request** to abort the certificate request for a PKI domain.

Syntax

pki abort-certificate-request domain *domain-name*

Views

System view

Predefined user roles

network-admin

Parameters

domain-name: Specifies a PKI domain by its name, a case-insensitive string of 1 to 31 characters. The domain name cannot contain the special characters listed in Table 8-8 .

Table 8-8 Special characters

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar	|	Quotation marks	"
Colon	:	Apostrophe	'

Usage guidelines

You can abort a certificate request and change some parameters, such as common name, country code, or FQDN, in the certificate request before the CA issues the certificate. Use the **display pki certificate request-status** command to display the certificate request status.

Examples

Abort the certificate request for PKI domain **1**.

```
<Switch> system-view
[Switch] pki abort-certificate-request domain 1
The certificate request is in process.
Confirm to abort it? [Y/N]:y
```

Related commands

display pki certificate request-status

pki request-certificate domain

8.1.23. pki certificate access-control-policy

Use **pki certificate access-control-policy** to create a certificate-based access control policy and enter its view, or enter the view of an existing certificate-based access control policy.

Use **undo pki certificate access-control-policy** to remove a certificate-based access control policy.

Syntax

pki certificate access-control-policy *policy-name*

undo pki certificate access-control-policy *policy-name*

Default

No certificate-based access control policies exist.

Views

System view

Predefined user roles

network-admin

Parameters

policy-name: Specifies a policy name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

A certificate-based access control policy contains a set of access control rules that permit or deny access to the device based on the attributes in the requesting client's certificate.

Examples

Create a certificate-based access control policy named **mypolicy** and enter its view.

```
<Switch> system-view
[Switch] pki certificate access-control-policy mypolicy
[Switch-pki-cert-acp-mypolicy]
```

Related commands

display pki certificate access-control-policy

8.1.24. pki certificate attribute-group

Use **pki certificate attribute-group** to create a certificate attribute group and enter its view, or enter the view of an existing certificate attribute group.

Use **undo pki certificate attribute-group** to remove a certificate attribute group.

Syntax

pki certificate attribute-group *group-name*

undo pki certificate attribute-group *group-name*

Default

No certificate attribute groups exist.

Views

System view

Predefined user roles

network-admin

Parameters

group-name: Specifies a group name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

A certificate attribute group is a set of attribute rules configured by using the **attribute** command. Each attribute rule defines a matching criterion for an attribute in the issuer name, subject name, or alternative subject name field of certificates.

A certificate attribute group must be associated with an access control rule. If a certificate attribute group does not have any attribute rules, the system determines that the all certificates match the associated access control rule.

Examples

Create a certificate attribute group named **mygroup** and enter its view.

```
<Switch> system-view
[Switch] pki certificate attribute-group mygroup
[Switch-pki-cert-attribute-group-mygroup]
```

Related commands

attribute

display pki certificate attribute-group

8.1.25. pki delete-certificate

Use **pki delete-certificate** to remove certificates from a PKI domain.

Syntax

pki delete-certificate domain *domain-name* { **ca** | **local** }

Views

System view

Predefined user roles

network-admin

Parameters

domain-name: Specifies a PKI domain by its name, a case-insensitive string of 1 to 31 characters. The domain name cannot contain the special characters listed in Table 8-9 .

Table 8-9 Special characters

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar	|	Quotation marks	"
Colon	:	Apostrophe	'

ca: Specifies the CA certificate.

local: Specifies the local certificates.

Usage guidelines

When you remove the CA certificate in a PKI domain, the system also removes the local certificates, peer certificates, and the CRL in the PKI domain.

To delete a specific peer certificate in a PKI domain, perform the following steps:

1. Execute the **display pki certificate** command to determine the serial number of the peer certificate.

Examples

Remove the CA certificate in PKI domain **aaa**.

```
<Switch> system-view
[Switch] pki delete-certificate domain aaa ca
Local certificates, peer certificates and CRL will also be deleted while deleting the CA certificate.
Confirm to delete the CA certificate? [Y/N]:y
[Switch]
```

Remove the local certificates in PKI domain **aaa**.

```
<Switch> system-view
[Switch] pki delete-certificate domain aaa local
[Switch]
```

Related commands

display pki certificate

8.1.26. pki domain

Use **pki domain** to create a PKI domain and enter its view, or enter the view of an existing PKI domain.

Use **undo pki domain** to remove a PKI domain.

Syntax

pki domain *domain-name*

undo pki domain *domain-name*

Default

No PKI domains exist.

Views

System view

Predefined user roles

network-admin

Parameters

domain-name: Specifies a PKI domain name, a case-insensitive string of 1 to 31 characters. The domain name cannot contain the special characters listed in Table 8-10 .

Table 8-10 Special characters

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar	|	Quotation marks	"
Colon	:	Apostrophe	'

Usage guidelines

When you remove a PKI domain, the certificates and the CRL in the domain are also removed.

Examples

Create a PKI domain named **aaa** and enter its view.

```
<Switch> system-view
[Switch] pki domain aaa
[Switch-pki-domain-aaa]
```

8.1.27. pki entity

Use **pki entity** to create a PKI entity and enter its view, or enter the view of an existing PKI entity.

Use **undo pki entity** to remove a PKI entity.

Syntax

pki entity *entity-name*

undo pki entity *entity-name*

Default

No PKI entities exist.

Views

System view

Predefined user roles

network-admin

Parameters

entity-name: Specifies a name for a PKI entity, a case-insensitive string of 1 to 31 characters.

Usage guidelines

A PKI entity includes the identity information that can be used by a CA to identify a certificate applicant. You can configure multiple attributes for a PKI entity, such as common name, organization, organization unit, locality, state, country, FQDN, and IP address. The information will be included as subject contents in the certificate issued by the CA.

Examples

Create a PKI entity named **en** and enter its view.

```
<Switch> system-view
[Switch] pki entity en
[Switch-pki-entity-en]
```

Related commands

pki domain

8.1.28. pki import

Use **pki import** to import the CA certificate, local certificates, or peer certificates for a PKI domain.

Syntax

pki import domain *domain-name* { **der** { **ca** | **local** | **peer** } **filename** *filename* | **p12 local filename** *filename* | **pem** { **ca** | **local** | **peer** } [**filename** *filename*] }

Views

System view

Predefined user roles

network-admin

Parameters

domain-name: Specifies a PKI domain by its name, a case-insensitive string of 1 to 31 characters. The domain name cannot contain the special characters listed in Table 8-11 .

Table 8-11 Special characters

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar	|	Quotation marks	"
Colon	:	Apostrophe	'

der: Specifies the DER certificate file format, including PKCS#7.

p12: Specifies the PKCS#12 certificate file format.

pem: Specifies the PEM certificate file format.

ca: Specifies the CA certificate.

local: Specifies the local certificates.

peer: Specifies the peer certificates.

filename *filename*: Specifies a certificate file name, a case-insensitive string. For a certificate in PEM format, you can also choose to copy and paste the certificate contents on the terminal instead of importing from a file.

Usage guidelines

Use this command to import a certificate in the following situations:

- The CRL repository is not specified or the CA server does not support SCEP.
- The certificate is packed with the server generated key pair in a single file. Only certificate files in PKCS12 or PEM format can contain key pairs.

Before you import certificates, complete the following tasks:

- Use FTP or TFTP to upload the certificate files to the storage media of the device. If FTP or TFTP is not available, display and copy the contents of a certificate to a file on the device. Make sure the certificate is in PEM format because only certificates in PEM format can be imported by this means.
- For the local certificates or peer certificates to be imported, the correct CA certificate chain must exist. The CA certificate chain can be stored on the device, or carried in the local certificates or peer certificates. If the PKI domain, the local certificates, or the peer certificates do not have the CA certificate chain, you must import the CA certificate first. To import a local or peer certificate, a CA certificate chain must exist in the PKI domain, or be carried in the local or peer certificate. If not, obtain it first.

When you import the local or peer certificates:

- If the local or peer certificates contain the CA certificate chain, you can import the CA certificate and the local or peer certificates at the same time. If the CA certificate already exists in a PKI domain, the system prompts you whether to overwrite the existing CA certificate.
- If the local or peer certificates do not contain the CA certificate chain, but the CA certificate already exists in a PKI domain, you can directly import the certificates.

You can import the CA certificate to a PKI domain when either of the following conditions is met:

- The CA certificate to be imported is the root CA certificate or contains the certificate chain with the root certificate.
- The CA certificate contains a certificate chain without the root certificate, but can form a complete certificate chain with an existing CA certificate on the device.

Contact the CA administrator to get information as prompted in the following scenarios:

- The system prompts you to confirm the certificate's fingerprint in the following situation:
  - The certificate file to be imported contains the root certificate, but the root certificate does not exist in any PKI domains on the device.
  - The **root-certificate fingerprint** command is not configured in the PKI domain to which the certificate file is to be imported.
- The system prompts you to enter the challenge password used for encrypting the private key if the local certificate to be imported contains a key pair.

When you import a local certificate file that contains a key pair, you can choose to update the domain with the key pair. Depending on the purpose of the key pair, the following conditions might apply:

- If the purpose of the key pair is general, the device uses the key pair to replace the local key pair that is found in this order:
  a. General-purpose key pair.
  b. Signature key pair.
  c. Encryption key pair.
- If the purpose of the key pair is signature, the device uses the key pair to replace the local key pair that is found in this order:
  a. General-purpose key pair.
  b. Signature key pair.
- If the purpose of the key pair is encryption, the device searches the domain for an encryption key pair.

If a matching key pair is found, the device asks whether you want to overwrite the existing key pair on the device. If no match is found, the device asks you to enter a key pair name (defaulting to the PKI domain name). Then, it generates the key pair according to the key algorithm and the purpose defined in the certificate file.

The import operation automatically updates or generates the correct key pair. When you perform the import operation, be sure to save the configuration file to avoid data loss.

Examples

Import CA certificate file **rootca_pem.cer** in PEM format to PKI domain **aaa**. The certificate file contains the root certificate.

```
<Switch> system-view
[Switch] pki import domain aaa pem ca filename rootca_pem.cer
The trusted CA's finger print is:
    MD5  fingerprint:FFFF 3EFF FFFF 37FF FFFF 137B FFFF 7535
    SHA1 fingerprint:FFFF FF7F FF2B FFFF 7618 FF4C FFFF 0A7D FFFF FF69
Is the finger print correct?(Y/N):y
[Switch]
```

Import CA certificate file **aca_pem.cer** in PEM format to PKI domain **bbb**. The certificate file does not contain the root certificate.

```
<Switch> system-view
[Switch] pki import domain bbb pem ca filename aca_pem.cer
[Switch]
```

Import local certificate file **local-ca.p12** in PKCS12 format to PKI domain **bbb**. The certificate file contains a key pair.

```
<Switch> system-view
[Switch] pki import domain bbb p12 local filename local-ca.p12
Please input challenge password:
******
[Switch]
```

Import the local certificate in PEM format to PKI domain **bbb** by copying and pasting the contents of the certificate. The certificate contains the key pair and the CA certificate chain.

```
<Switch> system-view
[Switch] pki import domain bbb pem local
Enter PEM-formatted certificate.
End with a Ctrl+c on a line by itself.
Bag Attributes
localKeyID: 01 00 00 00
friendlyName: {F7619D96-3AC2-40D4-B6F3-4EAB73DEED73}
Microsoft CSP Name: Microsoft Enhanced Cryptographic Provider v1.0
Key Attributes
X509v3 Key Usage: 10
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,8DCE37F0A61A4B8C

k9C3KHY5S3EtnF5iQymvHYYrVFy5ZdjSasU5y4XFubjdcvmpFHQteMjD0GKX6+xO
kuKbvpyCnWsPVg56sL/PDRyrRmqLmtUV3bpyQsFXgnc7p+Snj3CG2Ciow9XApybW
Ec1TDCD75yuQckpVQdhguTvoPQXf9zHmiGu5jLkySp2k7ec/Mc97Ef+qqpfnHpQp
GDmMqnFpp59ZzB21OGlbGzlPcsjoT+EGpZg6B1KrPiCyFim95L9dWVwX9sk+U1s2
+8wqac8jETwwM0UZ1NGJ50JJz1QYIzMbcrw+S5WlPxACTIz1cldlBlb1kpc+7mcX
4W+MxFzsL88IJ99T72eu4iUNsy26g0BZMAcc1sJA3A4w9RNhfs9hSG43S3hAh5li
JPp720LfYBlkQHn/MgMCZASWDJ5G0eSXQt9QymHAth4BiT9v7zetnQqf4q8plfd/
Xqd9zEFlBPpoJFtJqXwxHUCKgw6kJeC4CxHvi9ZCJU/upg9IpiguFPoaDOPia+Pm
GbRqSyy55clVde5GOccGN1DZ94DW7AypazgLpBbrkIYAdjFPRmq+zMOdyqsGMTNj
jnheI5l784pNOAKuGi0i/uXmRRcfoMh6qAnK6YZGS7rOLC9CfPmy8fgY+/Sl9d9x
Q00ruO1psxzh9c2YfuaiXFIx0auKl6o5+ZZYn7Rg/xy2Y0awVP+dO925GoAcHO40
cCl6jA/HsGAU9HkpwKHL35lmBDRLEzQeBFcaGwSm1JvRfE4tkJM7+Uz2QHJOfP10
0VLqMgxMlpk3TvBWgzHGJDe7TdzFCDPMPhod8pi4P8gGXmQd01PbyQ==
-----END RSA PRIVATE KEY-----
Bag Attributes
localKeyID: 01 00 00 00
subject=/CN=sldsslserver
issuer=/C=cn/O=ccc/OU=sec/CN=ssl
-----BEGIN CERTIFICATE-----
MIICjzCCAfigAwIBAgIRAJoDN+shVrofVHbk11SlqfcwDQYJKoZIhvcNAQEFBQAw
NzELMAkGA1UEBhMCY24xDDAKBgNVBAoTA2gzYzEMMAoGA1UECxMDc2VjMQwwCgYD
VQQDEwNzc2wwHhcNMTAxMDE1MDEyMzA2WhcNMTIwNzI2MDYzMDU0WjAXMRUwEwYD
VQQDEwxzbGRzc2xzZXJ2ZXIwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMLP
N3aTKV7NDndIOk0PpiikYPgxVih/geMXR3iYaANbcvRX07/FMDINWHJnBAZhCDvp
rFO552loGiPyl0wmFMK12TSL7sHvrxr0OdrFrqtWlbW+DsNGNcFSKZy3RvIngC2k
```

```
ZZqBeFPUytP185JUhbOrVaUDlisZi6NNshcIjd2BAgMBAAGjgbowgbcwHwYDVR0j
BBgwFoAUmoMpEynZYoPLQdR1LlKhZjg8kBEwDgYDVR0PAQH/BAQDAgP4MBEGCWCG
SAGG+EIBAQQEAwIGQDASBgNVHREECzAJggdoM2MuY29tMB0GA1UdDgQWBBQ8dpWb
3cJ/X5iDt8eg+JkeS9cvJjA+BgNVHR8ENzA1MDOgMaAvhi1odHRwOi8vczAzMTMw
LmgzYy5odWF3ZWktM2NvbS5jb206NDQ3L3NzbC5jcmwwDQYJKoZIhvcNAQEFBQAD
gYEAYS15x0kW474lu4twNzEy5dPjMSwtwfm/UK01S8GQjGV5tl9ZNiTHFGNEFx7k
zxBp/JPpcFM8hapAfrVHdQ/wstq0pVDdBkrVF6XKIBks6XgCvRl32gcaQt9yrQd9
5RbWdetuBljudjFj25airYO2u7pLeVmdWWx3WVvZBzOo8KU=
-----END CERTIFICATE-----
Bag Attributes: <Empty Attributes>
subject=/C=cn/O=ccc/OU=sec/CN=ssl
issuer=/C=cn/O=ccc/OU=sec/CN=ssl
-----BEGIN CERTIFICATE-----
MIIB7DCCAVUCEG+jJTPxxiE67pl2ff0SnOMwDQYJKoZIhvcNAQEFBQAwNzELMAkG
A1UEBhMCY24xDDAKBgNVBAoTA2gzYzEMMAoGA1UECxMDc2VjMQwwCgYDVQQDEwNz
c2wwHhcNMDkwNzMxMDY0ODQ2WhcNMTIwNzI5MDYyODU4WjA3MQswCQYDVQQGEwJj
bjEMMAoGA1UEChMDaDNjMQwwCgYDVQQLEwNzZWMxDDAKBgNVBAMTA3NzbDCBnzAN
BgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAt8QSMetQ70GONiFh7iJkvGQ8nC15zCF1
cqC/RcJhE/88LkKyQcu9j+Tz8Bk9Qj2UPaZdrk8fOrgtBsa7lZ+UO3j3l30q84l+
HjWq8yxVLRQahU3gqJze6pGR2l0s76u6GRyCX/zizGrHKqYlNnxK44NyRZx2klQ2
tKQAfpXCPIkCAwEAATANBgkqhkiG9w0BAQUFAAOBgQBWsaMgRbBMtYNrrYCMjY6g
c7PBjvajVOKNUMxaDalePmXfKCxl91+PKM7+i8I/zLcoQO+sHbva26a2/C4sNvoJ
2QZs6GtAOahP6CDqXC5VuNBU6eTKNKjL+mf6uuDeMxrlDNha0iymdrXXVIp5cuIu
fl7xgArs8Ks6aXDXM1o4DQ==
-----END CERTIFICATE-----


Please input the password:********
Local certificate already exist, confirm to overwrite it? [Y/N]:y
The PKI domain already has a CA certificate. If it is overwritten, local certificates,
peer certificates and CRL of this domain will also be deleted.
Overwrite it? [Y/N]:y
The system is going to save the key pair. You must specify a key pair name, which is a
case-insensitive string of 1 to 64 characters. Valid characters include a to z, A to Z,
0 to 9, and hyphens (-).
Please enter the key pair name [default name: bbb]:

The key pair already exists.
Please enter the key pair name:
import-key
```

Related commands

display pki certificate

public-key dsa

public-key ecdsa

public-key rsa

8.1.29. pki request-certificate

Use **pki request-certificate** to submit a local certificate request or generate a certificate request in PKCS#10 format.

Syntax

pki request-certificate domain *domain-name* [**password** *password*] [**pkcs10** [**filename** *filename*]]

Views

System view

Predefined user roles

network-admin

Parameters

domain-name: Specifies a PKI domain by its name, a case-insensitive string of 1 to 31 characters. The domain name cannot contain the special characters listed in Table 8-12 .

Table 8-12 Special characters

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar	|	Quotation marks	"
Colon	:	Apostrophe	'

password *password*: Sets the password for certificate revocation, a case-sensitive string of 1 to 31 characters. The password is contained in the certificate request and must be provided if the certificate is revoked.

pkcs10: Displays BASE64-encoded PKCS#10 certificate request information, which can be used to request a certificate by an out-of-band means, like phone, disk, or email.

filename *filename*: Specifies a local file for saving the certificate request in PKCS#10 format. The *filename* argument is case-insensitive.

Usage guidelines

If SCEP fails, you can perform one of the following tasks:

- Use the **pkcs10** keyword to print the BASE64-encoded request information.
- Use the **pkcs10 filename** *filename* option to save the request information to a local file and transfer the file to the CA by using an out-of-band means. The file name can contain an absolute path. If the specified path does exist, the request information cannot be saved.

This command is not saved in the configuration file.

Examples

Display information about the certificate request in PKCS#10 format.

```
<Switch> system-view
[Switch] pki request-certificate domain aaa pkcs10

*** Request for general certificate ***
```

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBTDCBtgIBADANMQswCQYDVQQDEwJqajCBnzANBgkqhkiG9w0BAQEFAAOBjQAw
gYkCgYEAw5Drj8ofs9THA4ezkDcQPBy8pvH1kumampPsJmx8sGG52NFtbrDTnTT5
ALx3LJijB3d/ndKpcHT/DfbJVDCn5gdw32tBZyCkEwMHZN3ol2z7Nmdcu5TED6iN8
4m+hfp1QWoV6lty3o9pxAXuQl8peUDcfN6WV3LBXYyl1WCtkLkECAwEAAaAAMA0G
CSqGSIb3DQEBBAUAA4GBAA8E7BaIdmT6NVCZgv/I/1tqZH3TS4e4H9Qo5NiCKiEw
R8owVmA0XVtGMbyqBNcDTG0f5NbHrXZQT5+MbFJOnm5K/mn1ro5TJKMTKV46PlCZ
JUjsugaY02GBY0BVcylpC9iIXLuXNIqjh1MBIqVsa1lQOHS7YMvnop6hXAQlkM4c
-----END NEW CERTIFICATE REQUEST-----
```

Request the local certificates.

```
[Switch] pki request-certificate domain openca
Start to request general certificate ...
…
Request certificate of domain openca successfully
```

Related commands

display pki certificate

8.1.30. pki retrieve-certificate

Use **pki retrieve-certificate** to obtain a certificate from the certificate distribution server.

Syntax

pki retrieve-certificate domain *domain-name* { **ca** | **local** }

Views

System view

Predefined user roles

network-admin

Parameters

domain-name: Specifies a PKI domain by its name, a case-insensitive string of 1 to 31 characters. The domain name cannot contain the special characters listed in Table 8-13 .

Table 8-13 Special characters

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar	|	Quotation marks	"
Colon	:	Apostrophe	'

ca: Specifies the CA certificate.

local: Specifies the local certificates.

Usage guidelines

In online mode:

- You can obtain the CA certificate through the SCEP protocol. If a CA certificate already exists locally, do not obtain the CA certificate again. To obtain a new CA certificate, use the **pki delete-certificate** command to remove the CA certificate and local certificates, and then obtain the CA certificate again.
- If a PKI domain already has local certificates, you can still perform the obtain operation and the obtained local certificates or peer certificates overwrite the existing ones. If RSA is used, a PKI domain can have two local certificates, one for signing and the other for encryption. Certificates for different purposes do not overwrite each other.

The obtained CA certificate, local certificates, and peer certificates are automatically verified before they are saved locally. If the verification fails, they are not saved.

This command is not saved in the configuration file.

Examples

Obtain the CA certificate from the certificate distribution server. (This operation requires the user to confirm the fingerprint of the root CA certificate.)

```
<Switch> system-view
[Switch] pki retrieve-certificate domain aaa ca
The trusted CA's finger print is:
    MD5  fingerprint:5C41 E657 A0D6 ECB4 6BD6 1823 7473 AABC
    SHA1 fingerprint:1616 E7A5 D89A 2A99 9419 1C12 D696 8228 87BC C266
Is the finger print correct?(Y/N):y
```

Obtain the local certificates from the certificate distribution server.

```
<Switch> system-view
[Switch] pki retrieve-certificate domain aaa local
```

Obtain the certificate of the peer entity **en1** from the certificate distribution server.

```
<Switch> system-view
[Switch] pki retrieve-certificate domain aaa peer en1
```

Related commands

display pki certificate

pki delete-certificate

8.1.31. pki retrieve-crl

Use **pki retrieve-crl** to obtain CRLs and save them locally.

Syntax

pki retrieve-crl domain *domain-name*

Views

System view

Predefined user roles

network-admin

Parameters

domain-name: Specifies a PKI domain by its name, a case-insensitive string of 1 to 31 characters. The domain name cannot contain the special characters listed in Table 8-14 .

Table 8-14 Special characters

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar	|	Quotation marks	"
Colon	:	Apostrophe	'

Usage guidelines

CRLs are used to verify the validity of the local certificates and the peer certificates in a PKI domain. To obtain CRLs, a PKI domain must have the correct CA certificate.

The URL of the CRL repository is specified by using the **crl url** command.

The device can obtain CRLs from the CRL repository through the HTTP, or SCEP protocol. Which protocol is used depends on the configuration of the CRL repository in the PKI domain:

- If the specified URL of the CRL repository is in HTTP format, the device obtains CRLs through the HTTP protocol.
- If the PKI domain is not configured with the CRL repository, the device looks up the local certificates and then the CA certificate for the CRL repository. If a CRL repository is found, the device obtains CRLs from the CRL repository. If no CRL repository is found, the device obtains CRLs through the SCEP protocol.

Examples

Obtain CRLs from the CRL repository.

```
<Switch> system-view
[Switch] pki retrieve-crl domain aaa
```

Related commands

crl url

8.1.32. pki storage

Use **pki storage** to specify the storage path for the certificates or CRLs.

Use **undo pki storage** to restore the default.

Syntax

pki storage { **certificates** | **crls** } *dir-path*

undo pki storage { **certificates** | **crls** }

Default

Certificates and CRLs are stored in the **PKI** directory on the storage media of the device. The **PKI** directory is automatically created when a certificate is successfully requested, obtained, or imported for the first time.

Views

System view

Predefined user roles

network-admin

Parameters

certificates: Specifies a storage path for certificates.

crls: Specifies a storage path for CRLs.

dir-path: Specifies a storage path, a case-sensitive string, which cannot start with a slash (/) or contain two dots plus a slash (../). The *dir-path* argument specifies an absolute path or a relative path, and the path must exist.

Usage guidelines

The specified storage path must be on the master device.

If the path to be specified does not exist, use the **mkdir** command to create the path first.

Certificate files use the .cer or .p12 file extension. CRL files use the .crl file extension. After you change the storage path for certificates or CRLs, the certificate files and CRL files in the original path are moved to the new path.

Examples

Specifies **flash:/pki-new** as the storage path for certificates.

```
<Switch> system-view
[Switch] pki storage certificates flash:/pki-new
```

Specifies **pki-new** as the storage path for CRLs.

```
<Switch> system-view
[Switch] pki storage crls pki-new
```

8.1.33. pki validate-certificate

Use **pki validate-certificate** to verify the validity of certificates.

Syntax

pki validate-certificate domain *domain-name* { **ca** | **local** }

Views

System view

Predefined user roles

network-admin

Parameters

domain-name: Specifies a PKI domain by its name, a case-insensitive string of 1 to 31 characters. The domain name cannot contain the special characters listed in Table 8-15 .

Table 8-15 Special characters

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar	|	Quotation marks	"
Colon	:	Apostrophe	'

ca: Specifies the CA certificate.

local: Specifies the local certificates.

Usage guidelines

Generally, certificates are automatically verified when you request, obtain, or import them, or when an application uses PKI.

You can also use this command to manually verify a certificate in the following aspects:

- Whether the certificate is issued by a trusted CA.
- Whether the certificate has expired.
- Whether the certificate is revoked. This check is performed only if CRL checking is enabled.

When CRL checking is enabled:

- To verify the local certificates, if the PKI domain has no CRLs, the device looks up the locally saved CRLs. If a correct CRL is found, the device loads the CRL to the PKI domain. If no correct CRL is found locally, the device obtains a correct CRL from the CA server and saves it locally.
- To verify the CA certificate, CRL checking is performed for the CA certificate chain from the current CA to the root CA.

Examples

Verify the validity of the CA certificate in PKI domain **aaa**.

```
<Switch> system-view
[Switch] pki validate-certificate domain aaa ca
Verifying certificate......
        Serial Number:
            f6:3c:15:31:fe:bb:ec:94:dc:3d:b9:3a:d9:07:70:e5
        Issuer:
            C=cn
            O=ccc
            OU=ppp
            CN=rootca
        Subject:
            C=cn
            O=abc
            OU=test
            CN=aca

Verify result: OK
Verifying certificate......
        Serial Number:
            5c:72:dc:c4:a5:43:cd:f9:32:b9:c1:90:8f:dd:50:f6
        Issuer:
            C=cn
            O=ccc
            OU=ppp
            CN=rootca
        Subject:
            C=cn
            O=ccc
            OU=ppp
            CN=rootca
```

```
Verify result: OK
```

Verify the local certificates in PKI domain **aaa**.

```
<Switch> system-view
[Switch] pki validate-certificate domain aaa local
Verifying certificate......
        Serial Number:
            bc:05:70:1f:0e:da:0d:10:16:1e
        Issuer:
            C=CN
            O=sec
            OU=software
            CN=bca
        Subject:
            O=OpenCA Labs
            OU=Users
            CN=fips fips-sec

Verify result: OK
```

Related commands

crl check

pki domain

8.1.34. public-key dsa

Use **public-key dsa** to specify a DSA key pair for certificate request.

Use **undo public-key** to restore the default.

Syntax

public-key dsa name *key-name* [**length** *key-length*]

undo public-key

Default

No key pair is specified for certificate request.

Views

PKI domain view

Predefined user roles

network-admin

Parameters

name *key-name*: Specifies a key pair by its name, a case-insensitive string of 1 to 64 characters. The key pair name can contain only letters, digits, and hyphens (-).

length *key-length*: Specifies the key length, in bits. The value range is 512 to 2048, and the default is 1024. A longer key means higher security but more public key calculation time.

Usage guidelines

You can specify a nonexistent key pair in this command. A key pair can be obtained in any of the following ways:

- Use the **public-key local create** command to generate a key pair.
- An application, like IKE using digital signature authentication, triggers the device to generate a key pair.
- Use the **pki import** command to import a certificate containing a key pair.

A PKI domain can have key pairs using only one type of cryptographic algorithm (DSA, ECDSA, or RSA).

If you configure a DSA key pair for a PKI domain multiple times, the most recent configuration takes effect.

The **length** *key-length* option takes effect only if you specify a nonexistent key pair. The device will automatically create the key pair by using the specified name and length before submitting a certificate request. The **length** *key-length* option is ignored if the specified key pair already exists or is already contained in an imported certificate.

Examples

Specify 2048-bit DSA key pair **abc** for certificate request.

```
<Switch> system-view
[Switch] pki domain aaa
[Switch-pki-domain-aaa] public-key dsa name abc length 2048
```

Related commands

pki import

public-key local create

8.1.35. public-key ecdsa

Use **public-key ecdsa** to specify an ECDSA key pair for certificate request.

Use **undo public-key** to restore the default.

Syntax

public-key ecdsa name *key-name* [**secp192r1** | **secp256r1** | **secp384r1** | **secp521r1**]

undo public-key

Default

No key pair is specified for certificate request.

Views

PKI domain view

Predefined user roles

network-admin

Parameters

name *key-name*: Specifies a key pair by its name, a case-insensitive string of 1 to 64 characters. The key pair name can contain only letters, digits, and hyphens (-).

secp192r1: Uses the secp192r1 curve to generate the key pair. The secp192r1 curve is used by default.

secp256r1: Uses the secp256r1 curve to generate the key pair.

secp384r1: Uses the secp384r1 curve to generate the key pair.

secp521r1: Uses the secp521r1 curve to generate the key pair.

Usage guidelines

You can specify a nonexistent key pair for a PKI domain.

A key pair can be obtained in any of the following ways:

- Use the **public-key local create** command to generate a key pair.
- An application, like IKE using digital signature authentication, triggers the device to generate a key pair.
- Use the **pki import** command to import a certificate containing a key pair.

A PKI domain can have key pairs using only one type of cryptographic algorithm (DSA, ECDSA, or RSA).

If you configure an ECDSA key pair for a PKI domain multiple times, the most recent configuration takes effect.

The specified elliptic curve takes effect only if you specify a nonexistent key pair. The device will automatically create the key pair by using the specified name and curve before submitting a certificate request. The curve parameter is ignored if the specified key pair already exists or is already contained in an imported certificate.

Examples

Specify 384-bit ECDSA key pair **abc** for certificate request.

```
<Switch> system-view
[Switch] pki domain aaa
[Switch-pki-domain-aaa] public-key ecdsa name abc secp384r1
```

Related commands

pki import

public-key local create

8.1.36. public-key rsa

Use **public-key rsa** to specify an RSA key pair for certificate request.

Use **undo public-key** to restore the default.

Syntax

public-key rsa { { **encryption name** *encryption-key-name* [**length** *key-length*] | **signature name** *signature-key-name* [**length** *key-length*] } * | **general name** *key-name* [**length** *key-length*] }

undo public-key

Default

No key pair is specified for certificate request.

Views

PKI domain view

Predefined user roles

network-admin

Parameters

encryption: Specifies a key pair for encryption.

name *encryption-key-name*: Specifies a key pair name, a case-insensitive string of 1 to 64 characters. The key pair name can contain only letters, digits, and hyphens (-).

signature: Specifies a key pair for signing.

name *signature-key-name*: Specifies a key pair name, a case-insensitive string of 1 to 64 characters. The key pair name can contain only letters, digits, and hyphens (-).

general: Specifies a key pair for both signing and encryption.

name *key-name*: Specifies a key pair name, a case-insensitive string of 1 to 64 characters. The key pair name can contain only letters, digits, and hyphens (-).

length *key-length*: Specifies the key length, in bits. The value range is 512 to 2048, and the default is 1024. A longer key means higher security but more public key calculation time.

Usage guidelines

You can specify a nonexistent key pair in this command. You can get a key pair in any of the following ways:

- Use the **public-key local create** command to generate a key pair.
- An application, like IKE using digital signature authentication, triggers the device to generate a key pair.
- Use the **pki import** command to import a certificate containing a key pair.

A PKI domain can have key pairs using only one type of cryptographic algorithm (DSA, ECDSA, or RSA).

A PKI domain can have two RSA key pairs of different purposes: one is the signing key pair, and the other is the encryption key pair. If you configure an RSA signing key pair or RSA encryption key pair multiple times, the most recent configuration takes effect. The RSA signing key pair and encryption key pair do not overwrite each other.

If you specify a signing key pair and an encryption key pair separately, their key length can be different.

The **length** *key-length* option takes effect only if you specify a nonexistent key pair. The device will automatically create the key pair by using the specified name and length before submitting a certificate request. The **length** *key-length* option is ignored if the specified key pair already exists or is already contained in an imported certificate.

Examples

Specify 2048-bit general purpose RSA key pair **abc** for certificate request.

```
<Switch> system-view
[Switch] pki domain aaa
[Switch-pki-domain-aaa] public-key rsa general name abc length 2048
```

Specify the following RSA key pairs for certificate request:

- 2048-bit RSA encryption key pair **rsa1**.
- 2048-bit RSA signing key pair **sig1**.

```
<Switch> system-view
[Switch] pki domain aaa
[Switch-pki-domain-aaa] public-key rsa encryption name rsa1 length 2048
```

```
[Switch-pki-domain-aaa] public-key rsa signature name sig1 length 2048
```

Related commands

pki import

public-key local create

8.1.37. root-certificate fingerprint

Use **root-certificate fingerprint** to set the fingerprint for verifying the root CA certificate.

Use **undo root-certificate fingerprint** to restore the default.

Syntax

root-certificate fingerprint { **md5** | **sha1** } *string*

undo root-certificate fingerprint

Default

No fingerprint is set for verifying the root CA certificate.

Views

PKI domain view

Predefined user roles

network-admin

Parameters

md5: Sets an MD5 fingerprint.

sha1: Sets an SHA1 fingerprint.

string: Sets the fingerprint in hexadecimal notation. If you specify the **MD5** keyword, the fingerprint is a string of 32 characters. If you specify the **SHA1** keyword, the fingerprint is a string of 40 characters.

Usage guidelines

If you set the certificate request mode to auto for a PKI domain that does not have a CA certificate, you must configure the fingerprint for root CA certificate verification. When an application (for example, IKE) triggers the device to request local certificates, the device automatically performs the following operations:

1. Obtains the CA certificate from the CA server.
2. Compares the fingerprint contained in the root CA certificate with the fingerprint configured in the PKI domain, if either of the following conditions exists:
   - The obtained CA certificate is a root certificate.
   - The obtained CA certificate is a certificate chain and contains a root certificate that does not exist on the device.

   If the two fingerprints do not match, or if no fingerprint is configured in the PKI domain, the device rejects the CA certificate and the local certificate request fails.

The fingerprint configured by this command is also used for root CA certificate verification when the device performs the following operations:

- Imports the CA certificate as requested by the **pki import** command.
- Obtains the CA certificate as requested by the **pki retrieve-certificate** command.

The device compares the fingerprint contained in the root CA certificate with the fingerprint configured in the PKI domain, if either of the following conditions exists:

- The CA certificate to be imported or obtained is a root certificate that does not exist on the device.
- The CA certificate to be imported or obtained is a certificate chain and contains a root certificate that does not exist on the device.

If the two fingerprints do not match, the device rejects the CA certificate. If no fingerprint is configured in the PKI domain, the device prompts you to manually verify the fingerprint of the root CA certificate.

Examples

Specify an MD5 fingerprint for verifying the root CA certificate.

```
<Switch> system-view
[Switch] pki domain aaa
[Switch-pki-domain-aaa] root-certificate fingerprint md5
12EF53FA355CD23E12EF53FA355CD23E
```

Specify an SHA1 fingerprint for verifying the root CA certificate.

```
<Switch> system-view
[Switch] pki domain aaa
[Switch-pki-domain-aaa] root-certificate fingerprint sha1
D1526110AAD7527FB093ED7FC037B0B3CDDDAD93
```

Related commands

certificate request mode

pki import

pki retrieve-certificate

8.1.38. state

Use **state** to set the state or province name for a PKI entity.

Use **undo state** to restore the default.

Syntax

state *state-name*

undo state

Default

No state name or province name is set for a PKI entity.

Views

PKI entity view

Predefined user roles

network-admin

Parameters

state-name: Specifies a state or province by its name, a case-sensitive string of 1 to 63 characters. No comma can be included.

Examples

Set the state name to **countryA** for PKI entity **en**.

```
<Switch> system-view
[Switch] pki entity en
[Switch-pki-entity-en] state countryA
```

Contents

A page of this section is **9-x-x**

9. SSH commands 9-1
9.1. SSH server commands 9-1
9.1.1. display ssh server 9-1
9.1.2. display ssh user-information 9-2
9.1.3. free ssh 9-3
9.1.4. scp server enable 9-4
9.1.5. sftp server enable 9-5
9.1.6. sftp server idle-timeout 9-5
9.1.7. ssh server acl 9-6
9.1.8. ssh server acl-deny-log enable 9-7
9.1.9. ssh server authentication-retries 9-8
9.1.10. ssh server authentication-timeout 9-9
9.1.11. ssh server compatible-ssh1x enable 9-9
9.1.12. ssh server dscp 9-10
9.1.13. ssh server enable 9-11
9.1.14. ssh server ipv6 acl 9-11
9.1.15. ssh server ipv6 dscp 9-12
9.1.16. ssh server rekey-interval 9-13
9.1.17. ssh user 9-13
9.2. SSH client commands 9-16
9.2.1. bye 9-16
9.2.2. cd 9-16
9.2.3. cdup 9-17
9.2.4. delete 9-17
9.2.5. delete ssh client server-public-key 9-18
9.2.6. dir 9-18
9.2.7. display sftp client source 9-19
9.2.8. display ssh client source 9-20
9.2.9. exit 9-20
9.2.10. get 9-20
9.2.11. help 9-21
9.2.12. ls 9-22
9.2.13. mkdir 9-23
9.2.14. put 9-23
9.2.15. pwd 9-24
9.2.16. quit 9-24
9.2.17. remove 9-24
9.2.18. rename 9-25
9.2.19. rmdir 9-25
9.2.20. scp 9-26
9.2.21. scp ipv6 9-28
9.2.22. sftp 9-30
9.2.23. sftp client ipv6 source 9-32
9.2.24. sftp client source 9-33
9.2.25. sftp ipv6 9-33
9.2.26. ssh client ipv6 source 9-35
9.2.27. ssh client source 9-36
9.2.28. ssh2 9-37
9.2.29. ssh2 ipv6 9-39
9.3. SSH2 commands 9-42
9.3.1. display ssh2 algorithm 9-42
9.3.2. ssh2 algorithm cipher 9-43

9.3.3. ssh2 algorithm key-exchange ····· 9-44
9.3.4. ssh2 algorithm mac ····· 9-45
9.3.5. ssh2 algorithm public-key ····· 9-46

9. SSH commands

9.1. SSH server commands

9.1.1. display ssh server

Use **display ssh server** on an SSH server to display the SSH server status or sessions.

Syntax

display ssh server { **session** | **status** }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

session: Specifies the SSH server sessions.

status: Specifies the SSH server status.

Examples

Display the SSH server status.

```
<Switch> display ssh server status
 Stelnet server: Disable
 SSH version : 2.0
 SSH authentication-timeout : 60 second(s)
 SSH server key generating interval : 0 hour(s)
 SSH authentication retries : 3 time(s)
 SFTP server: Disable
 SFTP server Idle-Timeout: 10 minute(s)
 NETCONF server: Disable
 SCP server: Disable
 SSH Server PKI domain name: aaa
```

Table 9-1 Command output

Field	Description
Stelnet server	Whether the Stelnet server is enabled.
SSH version	SSH protocol version. When the SSH supports SSH1, the protocol version is 1.99. Otherwise, the protocol version is 2.
SSH authentication-timeout	Authentication timeout timer.
SSH server key generating interval	Minimum interval for updating the RSA server key pair.
SSH authentication retries	Maximum number of authentication attempts for SSH

Field	Description
	users.
SFTP server	Whether the SFTP server is enabled.
SFTP server Idle-Timeout	SFTP connection idle timeout timer.
NETCONF server	Whether NETCONF over SSH is enabled.
SCP server	Whether the SCP server is enabled.
SSH Server PKI domain name	Name of the PKI domain specified for the SSH server.

Display the SSH server sessions.

```
<Switch> display ssh server session
UserPid    SessID Ver    Encrypt    State          Retries  Serv     Username
 184         0     2.0    aes128-cbc Established    1        Stelnet  abc@123
```

Table 9-2 Command output

Field	Description
UserPid	User process ID.
SessID	Session ID.
Ver	Protocol version of the SSH server.
Encrypt	Encryption algorithm used on the SSH server.
State	Session state: • **Init**—Initialization. • **Ver-exchange**—Version negotiation. • **Keys-exchange**—Key exchange. • **Auth-request**—Authentication request. • **Serv-request**—Session service request. • **Established**—The session is established. • **Disconnected**—The session is terminated.
Retries	Number of authentication failures.
Serv	Service type: • SCP. • SFTP. • Stelnet. • NETCONF.
Username	Username that the client uses to log in to the server.

9.1.2. display ssh user-information

Use **display ssh user-information** to display information about SSH users on an SSH server.

Syntax

display ssh user-information [*username*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

username: Specifies an SSH username, a case-sensitive string of 1 to 80 characters. If you do not specify an SSH user, this command displays information about all SSH users.

Usage guidelines

This command displays information only about SSH users that are configured by using the **ssh user** command on the SSH server.

Examples

Display information about all SSH users.

```
<Switch> display ssh user-information
 Total ssh users:2
 Username            Authentication-type  User-public-key-name  Service-type
 yemx                password                                   Stelnet|SFTP
 test                publickey            pubkey                SFTP
```

Table 9-3 Command output

Field	Description
Total ssh users	Total number of SSH users.
Authentication-type	Authentication methods: • Password authentication. • Publickey authentication. • Password-publickey authentication. • Any authentication.
User-public-key-name	Public key name of the user. This field is empty if the authentication method is password authentication.
Service-type	Service types: • Stelnet. • SFTP. • SCP. • NETCONF. If multiple service types are available for an SSH user, they are separated by vertical bars (|).

Related commands

ssh user

9.1.3. free ssh

Use **free ssh** to disconnect SSH sessions.

Syntax

free ssh { **user-ip** { *ip-address* | **ipv6** *ipv6-address* } [**port** *port-number*] | **user-pid** *pid-number* | **username** *username* }

Views

User view

Predefined user roles

network-admin

Parameters

user-ip: Specifies the user IP address of the SSH sessions to be disconnected.

ip-address: Specifies the user IPv4 address of the SSH sessions to be disconnected.

ipv6 *ipv6-address:* Specifies the user IPv6 address of the SSH sessions to be disconnected.

port *port-number*: Specifies the source port of the SSH session to be disconnected, in the range of 1 to 65535. If you do not specify a source port, this command disconnects all SSH sessions using the specified IP address.

user-pid *pid-number*: Specifies the user process ID of the SSH session to be disconnected, in the range of 1 to 2147483647. To view the user process ID of an SSH session, use the **display ssh server session** command.

username *username*: Specifies the username of the SSH session to be disconnected. To view the username of an SSH session, use the **display ssh server session** command.

Examples

Disconnect the SSH sessions with user IPv4 address 192.168.15.45.

```
<Switch> free ssh user-ip 192.168.15.45
Releasing SSH connection. Continue? [Y/N]:y
```

Disconnect the SSH sessions with user IPv6 address 2000::11.

```
<Switch> free ssh user-ip ipv6 2000::11
Releasing SSH connection. Continue? [Y/N]:y
```

Disconnect the SSH session with user process ID 417.

```
<Switch> free ssh user-pid 417
Releasing SSH connection. Continue? [Y/N]:y
```

Disconnect the SSH session with username **sshuser**.

```
<Switch> free ssh username sshuser
Releasing SSH connection. Continue? [Y/N]:y
```

Related commands

display ssh server session

9.1.4. scp server enable

Use **scp server enable** to enable the SCP server.

Use **undo scp server enable** to disable the SCP server.

Syntax

scp server enable

undo scp server enable

Default

The SCP server is disabled.

Views

System view

Predefined user roles

network-admin

Examples

Enable the SCP server.

```
<Switch> system-view
[Switch] scp server enable
```

Related commands

display ssh server

9.1.5. sftp server enable

Use **sftp server enable** to enable the SFTP server.

Use **undo sftp server enable** to disable the SFTP server.

Syntax

sftp server enable

undo sftp server enable

Default

The SFTP server is disabled.

Views

System view

Predefined user roles

network-admin

Examples

Enable the SFTP server.

```
<Switch> system-view
[Switch] sftp server enable
```

Related commands

display ssh server

9.1.6. sftp server idle-timeout

Use **sftp server idle-timeout** to set the idle timeout timer for SFTP connections on an SFTP server.

Use **undo sftp server idle-timeout** to restore the default.

Syntax

sftp server idle-timeout *time-out-value*

undo sftp server idle-timeout

Default

The idle timeout timer is 10 minutes for SFTP connections.

Views

System view

Predefined user roles

network-admin

Parameters

time-out-value: Specifies an idle timeout timer in the range of 1 to 35791 minutes.

Usage guidelines

If an SFTP connection is idle when the idle timeout timer expires, the system automatically terminates the connection. To promptly release connection resources, set the idle timeout timer to a small value when many SFTP connections concurrently exist.

Examples

Set the idle timeout timer to 500 minutes for SFTP connections.

```
<Switch> system-view
[Switch] sftp server idle-timeout 500
```

Related commands

display ssh server

9.1.7. ssh server acl

Use **ssh server acl** to specify an ACL to control IPv4 SSH connections to the server.

Use **undo ssh server acl** to restore the default.

Syntax

ssh server acl { *advanced-acl-number* | *basic-acl-number* | **mac** *mac-acl-number* }

undo ssh server acl

Default

No ACLs are specified and all IPv4 SSH clients can initiate SSH connections to the server.

Views

System view

Predefined user roles

network-admin

Parameters

advanced-acl-number: Specifies an IPv4 advanced ACL number in the range of 3000 to 3999.

basic-acl-number: Specifies an IPv4 basic ACL number in the range of 2000 to 2999.

mac *mac-acl-number:* Specifies a Layer 2 ACL by its number in the range of 4000 to 4999.

Usage guidelines

The ACL specified in this command filters IPv4 SSH clients' connection requests. Only the IPv4 SSH clients that the ACL permits can access the device. If the specified ACL does not exist or contains no rules, all IPv4 SSH clients can access the device.

The ACL takes effect only on SSH connections that are initiated after the ACL configuration.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure ACL 2001 and permit only the users at 1.1.1.1 to initiate SSH connections to the server.

```
<Switch> system-view
[Switch] acl basic 2001
[Switch-acl-ipv4-basic-2001] rule permit source 1.1.1.1 0
[Switch-acl-ipv4-basic-2001] quit
[Switch] ssh server acl 2001
```

Related commands

display ssh server

9.1.8. ssh server acl-deny-log enable

Use **ssh server acl-deny-log enable** to enable logging for SSH login attempts that are denied by the SSH login control ACL.

Use **undo ssh server acl-deny-log enable** to disable logging for SSH login attempts that are denied by the SSH login control ACL.

Syntax

ssh server acl-deny-log enable

undo ssh server acl-deny-log enable

Default

Logging is disabled for SSH login attempts that are denied by the SSH login control ACL.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Only SSH clients permitted by the SSH login control ACL can access the SSH server. The logging feature generates log messages for SSH login attempts that are denied by the SSH login control ACL, and sends the messages to the information center.

For information about log message output, see the information center in *Network Management and Monitoring Configuration Guide*. For information about configuring an SSH login control ACL, see the **ssh server acl** or **ssh server ipv6 acl** command.

Examples

Enable logging for SSH login attempts that are denied by the SSH login control ACL.

```
<Switch> system-view
[Switch] ssh server acl-deny-log enable
```

Related commands

ssh server acl

ssh server ipv6 acl

9.1.9. ssh server authentication-retries

Use **ssh server authentication-retries** to set the maximum number of authentication attempts for SSH users.

Use **undo ssh server authentication-retries** to restore the default.

Syntax

ssh server authentication-retries *retries*

undo ssh server authentication-retries

Default

The maximum number of authentication attempts is 3 for SSH users.

Views

System view

Predefined user roles

network-admin

Parameters

retries: Specifies the maximum number of authentication attempts for SSH users, in the range of 1 to 5.

Usage guidelines

Setting the maximum number of authentication attempts prevents malicious hacking of usernames and passwords.

If the total number of authentication attempts exceeds the upper limit specified in this command, further authentication is not allowed.

- For **any** authentication, an authentication attempt is a publickey or password authentication process.
- For **password-publickey** authentication, an authentication attempt contains both a publickey authentication process and a password authentication process. The server first uses publickey authentication, and then uses password authentication to authenticate the SSH user.

This configuration does not affect logged-in users. It affects only users that attempt to log in after the configuration.

Examples

Set the maximum number of authentication attempts to 4 for SSH users.

```
<Switch> system-view
[Switch] ssh server authentication-retries 4
```

Related commands

display ssh server

9.1.10. ssh server authentication-timeout

Use **ssh server authentication-timeout** to set the SSH user authentication timeout timer on the SSH server.

Use **undo ssh server authentication-timeout** to restore the default.

Syntax

ssh server authentication-timeout *time-out-value*

undo ssh server authentication-timeout

Default

The SSH user authentication timeout timer is 60 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

time-out-value: Specifies an authentication timeout timer in the range of 1 to 120 seconds.

Usage guidelines

If a user does not finish the authentication when the timeout timer expires, the connection cannot be established.

To prevent malicious occupation of TCP connections, set the authentication timeout timer to a small value.

Examples

Set the authentication timeout timer to 10 seconds for SSH users.

```
<Switch> system-view
[Switch] ssh server authentication-timeout 10
```

Related commands

display ssh server

9.1.11. ssh server compatible-ssh1x enable

Use **ssh server compatible-ssh1x enable** to enable the SSH server to support SSH1 clients.

Use **undo ssh server compatible-ssh1x** [**enable**] to restore the default.

Syntax

ssh server compatible-ssh1x enable

undo ssh server compatible-ssh1x [**enable**]

Default

The SSH server does not support SSH1 clients.

Views

System view

Predefined user roles

network-admin

network-operator

Usage guidelines

The **undo** form of this command restores the default setting whether you specify the **enable** keyword or not.

This configuration does not affect logged-in users. It affects only users that attempt to log in after the configuration.

Examples

Enable the SSH server to support SSH1 clients.

```
<Switch> system-view
[Switch] ssh server compatible-ssh1x enable
```

Related commands

display ssh server

9.1.12. ssh server dscp

Use **ssh server dscp** to set the DSCP value in the IPv4 SSH packets that the SSH server sends to SSH clients.

Use **undo ssh server dscp** to restore the default.

Syntax

ssh server dscp *dscp-value*

undo ssh server dscp

Default

The DSCP value is 48 in IPv4 SSH packets.

Views

System view

Predefined user roles

network-admin

Parameters

dscp-value: Specifies the DSCP value in the IPv4 SSH packets, in the range of 0 to 63. A bigger DSCP value represents a higher priority.

Usage guidelines

The DSCP value of a packet specifies the priority of the packet and affects the transmission priority of the packet.

Examples

Set the DSCP value to 30 for IPv4 SSH packets.

```
<Switch> system-view
[Switch] ssh server dscp 30
```

9.1.13. ssh server enable

Use **ssh server enable** to enable the Stelnet server.

Use **undo ssh server enable** to disable the Stelnet server.

Syntax

ssh server enable

undo ssh server enable

Default

The Stelnet server is disabled.

Views

System view

Predefined user roles

network-admin

Examples

Enable the Stelnet server.

```
<Switch> system-view
[Switch] ssh server enable
```

Related commands

display ssh server

9.1.14. ssh server ipv6 acl

Use **ssh server ipv6 acl** to specify an ACL to control IPv6 SSH connections to the server.

Use **undo ssh server ipv6 acl** to restore the default.

Syntax

ssh server ipv6 acl { **ipv6** { *advanced-acl-number* | *basic-acl-number* } | **mac** *mac-acl-number* }

undo ssh server ipv6 acl

Default

No ACLs are specified and all IPv6 SSH clients can initiate SSH connections to the server.

Views

System view

Predefined user roles

network-admin

Parameters

ipv6: Specifies the IPv6 ACL type.

advanced-acl-number: Specifies an IPv6 advanced ACL number in the range of 3000 to 3999.

basic-acl-number: Specifies an IPv6 basic ACL number in the range of 2000 to 2999.

mac *mac-acl-number:* Specifies a Layer 2 ACL by its number in the range of 4000 to 4999.

Usage guidelines

The ACL specified in this command filters IPv6 SSH clients' connection requests. Only the IPv6 SSH clients that the ACL permits can access the device. If the specified ACL does not exist or contains no rules, all IPv6 SSH clients can access the device.

The ACL takes effect only on SSH connections that are initiated after the ACL configuration.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure ACL 2001 and permit only the users on the subnet 1::1/64 to initiate SSH connections to the server.

```
<Switch> system-view
[Switch] acl ipv6 basic 2001
[Switch-acl6-ipv6-basic-2001] rule permit source 1::1 64
[Switch-acl6-ipv6-basic-2001] quit
[Switch] ssh server ipv6 acl ipv6 2001
```

Related commands

display ssh server

9.1.15. ssh server ipv6 dscp

Use **ssh server ipv6 dscp** to set the DSCP value in the IPv6 SSH packets that the SSH server sends to SSH clients.

Use **undo ssh server ipv6 dscp** to restore the default.

Syntax

ssh server ipv6 dscp *dscp-value*

undo ssh server ipv6 dscp

Default

The DSCP value is 48 in IPv6 SSH packets.

Views

System view

Predefined user roles

network-admin

Parameters

dscp-value: Specifies the DSCP value in the IPv6 SSH packets, in the range of 0 to 63. A bigger DSCP value represents a higher priority.

Usage guidelines

The DSCP value of an IPv6 packet specifies the priority of the packet and affects the transmission priority of the packet.

Examples

Set the DSCP value to 30 for IPv6 SSH packets.

```
<Switch> system-view
[Switch] ssh server ipv6 dscp 30
```

9.1.16. ssh server rekey-interval

Use **ssh server rekey-interval** to set the minimum interval for updating the RSA server key pair.

Use **undo ssh server rekey-interval** to restore the default.

Syntax

ssh server rekey-interval *interval*

undo ssh server rekey-interval

Default

The minimum interval for updating the RSA server key pair is 0 hours. The system does not update the RSA server key pair.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the minimum interval for updating the RSA server key pair, in the range of 1 to 24 hours.

Usage guidelines

Periodically updating the RSA server key pair prevents malicious hacking to the key pair and enhances security of the SSH connections.

The system starts to count down the configured minimum update interval after the first SSH1 user logs in to the server. If a new SSH1 user logs in to the server after the interval, the system performs the following operations:

1. Updates the RSA server key pair.
2. Uses the updated RSA server key pair for key pair negotiation with the new user.
3. Resets the interval and starts to count down the interval again.

This command takes effect only on SSH1 clients.

Examples

Set the minimum interval to 3 hours for updating the RSA server key pair.

```
<Switch> system-view
[Switch] ssh server rekey-interval 3
```

Related commands

display ssh server

9.1.17. ssh user

Use **ssh user** to create an SSH user and specify the service type and authentication method.

Use **undo ssh user** to delete an SSH user.

Syntax

ssh user *username* **service-type** { **all** | **netconf** | **scp** | **sftp** | **stelnet** } **authentication-type** { **password** | { **any** | **password-publickey** | **publickey** } [**assign publickey** *keyname*&<1-6>] }

undo ssh user *username*

Default

No SSH users exist.

Views

System view

Predefined user roles

network-admin

Parameters

username: Specifies an SSH username, a case-sensitive string of 1 to 80 characters. The username cannot be **a**, **al**, or **all**. In addition, the username cannot include vertical bars (|), colons (:), asterisks (*), question marks (?), or angle brackets (< >). The at sign (@), slash (/), and backslash (\) can only be used to append ISP domain names to usernames in the *pureusername@domain*, *pureusername\domain*, and *pureusername/domain* format. Do not include hyphens (-) in the username of an SCP user. Otherwise, SCP logins using that username will fail.

service-type: Specifies a service type for the SSH user.

- **all**: Specifies service types Stelnet, SFTP, SCP, and NETCONF.
- **scp**: Specifies the service type SCP.
- **sftp**: Specifies the service type SFTP.
- **stelnet**: Specifies the service type Stelnet.
- **netconf**: Specifies the service type NETCONF.

authentication-type: Specifies an authentication method for the SSH user.

- **password**: Specifies password authentication. This authentication method provides easy and fast encryption, but it is vulnerable. It can work with AAA to implement user authentication, authorization, and accounting.
- **any**: Specifies either password authentication or publickey authentication.
- **password-publickey**: Specifies both password authentication and publickey authentication for SSH2 clients. In SSH2, the password-publickey authentication method provides higher security. If the client runs SSH1, this keyword specifies either password authentication or publickey authentication.
- **publickey**: Specifies publickey authentication. This authentication method has complicated and slow encryption, but it provides strong authentication that can defend against brute-force attacks. This authentication method is easy to use. If this method is configured, the authentication process completes automatically without entering any password.

assign: Specifies parameters used for client verification.

- **publickey** *keyname*&<1-6>: Specifies a space-separated list of up to six SSH client public keys. The *keyname* argument represents the SSH client's public key configured on the server. It is a case-sensitive string of 1 to 64 characters. The server uses the client's public key to check the validity of the client. If the public key file of the client is changed, you must update the client's public key on the server promptly. If you specify multiple client public keys, the device verifies the user identity by using the public keys in the order they are specified. The user is valid if the user passes one public key check.

Usage guidelines

Use this command to configure an SSH user depending on the authentication method.

- If the authentication method is **publickey**, you must create an SSH user and a local user on the SSH server. The two users must have the same username, so that the SSH user can be assigned the correct working directory and user role.
- If the authentication method is **password**, you must perform one of the following tasks:
  - For local authentication, configure a local user on the SSH server.
  - For remote authentication, configure an SSH user on a remote authentication server, for example, a RADIUS server.

  You do not need to create an SSH user by using the **ssh user** command. However, if you want to display all SSH users, including the password-only SSH users, for centralized management, you can use this command to create them. If such an SSH user has been created, make sure you have specified the correct service type and authentication method.
- If the authentication method is **password-publickey** or **any**, you must create an SSH user on the SSH server and perform one of the following tasks:
  - For local authentication, configure a local user on the SSH server.
  - For remote authentication, configure an SSH user on a remote authentication server, for example, a RADIUS server.

  In either case, the local user or the SSH user configured on the remote authentication server must have the same username as the SSH user.

For an SFTP or SCP user, the working directory depends on the authentication method.

- If the authentication method is **publickey** or **password-publickey**, the working directory is specified by the **authorization-attribute** command in the associated local user view.
- If the authentication method is **password**, the working directory is authorized by AAA.

For an SSH user, the user role also depends on the authentication method.

- If the authentication method is **publickey** or **password-publickey**, the user role is specified by the **authorization-attribute** command in the associated local user view.
- If the authentication method is **password**, the user role is authorized by AAA.

If you use this command to specify a host public key for a user multiple times, the most recent configuration takes effect. If a host public key is not specified for the user, the user uses certificate authentication for login.

The command configuration does not affect logged-in users. It affects only users that attempt to log in after the configuration.

Examples

Create an SSH user named **user1**. Specify the service type as **sftp** and the authentication method as **password-publickey** for the user. Assign the host public key **key1** to the user.

```
<Switch> system-view
[Switch] ssh user user1 service-type sftp authentication-type password-publickey assign publickey key1
```

Create a local device management user named **user1**. Specify the password as **123456TESTplat&!** in plain text and the service type as **ssh** for the user. Assign the working directory **flash:** and the **network-admin** user role to the user.

```
[Switch] local-user user1 class manage
[Switch-luser-manage-user1] password simple 123456TESTplat&!
[Switch-luser-manage-user1] service-type ssh
[Switch-luser-manage-user1] authorization-attribute work-directory flash: user-role network-admin
```

Related commands

authorization-attribute

display ssh user-information

local-user

9.2. SSH client commands

9.2.1. bye

Use **bye** to terminate the connection with the SFTP server and return to user view.

Syntax

bye

Views

SFTP client view

Predefined user roles

network-admin

network-operator

Usage guidelines

This command has the same function as the **exit** and **quit** commands.

Examples

Terminate the connection with the SFTP server.

```
sftp> bye
<Switch>
```

9.2.2. cd

Use **cd** to change the working directory on the SFTP server.

Syntax

cd [*remote-path*]

Views

SFTP client view

Predefined user roles

network-admin

Parameters

remote-path: Specifies the name of a directory on the server.

Usage guidelines

You can use the **cd ..** command to return to the upper-level directory.

You can use the **cd /** command to return to the root directory of the system.

Examples

Change the working directory to **new1**.

```
sftp> cd new1
Current Directory is:/new1
sftp> pwd
Remote working directory: /new1
sftp>
```

9.2.3. cdup

Use **cdup** to return to the upper-level directory.

Syntax

cdup

Views

SFTP client view

Predefined user roles

network-admin

Example

Return to the upper-level directory from the current working directory **/test1**.

```
sftp> cd test1
Current Directory is:/test1
sftp> pwd
Remote working directory: /test1
sftp> cdup
Current Directory is:/
sftp> pwd
Remote working directory: /
sftp>
```

9.2.4. delete

Use **delete** to delete a file from the SFTP server.

Syntax

delete *remote-file*

Views

SFTP client view

Predefined user roles

network-admin

Parameters

remote-file: Specifies a file by its name.

Usage guidelines

This command has the same function as the **remove** command.

Examples

Delete file **temp.c** from the SFTP server.

```
sftp> delete temp.c
Removing /temp.c
```

9.2.5. delete ssh client server-public-key

Use **delete ssh client server-public-key** to delete server public key information saved in the public key file of the SSH client.

Syntax

delete ssh client server-public-key [**server-ip** *ip-address*]

Views

System view

Predefined user roles

network-admin

Parameters

server-ip *ip-address*: Specifies the IP address of the server whose public key information will be deleted. If you do not specify a server IP address, this command deletes the public keys of all servers from the client's public key file.

Examples

Delete all server public keys saved in the public key file of the SSH client.

```
<Switch> system-view
[Switch] delete ssh client server-public-key
Public keys of all SSH servers will be deleted. Continue? [Y/N]:y
```

Delete the public key of server 2.2.2.1 saved in the public key file of the SSH client.

```
<Switch> system-view
[Switch] delete ssh client server-public-key server-ip 2.2.2.1
```

9.2.6. dir

Use **dir** to display information about the files and subdirectories under a directory.

Syntax

dir [**-a** | **-l**] [*remote-path*]

Views

SFTP client view

Predefined user roles

network-admin

Parameters

-a: Displays detailed information about files and subdirectories under a directory in a list, including the files and subdirectories with names starting with dots (.).

-l: Displays detailed information about the files and subdirectories under a directory in a list, excluding the files and subdirectories with names starting with dots (.).

remote-path: Specifies the name of the directory to be queried. If you do not specify this argument, the command displays information about the files and subdirectories under the current working directory.

Usage guidelines

If you do not specify both of the **-a** and **-l** keywords, this command displays the names of the files and subdirectories under a directory.

This command has the same function as the **ls** command.

Examples

Display detailed information about the files and subdirectories under the current directory, including the files and subdirectories with names starting with dots (.).

```
sftp> dir -a
drwxrwxrwx    2 1        1               512 Dec 18 14:12 .
drwxrwxrwx    2 1        1               512 Dec 18 14:12 ..
-rwxrwxrwx    1 1        1               301 Dec 18 14:11 010.pub
-rwxrwxrwx    1 1        1               301 Dec 18 14:12 011.pub
-rwxrwxrwx    1 1        1               301 Dec 18 14:12 012.pub
```

Display detailed information about the files and subdirectories under the current directory, excluding the files and subdirectories with names starting with dots (.).

```
sftp> dir -l
-rwxrwxrwx    1 1        1               301 Dec 18 14:11 010.pub
-rwxrwxrwx    1 1        1               301 Dec 18 14:12 011.pub
-rwxrwxrwx    1 1        1               301 Dec 18 14:12 012.pub
```

9.2.7. display sftp client source

Use **display sftp client source** to display the source IP address configuration of the SFTP client.

Syntax

display sftp client source

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display the source IP address configuration of the SFTP client.

```
<Switch> display sftp client source
The source IP address of the SFTP client is 192.168.0.1
The source IPv6 address of the SFTP client is 2:2::2:2.
```

Related commands

sftp client ipv6 source

sftp client source

9.2.8. display ssh client source

Use **display ssh client source** to display the source IP address configuration of the Stelnet client.

Syntax

display ssh client source

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display the source IP address configuration of the Stelnet client.

```
<Switch> display ssh client source
The source IP address of the SSH client is 192.168.0.1
The source IPv6 address of the SSH client is 2:2::2:2.
```

Related commands

ssh client ipv6 source

ssh client source

9.2.9. exit

Use **exit** to terminate the SFTP connection and return to user view.

Syntax

exit

Views

SFTP client view

Predefined user roles

network-admin

network-operator

Usage guidelines

This command has the same function as the **bye** and **quit** commands.

Examples

Terminate the SFTP connection.

```
sftp> exit
<Switch>
```

9.2.10. get

Use **get** to download a file from the SFTP server and save it locally.

Syntax

get *remote-file* [*local-file*]

Views

SFTP client view

Predefined user roles

network-admin

Parameters

remote-file: Specifies the name of a file on the SFTP server.

local-file: Specifies the name for the local file. If you do not specify this argument, the file will be saved locally with the same name as the file on the SFTP server.

Examples

Download file **temp1.c** and save it as **temp.c** locally.

```
sftp> get temp1.c temp.c
Fetching /temp1.c to temp.c
/temp.c                                          100% 1424     1.4KB/s   00:00
```

9.2.11. help

Use **help** to display help information on the SFTP client.

Syntax

help

Views

SFTP client view

Predefined user roles

network-admin

network-operator

Usage guidelines

This command has the same function as entering the question mark (?).

Examples

Display help information on the SFTP client.

```
sftp> help
Available commands:
  bye                            Quit sftp
  cd [path]                      Change remote directory to 'path'
  cdup                           Change remote directory to the parent directory
  delete path                    Delete remote file
  dir [-a|-l][path]              Display remote directory listing
       -a                          List all filenames
       -l                          List filename including the specific
                                   information of the file
  exit                           Quit sftp
  get remote-path [local-path] Download file
```

```
help                          Display this help text
ls [-a|-l][path]              Display remote directory
     -a                          List all filenames
     -l                          List filename including the specific
                                 information of the file
mkdir path                    Create remote directory
put local-path [remote-path]  Upload file
pwd                           Display remote working directory
quit                          Quit sftp
rename oldpath newpath        Rename remote file
remove path                   Delete remote file
rmdir path                    Delete remote empty directory
?                             Synonym for help
```

9.2.12. ls

Use **ls** to display information about the files and subdirectories under a directory.

Syntax

ls [**-a** | **-l**] [*remote-path*]

Views

SFTP client view

Predefined user roles

network-admin

Parameters

-a: Displays detailed information about files and subdirectories under a directory in a list, including the files and subdirectories with names starting with dots (.).

-l: Displays detailed information about the files and subdirectories under a directory in a list, excluding the files and subdirectories with names starting with dots (.).

remote-path: Specifies the name of the directory to be queried. If you do not specify this argument, the command displays information about the files and subdirectories under the current working directory.

Usage guidelines

If you do not specify both of the **-a** and **-l** keywords, this command displays the names of the files and subdirectories under a directory.

This command has the same function as the **dir** command.

Examples

Display detailed information about the files and subdirectories under the current directory, including the files and subdirectories with names starting with dots (.).

```
sftp> ls -a
drwxrwxrwx    2 1        1               512 Dec 18 14:12 .
drwxrwxrwx    2 1        1               512 Dec 18 14:12 ..
-rwxrwxrwx    1 1        1               301 Dec 18 14:11 010.pub
-rwxrwxrwx    1 1        1               301 Dec 18 14:12 011.pub
-rwxrwxrwx    1 1        1               301 Dec 18 14:12 012.pub
```

Display detailed information about the files and subdirectories under the current working directory, excluding the files and subdirectories with names starting with dots (.).

```
sftp> ls -l
-rwxrwxrwx    1 1        1               301 Dec 18 14:11 010.pub
-rwxrwxrwx    1 1        1               301 Dec 18 14:12 011.pub
-rwxrwxrwx    1 1        1               301 Dec 18 14:12 012.pub
```

9.2.13. mkdir

Use **mkdir** to create a directory on the SFTP server.

Syntax

mkdir *remote-path*

Views

SFTP client view

Predefined user roles

network-admin

Parameters

remote-path: Specifies the name of a directory.

Examples

Create a directory named **test** on the SFTP server.

```
sftp> mkdir test
```

9.2.14. put

Use **put** to upload a local file to the SFTP server.

Syntax

put *local-file* [*remote-file*]

Views

SFTP client view

Predefined user roles

network-admin

Parameters

local-file: Specifies the name of a local file.

remote-file: Specifies the name of a file on an SFTP server. If you do not specify this argument, the file will be remotely saved with the same name as the local file.

Examples

Upload the local file **startup.bak** to the SFTP server and save it as **startup01.bak**.

```
sftp> put startup.bak startup01.bak
Uploading startup.bak to /startup01.bak
startup01.bak                                 100% 1424     1.4KB/s   00:00
```

9.2.15. pwd

Use **pwd** to display the current working directory of the SFTP server.

Syntax

pwd

Views

SFTP client view

Predefined user roles

network-admin

Examples

Display the current working directory of the SFTP server.

```
sftp> pwd
Remote working directory: /
```

The output shows that the current working directory is the root directory.

9.2.16. quit

Use **quit** to terminate the SFTP connection and return to user view.

Syntax

quit

Views

SFTP client view

Predefined user roles

network-admin

network-operator

Usage guidelines

This command has the same function as the **bye** and **exit** commands.

Examples

Terminate the SFTP connection.

```
sftp> quit
<Switch>
```

9.2.17. remove

Use **remove** to delete a file from the SFTP server.

Syntax

remove *remote-file*

Views

SFTP client view

Predefined user roles

network-admin

Parameters

remote-file: Specifies a file by its name.

Usage guidelines

This command has the same function as the **delete** command.

Examples

Delete file **temp.c** from the SFTP server.

```
sftp> remove temp.c
Removing /temp.c
```

9.2.18. rename

Use **rename** to change the name of a file or directory on the SFTP server.

Syntax

rename *old-name new-name*

Views

SFTP client view

Predefined user roles

network-admin

Parameters

oldname: Specifies the name of an existing file or directory.

newname: Specifies a new name for the existing file or directory.

Examples

Change the name of a file on the SFTP server from **temp1.c** to **temp2.c**.

```
sftp> dir
aa.pub  temp1.c
sftp> rename temp1.c temp2.c
sftp> dir
aa.pub  temp2.c
```

9.2.19. rmdir

Use **rmdir** to delete a directory from the SFTP server.

Syntax

rmdir *remote-path*

Views

SFTP client view

Predefined user roles

network-admin

Parameters

remote-path: Specifies a directory.

Examples

Delete subdirectory **temp1** under the current directory on the SFTP server.

```
sftp> rmdir temp1
```

9.2.20. scp

Use **scp** to establish a connection to an IPv4 SCP server and transfer files with the server.

Syntax

scp *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] { **put** | **get** } *source-file-name* [*destination-file-name*] [**identity-key** { **dsa** | **rsa** } | **prefer-compress zlib** | **prefer-ctos-cipher** { **3des-cbc** | **aes128-cbc** | **des-cbc** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** } | **prefer-stoc-cipher** { **3des-cbc** | **aes128-cbc** | **des-cbc** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] * [**public-key** *keyname* | **source** { **interface** *interface-type interface-number* | **ip** *ip-address* }] *

Views

User view

Predefined user roles

network-admin

Parameters

server: Specifies a server by its IPv4 address or host name, a case-insensitive string of 1 to 253 characters.

port-number: Specifies the port number of the server, in the range of 1 to 65535. The default is 22.

vpn-instance *vpn-instance-name*: Specifies the VPN instance to which the server belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters.

get: Downloads the file.

put: Uploads the file.

source-file-name: Specifies the name of the source file, a case-sensitive string of 1 to 255 characters.

destination-file-name: Specifies the name of the target file, a case-sensitive string of 1 to 255 characters. If you do not specify this argument, the target file uses the same file name as the source file.

identity-key: Specifies a public key algorithm for publickey authentication of the client. If the server uses publickey authentication, you must specify this keyword. The client generates the digital signature or certificate by using the local private key that is associated with the specified algorithm.

- **dsa**: Specifies public key algorithm DSA.
- **rsa**: Specifies public key algorithm RSA.

prefer-compress: Specifies the preferred compression algorithm for data compression between the server and the client.

zlib: Specifies compression algorithm zlib.

prefer-ctos-cipher: Specifies the preferred client-to-server encryption algorithm. Supported algorithms are DES-CBC, 3DES-CBC, and AES128-CBC, in ascending order of security strength and computation time.

- **3des-cbc**: Specifies encryption algorithm 3DES-CBC.
- **aes128-cbc**: Specifies encryption algorithm AES128-CBC.
- **des-cbc**: Specifies encryption algorithm DES-CBC.

prefer-ctos-hmac: Specifies the preferred client-to-server HMAC algorithm. Supported algorithms are MD5, MD5-96, SHA1, and SHA1-96, in ascending order of security strength and computation time.

- **md5**: Specifies HMAC algorithm HMAC-MD5.
- **md5-96**: Specifies HMAC algorithm HMAC-MD5-96.
- **sha1**: Specifies HMAC algorithm HMAC-SHA1.
- **sha1-96**: Specifies HMAC algorithm HMAC-SHA1-96.

prefer-kex: Specifies the preferred key exchange algorithm. Supported algorithms are diffie-hellman-group-exchange-sha1, diffie-hellman-group1-sha1, and diffie-hellman-group14-sha1, in ascending order of security strength and computation time.

- **dh-group-exchange-sha1**: Specifies key exchange algorithm diffie-hellman-group-exchange-sha1.
- **dh-group1-sha1**: Specifies key exchange algorithm diffie-hellman-group1-sha1.
- **dh-group14-sha1**: Specifies key exchange algorithm diffie-hellman-group14-sha1.

prefer-stoc-cipher: Specifies the preferred server-to-client encryption algorithm. Supported algorithms are the same as the client-to-server encryption algorithms (see the **prefer-ctos-cipher** keyword).

prefer-stoc-hmac: Specifies the preferred server-to-client HMAC algorithm. Supported algorithms are the same as the client-to-server HMAC algorithms (see the **prefer-ctos-hmac** keyword).

public-key *keyname*: Specifies the server's host public key that the client uses to authenticate the server. The *keyname* argument is a case-insensitive string of 1 to 64 characters.

source: Specifies a source IPv4 address or source interface for SCP packets. By default, the device uses the primary IPv4 address of the output interface in the routing entry as the source address of SCP packets. As a best practice to ensure successful SCP connections, specify a loopback interface as the source interface or specify that interface's IPv4 address as the source IPv4 address.

- **interface** *interface-type interface-number*: Specifies a source interface by its type and number. The IPv4 address of this interface is the source IPv4 address of the SCP packets.
- **ip** *ip-address*: Specifies a source IPv4 address.

Usage guidelines

If you do not specify a username and password in the command, you must provide the username and password in an interactive way.

If the SCP server uses publickey authentication, the password specified by this command is ignored.

Examples

Connect the SCP client to SCP server **200.1.1.1**. Specify the public key of the server as **svkey**, and download file **abc.txt** from the server. The SCP client uses publickey authentication. Use the following algorithms:

- Preferred key exchange algorithm: **dh-group14-sha1**.
- Preferred server-to-client encryption algorithm: **aes128-cbc**.
- Preferred client-to-server HMAC algorithm: **sha1**.
- Preferred server-to-client HMAC algorithm: **sha1-96**.
- Preferred compression algorithm: **zlib**.

```
<Switch> scp 200.1.1.1 get abc.txt prefer-kex dh-group14-sha1 prefer-stoc-cipher
aes128-cbc prefer-ctos-hmac sha1 prefer-stoc-hmac sha1-96 prefer-compress zlib public-key
svkey
Username:
```

9.2.21. scp ipv6

Use **scp ipv6** to establish a connection to an IPv6 SCP server and transfer files with the server.

Syntax

scp ipv6 *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**-i** *interface-type interface-number*] { **put** | **get** } *source-file-name* [*destination-file-name*] [**identity-key** { **dsa** | **rsa** } | **prefer-compress zlib** | **prefer-ctos-cipher** { **3des-cbc** | **aes128-cbc** | **des-cbc** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** } | **prefer-stoc-cipher** { **3des-cbc** | **aes128-cbc** | **des-cbc** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] * [**public-key** *keyname* | **source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }] *

Views

User view

Predefined user roles

network-admin

Parameters

server: Specifies a server by its IPv6 address or host name, a case-insensitive string of 1 to 253 characters.

port-number: Specifies the port number of the server, in the range of 1 to 65535. The default is 22.

vpn-instance *vpn-instance-name*: Specifies the VPN instance to which the server belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters.

-i *interface-type interface-number:* Specifies an output interface by its type and number for SCP packets. This option is used only when the server uses a link-local address to provide the SCP service for the client. The specified output interface on the SCP client must have a link-local address.

get: Downloads the file.

put: Uploads the file.

source-file-name: Specifies the name of the source file, a case-sensitive string of 1 to 255 characters.

destination-file-name: Specifies the name of the target file, a case-sensitive string of 1 to 255 characters. If you do not specify this argument, the target file uses the same file name as the source file.

identity-key: Specifies a public key algorithm for publickey authentication of the client. If the server uses publickey authentication, you must specify this keyword. The client generates the digital signature or certificate by using the local private key that is associated with the specified algorithm.

- **dsa**: Specifies public key algorithm DSA.
- **rsa**: Specifies public key algorithm RSA.

prefer-compress: Specifies the preferred compression algorithm for data compression between the server and the client.

zlib: Specifies compression algorithm zlib.

prefer-ctos-cipher: Specifies the preferred client-to-server encryption algorithm. Supported algorithms are DES-CBC, 3DES-CBC, and AES128-CBC, in ascending order of security strength and computation time.

- **3des-cbc**: Specifies encryption algorithm 3DES-CBC.
- **aes128-cbc**: Specifies encryption algorithm AES128-CBC.
- **des-cbc**: Specifies encryption algorithm DES-CBC.

prefer-ctos-hmac: Specifies the preferred client-to-server HMAC algorithm. Supported algorithms are MD5, MD5-96, SHA1, and SHA1-96, in ascending order of security strength and computation time.

- **md5**: Specifies HMAC algorithm HMAC-MD5.
- **md5-96**: Specifies HMAC algorithm HMAC-MD5-96.
- **sha1**: Specifies HMAC algorithm HMAC-SHA1.
- **sha1-96**: Specifies HMAC algorithm HMAC-SHA1-96.

prefer-kex: Specifies the preferred key exchange algorithm. Supported algorithms are diffie-hellman-group-exchange-sha1, diffie-hellman-group1-sha1, and diffie-hellman-group14-sha1, in ascending order of security strength and computation time.

- **dh-group-exchange-sha1**: Specifies key exchange algorithm diffie-hellman-group-exchange-sha1.
- **dh-group1-sha1**: Specifies key exchange algorithm diffie-hellman-group1-sha1.
- **dh-group14-sha1**: Specifies key exchange algorithm diffie-hellman-group14-sha1.

prefer-stoc-cipher: Specifies the preferred server-to-client encryption algorithm. Supported algorithms are the same as the client-to-server encryption algorithms (see the **prefer-ctos-cipher** keyword).

prefer-stoc-hmac: Specifies the preferred server-to-client HMAC algorithm. Supported algorithms are the same as the client-to-server HMAC algorithms (see the **prefer-ctos-hmac** keyword).

public-key *keyname*: Specifies the server's host public key that the client uses to authenticate the server. The *keyname* argument is a case-insensitive string of 1 to 64 characters.

source: Specifies a source IPv6 address or source interface for IPv6 SCP packets. By default, the device automatically selects a source address for IPv6 SCP packets in compliance with RFC 3484. As a best practice to ensure successful SCP connections, specify a loopback interface as the source interface or specify that interface's IPv6 address as the source IPv6 address.

- **interface** *interface-type interface-number*: Specifies a source interface by its type and number. The IPv6 address of this interface is the source IPv6 address of the IPv6 SCP packets.
- **ipv6** *ipv6-address*: Specifies a source IPv6 address.

Usage guidelines

If you do not specify a username and password in the command, you must provide the username and password in an interactive way.

If the SCP server uses publickey authentication, the password specified by this command is ignored.

Examples

Connect an SCP client to SCP server **2000::1**. Specify the public key of the server as **svkey**, and download file **abc.txt** from the server. The SCP client uses publickey authentication. Use the following algorithms:

- Preferred key exchange algorithm: **dh-group14-sha1**.
- Preferred server-to-client encryption algorithm: **aes128-cbc**.
- Preferred client-to-server HMAC algorithm: **sha1**.
- Preferred server-to-client HMAC algorithm: **sha1-96**.
- Preferred compression algorithm: **zlib**.

```
<Switch> scp ipv6 2000::1 get abc.txt prefer-kex dh-group14-sha1 prefer-stoc-cipher
aes128-cbc prefer-ctos-hmac sha1 prefer-stoc-hmac sha1-96 prefer-compress zlib public-key
svkey
Username:
```

9.2.22. sftp

Use **sftp** to establish a connection to an IPv4 SFTP server and enter SFTP client view.

Syntax

sftp *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**identity-key** { **dsa** | **rsa** } | **prefer-compress zlib** | **prefer-ctos-cipher** { **3des-cbc** | **aes128-cbc** | **des-cbc** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** } | **prefer-stoc-cipher** { **3des-cbc** | **aes128-cbc** | **des-cbc** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] * [**dscp** *dscp-value* | { **public-key** *keyname* } | **source** { **interface** *interface-type interface-number* | **ip** *ip-address* }] *

Views

User view

Predefined user roles

network-admin

Parameters

server: Specifies a server by its IPv4 address or host name, a case-insensitive string of 1 to 253 characters.

port-number: Specifies the port number of the server, in the range of 1 to 65535. The default is 22.

vpn-instance *vpn-instance-name*: Specifies the VPN instance to which the server belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters.

identity-key: Specifies a public key algorithm for publickey authentication of the client. If the server uses publickey authentication, you must specify this keyword. The client generates the digital signature or certificate by using the local private key that is associated with the specified algorithm.

- **dsa**: Specifies public key algorithm DSA.
- **rsa**: Specifies public key algorithm RSA.

prefer-compress: Specifies the preferred compression algorithm for data compression between the server and the client.

zlib: Specifies compression algorithm zlib.

prefer-ctos-cipher: Specifies the preferred client-to-server encryption algorithm. Supported algorithms are DES-CBC, 3DES-CBC, and AES128-CBC, in ascending order of security strength and computation time.

- **3des-cbc**: Specifies encryption algorithm 3DES-CBC.
- **aes128-cbc**: Specifies encryption algorithm AES128-CBC.
- **des-cbc**: Specifies encryption algorithm DES-CBC.

prefer-ctos-hmac: Specifies the preferred client-to-server HMAC algorithm. Supported algorithms are MD5, MD5-96, SHA1, and SHA1-96, in ascending order of security strength and computation time.

- **md5**: Specifies HMAC algorithm HMAC-MD5.
- **md5-96**: Specifies HMAC algorithm HMAC-MD5-96.
- **sha1**: Specifies HMAC algorithm HMAC-SHA1.
- **sha1-96**: Specifies HMAC algorithm HMAC-SHA1-96.

prefer-kex: Specifies the preferred key exchange algorithm. Supported algorithms are diffie-hellman-group-exchange-sha1, diffie-hellman-group1-sha1, and diffie-hellman-group14-sha1, in ascending order of security strength and computation time.

- **dh-group-exchange-sha1**: Specifies key exchange algorithm diffie-hellman-group-exchange-sha1.
- **dh-group1-sha1**: Specifies key exchange algorithm diffie-hellman-group1-sha1.
- **dh-group14-sha1**: Specifies key exchange algorithm diffie-hellman-group14-sha1.

prefer-stoc-cipher: Specifies the preferred server-to-client encryption algorithm. Supported algorithms are the same as the client-to-server encryption algorithms (see the **prefer-ctos-cipher** keyword).

prefer-stoc-hmac: Specifies the preferred server-to-client HMAC algorithm. Supported algorithms are the same as the client-to-server HMAC algorithms (see the **prefer-ctos-hmac** keyword).

dscp *dscp-value*: Specifies the DSCP value in the IPv4 SFTP packets. The value range for the *dscp-value* argument is 0 to 63, and the default value is 48. The DSCP value determines the transmission priority of the packet.

public-key *keyname*: Specifies the server's host public key that the client uses to authenticate the server. The *keyname* argument is a case-insensitive string of 1 to 64 characters.

source: Specifies a source IPv4 address or source interface for the SFTP packets. By default, the device uses the primary IPv4 address of the output interface in the routing entry as the source address of SFTP packets. As a best practice to ensure successful SFTP connections, specify a loopback interface as the source interface or specify that interface's IPv4 address as the source IPv4 address.

- **interface** *interface-type interface-number*: Specifies a source interface by its type and number. The primary IPv4 address of this interface is the source IPv4 address of the SFTP packets.
- **ip** *ip-address*: Specifies a source IPv4 address.

Examples

Connect an SFTP client to SFTP server **10.1.1.2** and specify the public key of the server as **svkey**. The SFTP client uses publickey authentication. Use the following algorithms:

- Preferred key exchange algorithm: **dh-group14-sha1**.
- Preferred server-to-client encryption algorithm: **aes128-cbc**.
- Preferred client-to-server HMAC algorithm: **sha1**.
- Preferred server-to-client HMAC algorithm: **sha1-96**.
- Preferred compression algorithm: **zlib**.

```
<Switch> sftp 10.1.1.2 prefer-kex dh-group14-sha1 prefer-stoc-cipher aes128-cbc
prefer-ctos-hmac sha1 prefer-stoc-hmac sha1-96 prefer-compress zlib public-key svkey
```

9.2.23. sftp client ipv6 source

Use **sftp client ipv6 source** to configure the source IPv6 address for SFTP packets that are sent by the SFTP client.

Use **undo sftp client ipv6 source** to restore the default.

Syntax

sftp client ipv6 source { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }

undo sftp client ipv6 source

Default

The source IPv6 address for outgoing SFTP packets is not configured. The SFTP client automatically selects an IPv6 address for outgoing SFTP packets in compliance with RFC 3484.

Views

System view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies a source interface by its type and number. The SFTP client selects the interface's address that most specifically matches the destination address of outgoing SFTP packets as the source address of the SFTP packets.

ipv6 *ipv6-address*: Specifies a source IPv6 address.

Usage guidelines

This command takes effect on all IPv6 SFTP connections. The source IPv6 address specified in the **sftp ipv6** command takes effect only on the current IPv6 SFTP connection. If you specify the source IPv6 address both in this command and the **sftp ipv6** command, the source IPv6 address specified in the **sftp ipv6** command takes effect.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify **2:2::2:2** as the source IPv6 address for SFTP packets.

```
<Switch> system-view
[Switch] sftp client ipv6 source ipv6 2:2::2:2
```

Related commands

display sftp client source

9.2.24. sftp client source

Use **sftp client source** to configure the source IPv4 address for SFTP packets that are sent by the SFTP client.

Use **undo sftp client source** to restore the default.

Syntax

sftp client source { **interface** *interface-type interface-number* | **ip** *ip-address* }

undo sftp client source

Default

The source IPv4 address for outgoing SFTP packets is not configured. The SFTP client uses the primary IPv4 address of the output interface in the matching routing entry as the source IPv4 address of outgoing SFTP packets.

Views

System view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies a source interface by its type and number. The SFTP client uses the primary IPv4 address of the interface as the source address of outgoing SFTP packets.

ip *ip-address*: Specifies a source IPv4 address.

Usage guidelines

This command takes effect on all SFTP connections. The source IPv4 address specified in the **sftp** command takes effect only on the current SFTP connection. If you specify the source IPv4 address both in this command and the **sftp** command, the source IPv4 address specified in the **sftp** command takes effect.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify **192.168.0.1** as the source IPv4 address for SFTP packets.

```
<Switch> system-view
[Switch] sftp client source ip 192.168.0.1
```

Related commands

display sftp client source

9.2.25. sftp ipv6

Use **sftp ipv6** to connect an SFTP client to an IPv6 SFTP server and enter SFTP client view.

Syntax

sftp ipv6 *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**-i** *interface-type interface-number*] [**identity-key** { **dsa** | **rsa** } | **prefer-compress zlib** | **prefer-ctos-cipher** { **3des-cbc** | **aes128-cbc** | **des-cbc** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** } | **prefer-stoc-cipher** { **3des-cbc** | **aes128-cbc** | **des-cbc** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] * [**dscp** *dscp-value* | **public-key** *keyname* | **source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }] *

Views

User view

Predefined user roles

network-admin

Parameters

server: Specifies a server by its IPv6 address or host name, a case-insensitive string of 1 to 253 characters.

port-number: Specifies the port number of the server, in the range of 1 to 65535. The default is 22.

vpn-instance *vpn-instance-name*: Specifies the VPN instance to which the server belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters.

-i *interface-type interface-number:* Specifies an output interface by its type and number for IPv6 SFTP packets. This option is used only when the server uses a link-local address to provide the SFTP service for the client. The specified output interface on the SFTP client must have a link-local address.

identity-key: Specifies a public key algorithm for publickey authentication of the client. If the server uses publickey authentication, you must specify this keyword. The client generates the digital signature or certificate by using the local private key that is associated with the specified algorithm.

- **dsa**: Specifies public key algorithm DSA.
- **rsa**: Specifies public key algorithm RSA.

prefer-compress: Specifies the preferred compression algorithm for data compression between the server and the client.

zlib: Specifies compression algorithm zlib.

prefer-ctos-cipher: Specifies the preferred client-to-server encryption algorithm. Supported algorithms are DES-CBC, 3DES-CBC, and AES128-CBC, in ascending order of security strength and computation time.

- **3des-cbc**: Specifies encryption algorithm 3DES-CBC.
- **aes128-cbc**: Specifies encryption algorithm AES128-CBC.
- **des-cbc**: Specifies encryption algorithm DES-CBC.

prefer-ctos-hmac: Specifies the preferred client-to-server HMAC algorithm. Supported algorithms are MD5, MD5-96, SHA1, and SHA1-96, in ascending order of security strength and computation time.

- **md5**: Specifies HMAC algorithm HMAC-MD5.
- **md5-96**: Specifies HMAC algorithm HMAC-MD5-96.
- **sha1**: Specifies HMAC algorithm HMAC-SHA1.

- **sha1-96**: Specifies HMAC algorithm HMAC-SHA1-96.

prefer-kex: Specifies the preferred key exchange algorithm. Supported algorithms are diffie-hellman-group-exchange-sha1, diffie-hellman-group1-sha1, and diffie-hellman-group14-sha1, in ascending order of security strength and computation time.

- **dh-group-exchange-sha1**: Specifies key exchange algorithm diffie-hellman-group-exchange-sha1.
- **dh-group1-sha1**: Specifies key exchange algorithm diffie-hellman-group1-sha1.
- **dh-group14-sha1**: Specifies key exchange algorithm diffie-hellman-group14-sha1.

prefer-stoc-cipher: Specifies the preferred server-to-client encryption algorithm. Supported algorithms are the same as the client-to-server encryption algorithms (see the **prefer-ctos-cipher** keyword).

prefer-stoc-hmac: Specifies the preferred server-to-client HMAC algorithm. Supported algorithms are the same as the client-to-server HMAC algorithms (see the **prefer-ctos-hmac** keyword).

dscp *dscp-value*: Specifies the DSCP value in the IPv6 SFTP packets. The value range for the *dscp-value* argument is 0 to 63, and the default value is 48. The DSCP value determines the transmission priority of the packet.

public-key *keyname*: Specifies the host public key of the server that the client uses to authenticate the server. The *keyname* argument is a case-insensitive string of 1 to 64 characters.

source: Specifies a source IPv6 address or source interface for IPv6 SFTP packets. By default, the device automatically selects a source address for IPv6 SFTP packets in compliance with RFC 3484. As a best practice to ensure successful SFTP connections, specify a loopback interface as the source interface or specify that interface's IPv6 address as the source IPv6 address.

- **interface** *interface-type interface-number*: Specifies a source interface by its type and number. The IPv6 address of this interface is the source IPv6 address of the IPv6 SFTP packets.
- **ipv6** *ipv6-address*: Specifies a source IPv6 address.

Examples

Connect an SFTP client to SFTP server **2000::1** and specify the public key of the server as **svkey**. The SFTP client uses publickey authentication. Use the following algorithms:

- Preferred key exchange algorithm: **dh-group14-sha1**.
- Preferred server-to-client encryption algorithm: **aes128-cbc**.
- Preferred client-to-server HMAC algorithm: **sha1**.
- Preferred server-to-client HMAC algorithm: **sha1-96**.
- Preferred compression algorithm: **zlib**.

```
<Switch> sftp ipv6 2000::1 prefer-kex dh-group14-sha1 prefer-stoc-cipher aes128-cbc
prefer-ctos-hmac sha1 prefer-stoc-hmac sha1-96 prefer-compress zlib public-key svkey
Username:
```

9.2.26. ssh client ipv6 source

Use **ssh client ipv6 source** to configure the source IPv6 address for SSH packets that are sent by the Stelnet client.

Use **undo ssh client ipv6 source** to restore the default.

Syntax

ssh client ipv6 source { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }

undo ssh client ipv6 source

Default

The source IPv6 address for outgoing SSH packets is not configured. The Stelnet client automatically selects an IPv6 address for outgoing SSH packets in compliance with RFC 3484.

Views

System view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies a source interface by its type and number. The Stelnet client selects the interface's address that most specifically matches the destination address of outgoing SSH packets as the source address of the SSH packets.

ipv6 *ipv6-address*: Specifies a source IPv6 address.

Usage guidelines

This command takes effect on all IPv6 Stelnet connections. The source IPv6 address specified in the **ssh2 ipv6** command takes effect only on the current IPv6 Stelnet connection. If you specify the source IPv6 address both in this command and the **ssh2 ipv6** command, the source IPv6 address specified in the **ssh2 ipv6** command takes effect.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify **2:2::2:2** as the source IPv6 address for SSH packets that are sent by the Stelnet client.

```
<Switch> system-view
[Switch] ssh client ipv6 source ipv6 2:2::2:2
```

Related commands

display ssh client source

9.2.27. ssh client source

Use **ssh client source** to configure the source IPv4 address for SSH packets that are sent by the Stelnet client.

Use **undo ssh client source** to restore the default.

Syntax

ssh client source { **interface** *interface-type interface-number* | **ip** *ip-address* }

undo ssh client source

Default

The source IPv4 address for outgoing SSH packets is not configured. The Stelnet client uses the primary IPv4 address of the output interface in the matching routing entry as the source address of outgoing SSH packets.

Views

System view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies a source interface by its type and number. The Stelnet client uses the primary IPv4 address of the interface as the source address of outgoing SSH packets.

ip *ip-address*: Specifies a source IPv4 address.

Usage guidelines

This command takes effect on all Stelnet connections. The source IPv4 address specified in the **ssh2** command takes effect only on the current Stelnet connection. If you specify the source IPv4 address both in this command and the **ssh2** command, the source IPv4 address specified in the **ssh2** command takes effect.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify **192.168.0.1** as the source IPv4 address for SSH packets.

```
<Switch> system-view
[Switch] ssh client source ip 192.168.0.1
```

Related commands

display ssh client source

9.2.28. ssh2

Use **ssh2** to establish a connection to an IPv4 Stelnet server.

Syntax

ssh2 *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**identity-key** { **dsa** | **rsa** } | **prefer-compress zlib** | **prefer-ctos-cipher** { **3des-cbc** | **aes128-cbc** | **des-cbc** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** } | **prefer-stoc-cipher** { **3des-cbc** | **aes128-cbc** | **des-cbc** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] * [**dscp** *dscp-value* | **escape** *character* | **public-key** *keyname* | **source** { **interface** *interface-type interface-number* | **ip** *ip-address* }] *

Views

User view

Predefined user roles

network-admin

Parameters

server: Specifies a server by its IPv4 address or host name, a case-insensitive string of 1 to 253 characters.

port-number: Specifies the port number of the server, in the range 1 to 65535. The default is 22.

vpn-instance *vpn-instance-name*: Specifies the VPN instance to which the server belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters.

identity-key: Specifies a public key algorithm for publickey authentication of the client. If the server uses publickey authentication, you must specify this keyword. The client generates the digital signature or certificate by using the local private key that is associated with the specified algorithm.

- **dsa**: Specifies public key algorithm DSA.
- **rsa**: Specifies public key algorithm RSA.

prefer-compress: Specifies the preferred compression algorithm for data compression between the server and the client.

zlib: Specifies compression algorithm zlib.

prefer-ctos-cipher: Specifies the preferred client-to-server encryption algorithm. Supported algorithms are DES-CBC, 3DES-CBC, and AES128-CBC, in ascending order of security strength and computation time.

- **3des-cbc**: Specifies encryption algorithm 3DES-CBC.
- **aes128-cbc**: Specifies encryption algorithm AES128-CBC.
- **des-cbc**: Specifies encryption algorithm DES-CBC.

prefer-ctos-hmac: Specifies the preferred client-to-server HMAC algorithm. Supported algorithms are MD5, MD5-96, SHA1, and SHA1-96, in ascending order of security strength and computation time.

- **md5**: Specifies HMAC algorithm HMAC-MD5.
- **md5-96**: Specifies HMAC algorithm HMAC-MD5-96.
- **sha1**: Specifies HMAC algorithm HMAC-SHA1.
- **sha1-96**: Specifies HMAC algorithm HMAC-SHA1-96.

prefer-kex: Specifies the preferred key exchange algorithm. Supported algorithms are diffie-hellman-group-exchange-sha1, diffie-hellman-group1-sha1, and diffie-hellman-group14-sha1, in ascending order of security strength and computation time.

- **dh-group-exchange-sha1**: Specifies key exchange algorithm diffie-hellman-group-exchange-sha1.
- **dh-group1-sha1**: Specifies key exchange algorithm diffie-hellman-group1-sha1.
- **dh-group14-sha1**: Specifies key exchange algorithm diffie-hellman-group14-sha1.

prefer-stoc-cipher: Specifies the preferred server-to-client encryption algorithm. Supported algorithms are the same as the client-to-server encryption algorithms (see the **prefer-ctos-cipher** keyword).

prefer-stoc-hmac: Specifies the preferred server-to-client HMAC algorithm. Supported algorithms are the same as the client-to-server HMAC algorithms (see the **prefer-ctos-hmac** keyword).

dscp *dscp-value*: Specifies the DSCP value in the IPv4 SSH packets. The value range for the *dscp-value* argument is 0 to 63, and the default value is 48. The DSCP value determines the transmission priority of the packet.

escape *character*: Specifies a case-sensitive escape character. By default, the escape character is a tilde (~).

public-key *keyname*: Specifies the host public key of the server that the client uses to authenticate the server. The *keyname* argument is a case-insensitive string of 1 to 64 characters.

source: Specifies a source IPv4 address or source interface for SSH packets. By default, the device uses the primary IPv4 address of the output interface in the routing entry as the source address of SSH packets. As a best practice to ensure successful Stelnet connections, specify a loopback interface as the source interface or specify that interface's IPv4 address as the source IPv4 address.

- **interface** *interface-type interface-number*: Specifies a source interface by its type and number. The primary IPv4 address of this interface is the source IPv4 address of the SSH packets.
- **ip** *ip-address*: Specifies a source IPv4 address.

Usage guidelines

The combination of an escape character and a dot (.) works as an escape sequence. This escape sequence is typically used to quickly terminate an SSH connection when the server reboots or malfunctions.

For the escape sequence to take effect, you must enter it at the very beginning of a line. If you have entered other characters or performed operations in a line, enter the escape sequence in the next line.

As a best practice, use the default escape character (~). Do not use any character in SSH usernames as the escape character.

Examples

Establish a connection to Stelnet server **3.3.3.3** and specify the public key of the server as **svkey**. The Stelnet client uses publickey authentication. Specify the dollar sign ($) as the escape character. Use the following algorithms:

- Preferred key exchange algorithm: **dh-group14-sha1**.
- Preferred server-to-client encryption algorithm: **aes128-cbc**.
- Preferred client-to-server HMAC algorithm: **sha1**.
- Preferred server-to-client HMAC algorithm: **sha1-96**.
- Preferred compression algorithm: **zlib**.

```
<Switch> ssh2 3.3.3.3 prefer-kex dh-group14-sha1 prefer-stoc-cipher aes128-cbc
prefer-ctos-hmac sha1 prefer-stoc-hmac sha1-96 prefer-compress zlib public-key svkey
escape $
```

9.2.29. ssh2 ipv6

Use **ssh2 ipv6** to establish a connection to an IPv6 Stelnet server.

Syntax

ssh2 ipv6 *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**-i** *interface-type interface-number*] [**identity-key** { **dsa** | **rsa** } | **prefer-compress zlib** | **prefer-ctos-cipher** { **3des-cbc** | **aes128-cbc** | **des-cbc** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** } | **prefer-stoc-cipher** { **3des-cbc** | **aes128-cbc** | **des-cbc** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] * [**dscp** *dscp-value* | **escape** *character* | **public-key** *keyname* | **source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }] *

Views

User view

Predefined user roles

network-admin

Parameters

server: Specifies a server by its IPv6 address or host name, a case-insensitive string of 1 to 253 characters.

port-number: Specifies the port number of the server, in the range 1 to 65535. The default is 22.

vpn-instance *vpn-instance-name:* Specifies the VPN instance to which the server belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters.

-i *interface-type interface-number:* Specifies an output interface by its type and number for IPv6 SSH packets. This option is used only when the server uses a link-local address to provide the Stelnet service for the client. The specified output interface on the Stelnet client must have a link-local address.

identity-key: Specifies a public key algorithm for publickey authentication of the client. If the server uses publickey authentication, you must specify this keyword. The client generates the digital signature or certificate by using the local private key that is associated with the specified algorithm.

- **dsa**: Specifies public key algorithm DSA.
- **rsa**: Specifies public key algorithm RSA.

prefer-compress: Specifies the preferred compression algorithm for data compression between the server and the client. By default, compression is not supported.

zlib: Specifies compression algorithm zlib.

prefer-ctos-cipher: Specifies the preferred client-to-server encryption algorithm. Supported algorithms are DES-CBC, 3DES-CBC, and AES128-CBC, in ascending order of security strength and computation time.

- **3des-cbc**: Specifies encryption algorithm 3DES-CBC.
- **aes128-cbc**: Specifies encryption algorithm AES128-CBC.
- **des-cbc**: Specifies encryption algorithm DES-CBC.

prefer-ctos-hmac: Specifies the preferred client-to-server HMAC algorithm. Supported algorithms are MD5, MD5-96, SHA1, and SHA1-96, in ascending order of security strength and computation time.

- **md5**: Specifies HMAC algorithm HMAC-MD5.
- **md5-96**: Specifies HMAC algorithm HMAC-MD5-96.
- **sha1**: Specifies HMAC algorithm HMAC-SHA1.
- **sha1-96**: Specifies HMAC algorithm HMAC-SHA1-96.

prefer-kex: Specifies the preferred key exchange algorithm. Supported algorithms are diffie-hellman-group-exchange-sha1, diffie-hellman-group1-sha1, and diffie-hellman-group14-sha1, in ascending order of security strength and computation time.

- **dh-group-exchange-sha1**: Specifies key exchange algorithm diffie-hellman-group-exchange-sha1.
- **dh-group1-sha1**: Specifies key exchange algorithm diffie-hellman-group1-sha1.
- **dh-group14-sha1**: Specifies key exchange algorithm diffie-hellman-group14-sha1.

prefer-stoc-cipher: Specifies the preferred server-to-client encryption algorithm. Supported algorithms are the same as the client-to-server encryption algorithms (see the **prefer-ctos-cipher** keyword).

prefer-stoc-hmac: Specifies the preferred server-to-client HMAC algorithm. Supported algorithms are the same as the client-to-server HMAC algorithms (see the **prefer-ctos-hmac** keyword).

dscp *dscp-value*: Specifies the DSCP value in the IPv6 SSH packets. The value range for the *dscp-value* argument is 0 to 63, and the default value is 48. The DSCP value determines the transmission priority of the packet.

escape *character*: Specifies a case-sensitive escape character. By default, the escape character is a tilde (~).

public-key *keyname*: Specifies the server by its host public key that the client uses to authenticate the server. The *keyname* argument is a case-insensitive string of 1 to 64 characters.

source: Specifies a source IPv6 address or source interface for IPv6 SSH packets. By default, the device automatically selects a source address for IPv6 SSH packets in compliance with RFC 3484. As a best practice to ensure successful Stelnet connections, specify a loopback interface as the source interface or specify that interface's IPv6 address as the source IPv6 address.

- **interface** *interface-type interface-number*: Specifies a source interface by its type and number. The IPv6 address of this interface is the source IPv6 address of the IPv6 SSH packets.
- **ipv6** *ipv6-address*: Specifies a source IPv6 address.

Usage guidelines

The combination of an escape character and a dot (.) works as an escape sequence. This escape sequence is typically used to quickly terminate an SSH connection when the server reboots or malfunctions.

For the escape sequence to take effect, you must enter it at the very beginning of a line. If you have entered other characters or performed operations in a line, enter the escape sequence in the next line.

As a best practice, use the default escape character (~). Do not use any characters in SSH usernames as the escape character.

Examples

Establish a connection to Stelnet server **2000::1** and specify the public key of the server as **svkey**. The SSH client uses publickey authentication. Specify the dollar sign ($) as the escape character. Use the following algorithms:

- Preferred key exchange algorithm: **dh-group14-sha1**.
- Preferred server-to-client encryption algorithm: **aes128-cbc**.
- Preferred client-to-server HMAC algorithm: **sha1**.
- Preferred server-to-client HMAC algorithm: **sha1-96**.
- Preferred compression algorithm: **zlib**.

```
<Switch> ssh2 ipv6 2000::1 prefer-kex dh-group14-sha1 prefer-stoc-cipher aes128-cbc
prefer-ctos-hmac sha1 prefer-stoc-hmac sha1-96 prefer-compress zlib public-key svkey
escape $
```

9.3. SSH2 commands

9.3.1. display ssh2 algorithm

> 🕮 **MEMO :**
>
> **display ssh 2 algorithm** command is supported from later software, including Version 7.2.17.

Use **display ssh2 algorithm** to display algorithms used by SSH2 in the algorithm negotiation stage.

Syntax

display ssh2 algorithm

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display algorithms used by SSH2 in the algorithm negotiation stage.

```
<Switch> display ssh2 algorithm
 Key exchange algorithms: ecdh-sha2-nistp256 ecdh-sha2-nistp384 dh-group-exchange-sha1
dh-group14-sha1 dh-group1-sha1
 Public key algorithms: x509v3-ecdsa-sha2-nistp256 x509v3-ecdsa-sha2-nistp384
ecdsa-sha2-nistp256 ecdsa-sha2-nistp384 rsa dsa
 Encryption algorithms: aes128-ctr aes192-ctr aes256-ctr aes128-gcm aes256-gcm aes128-cbc
3des-cbc aes256-cbc des-cbc
 MAC algorithms: sha2-256 sha2-512 sha1 md5 sha1-96 md5-96
```

Table 9-4 Command output

Field	Description
Key exchange algorithms	Key exchange algorithms in descending order of priority for algorithm negotiation.
Public key algorithms	Public key algorithms in descending order of priority for algorithm negotiation.
Encryption algorithms	Encryption algorithms in descending order of priority for algorithm negotiation.
MAC algorithms	HMAC algorithms in descending order of priority for algorithm negotiation.

Related commands

ssh2 algorithm cipher

ssh2 algorithm key-exchange

ssh2 algorithm mac

ssh2 algorithm public-key

9.3.2. ssh2 algorithm cipher

> 🕮 **MEMO :**
>
> **ssh2 algorithm cipher** command is supported from later software, including Version 7.2.17.

Use **ssh2 algorithm cipher** to specify encryption algorithms for SSH2.

Use **undo ssh2 algorithm cipher** to restore the default.

Syntax

ssh2 algorithm cipher { **3des-cbc** | **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** | **des-cbc** } *

undo ssh2 algorithm cipher

Default

SSH2 uses encryption algorithms AES128-CTR, AES192-CTR, AES256-CTR, AES128-GCM, AES256-GCM, AES128-CBC, 3DES-CBC, AES256-CBC, and DES-CBC in descending order of priority for algorithm negotiation.

Views

System view

Predefined user roles

network-admin

Parameters

3des-cbc: Specifies encryption algorithm 3DES-CBC.

aes128-cbc: Specifies encryption algorithm AES128-CBC.

aes128-ctr: Specifies encryption algorithm AES128-CTR.

aes128-gcm: Specifies encryption algorithm AES128-GCM.

aes192-ctr: Specifies encryption algorithm AES192-CTR.

aes256-cbc: Specifies encryption algorithm AES256-CBC.

aes256-ctr: Specifies encryption algorithm AES256-CTR.

aes256-gcm: Specifies encryption algorithm AES256-GCM.

des-cbc: Specifies encryption algorithm DES-CBC.

Usage guidelines

If you specify the encryption algorithms, SSH2 uses only the specified algorithms for algorithm negotiation. The algorithm specified earlier has a higher priority during negotiation.

Examples

Specify algorithm **aes256-cbc** as the encryption algorithm for SSH2.

```
<Switch> system-view
[Switch] ssh2 algorithm cipher aes256-cbc
```

Related commands

display ssh2 algorithm

ssh2 algorithm key-exchange

ssh2 algorithm mac

ssh2 algorithm public-key

9.3.3. ssh2 algorithm key-exchange

> 🕮 **MEMO :**
>
> **ssh2 algorithm key-exchange** command is supported from later software, including Version 7.2.17.

Use **ssh2 algorithm key-exchange** to specify key exchange algorithms for SSH2.

Use **undo ssh2 algorithm key-exchange** to restore the default.

Syntax

ssh2 algorithm key-exchange { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** | **ecdh-sha2-nistp256** | **ecdh-sha2-nistp384** } *

undo ssh2 algorithm key-exchange

Default

SSH2 uses key exchange algorithms ecdh-sha2-nistp256, ecdh-sha2-nistp384, diffie-hellman-group-exchange-sha1, diffie-hellman-group14-sha1, and diffie-hellman-group1-sha1 in descending order of priority for algorithm negotiation.

Views

System view

Predefined user roles

network-admin

Parameters

dh-group-exchange-sha1: Specifies key exchange algorithm diffie-hellman-group-exchange-sha1.

dh-group1-sha1: Specifies key exchange algorithm diffie-hellman-group1-sha1.

dh-group14-sha1: Specifies key exchange algorithm diffie-hellman-group14-sha1.

ecdh-sha2-nistp256: Specifies key exchange algorithm ecdh-sha2-nistp256.

ecdh-sha2-nistp384: Specifies key exchange algorithm ecdh-sha2-nistp384.

Usage guidelines

If you specify the key exchange algorithms, SSH2 uses only the specified algorithms for algorithm negotiation. The algorithm specified earlier has a higher priority during negotiation.

Examples

Specify algorithm **dh-group1-sha1** as the key exchange algorithm for SSH2.

```
<Switch> system-view
[Switch] ssh2 algorithm key-exchange dh-group1-sha1
```

Related commands

display ssh2 algorithm

ssh2 algorithm cipher

ssh2 algorithm mac

ssh2 algorithm public-key

9.3.4. ssh2 algorithm mac

> 🕮 **MEMO :**
>
> **ssh2 algorithm mac** command is supported from later software, including Version 7.2.17.

Use **ssh2 algorithm mac** to specify HMAC algorithms for SSH2.

Use **undo ssh2 algorithm mac** to restore the default.

Syntax

ssh2 algorithm mac { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** } *

undo ssh2 algorithm mac

Default

SSH2 uses HMAC algorithms SHA2-256, SHA2-512, SHA1, MD5, SHA1-96, and MD5-96 in descending order of priority for algorithm negotiation.

Views

System view

Predefined user roles

network-admin

Parameters

md5: Specifies HMAC algorithm HMAC-MD5.

md5-96: Specifies HMAC algorithm HMAC-MD5-96.

sha1: Specifies HMAC algorithm HMAC-SHA1.

sha1-96: Specifies HMAC algorithm HMAC-SHA1-96.

sha2-256: Specifies HMAC algorithm HMAC-SHA2-256.

sha2-512: Specifies HMAC algorithm HMAC-SHA2-512.

Usage guidelines

If you specify the HMAC algorithms, SSH2 uses only the specified algorithms for algorithm negotiation. The algorithm specified earlier has a higher priority during negotiation.

Examples

Specify algorithm **md5** as the HMAC algorithm for SSH2.

```
<Switch> system-view
[Switch] ssh2 algorithm mac md5
```

Related commands

display ssh2 algorithm

ssh2 algorithm cipher

ssh2 algorithm key-exchange

ssh2 algorithm public-key

9.3.5. ssh2 algorithm public-key

> 🕮 **MEMO :**
>
> **ssh2 algorithm public-key** command is supported from later software, including Version 7.2.17.

Use **ssh2 algorithm public-key** to specify public key algorithms for SSH2.

Use **undo ssh2 algorithm public-key** to restore the default.

Syntax

ssh2 algorithm public-key { **dsa** | **ecdsa-sha2-nistp256** | **ecdsa-sha2-nistp384** | **rsa** | **x509v3-ecdsa-sha2-nistp256** | **x509v3-ecdsa-sha2-nistp384** } *

undo ssh2 algorithm public-key

Default

SSH2 uses public key algorithms x509v3-ecdsa-sha2-nistp256, x509v3-ecdsa-sha2-nistp384, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, RSA, and DSA in descending order of priority for algorithm negotiation.

Views

System view

Predefined user roles

network-admin

Parameters

dsa: Specifies public key algorithm DSA.

ecdsa-sha2-nistp256: Specifies public key algorithm ecdsa-sha2-nistp256.

ecdsa-sha2-nistp384: Specifies public key algorithm ecdsa-sha2-nistp384.

rsa: Specifies public key algorithm RSA.

x509v3-ecdsa-sha2-nistp256: Specifies public key algorithm x509v3-ecdsa-sha2-nistp256.

x509v3-ecdsa-sha2-nistp384: Specifies public key algorithm x509v3-ecdsa-sha2-nistp384.

Usage guidelines

If you specify the public key algorithms, SSH2 uses only the specified algorithms for algorithm negotiation. The algorithm specified earlier has a higher priority during negotiation.

Examples

Specify algorithm **dsa** as the public key algorithm for SSH2.

```
<Switch> system-view
```

```
[Switch] ssh2 algorithm public-key dsa
```

Related commands

display ssh2 algorithm

ssh2 algorithm cipher

ssh2 algorithm key-exchange

ssh2 algorithm mac

Contents

A page of this section is **9-x-x**

10. SSL commands 10-0
10.1. SSL commands 10-0
10.1.1. display ssl server-policy 10-0
10.1.2. pki-domain (SSL client policy view) 10-0
10.1.3. pki-domain (SSL server policy view) 10-1
10.1.4. security-enhanced level 10-2
10.1.5. ssl server-policy 10-3
10.1.6. ssl version disable 10-3

10. SSL commands

10.1. SSL commands

10.1.1. display ssl server-policy

Use **display ssl server-policy** to display SSL server policy information.

Syntax

display ssl server-policy [*policy-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

policy-name: Specifies an SSL server policy by its name, a case-insensitive string of 1 to 31 characters. If you do not specify a policy name, this command displays information about all SSL server policies.

Examples

Display information about the SSL server policy **policy1**.

```
<Switch> display ssl server-policy policy1
 SSL server policy: policy1
     PKI domain: server-domain
     Ciphersuites:
         DHE_RSA_AES_128_CBC_SHA
         RSA_AES_128_CBC_SHA
     Session cache size: 600
     Caching timeout: 3600 seconds
     Client-verify: Enabled
```

Table 10-1 Command output

Field	Description
Caching timeout	Session cache timeout time in seconds.
Client-verify	SSL client authentication mode, including: • **Disabled**—SSL client authentication is disabled. • **Enabled**—SSL client authentication is mandatory. • **Optional**—SSL client authentication is optional.

10.1.2. pki-domain (SSL client policy view)

Use **pki-domain** to specify a PKI domain for an SSL client policy.

Use **undo pki-domain** to restore the default.

Syntax

pki-domain *domain-name*

undo pki-domain

Default

No PKI domain is specified for an SSL client policy.

Views

SSL client policy view

Predefined user roles

network-admin

Parameters

domain-name: Specifies a PKI domain by its name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

If you specify a PKI domain for an SSL client policy, the SSL client that uses the SSL client policy will obtain its digital certificate through the specified PKI domain.

Examples

Specify PKI domain **client-domain** for SSL client policy **policy1**.

```
<Switch> system-view
[Switch] ssl client-policy policy1
[Switch-ssl-client-policy-policy1] pki-domain client-domain
```

Related commands

pki domain

10.1.3. pki-domain (SSL server policy view)

Use **pki-domain** to specify a PKI domain for an SSL server policy.

Use **undo pki-domain** to restore the default.

Syntax

pki-domain *domain-name*

undo pki-domain

Default

No PKI domain is specified for an SSL server policy.

Views

SSL server policy view

Predefined user roles

network-admin

Parameters

domain-name: Specifies a PKI domain by its name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

If you specify a PKI domain for an SSL server policy, the SSL server that uses the SSL server policy will obtain its digital certificate through the specified PKI domain.

Examples

Specify PKI domain **server-domain** for SSL server policy **policy1**.

```
<Switch> system-view
[Switch] ssl server-policy policy1
[Switch-ssl-server-policy-policy1] pki-domain server-domain
```

Related commands

display ssl server-policy

pki domain

10.1.4. security-enhanced level

Use **security-enhanced level** to specify a security enhanced level for the device.

Use **undo security-enhanced level** to restore the default.

Syntax

security-enhanced level 1

undo security-enhanced level

Default

The security enhanced level is 1 for the device.

Views

System view

Predefined user roles

network-admin

Parameters

level-value: Specifies the security enhanced level. QX-S5600G series supports only level 1.

Usage guidelines

The security enhanced level for the device can be 1.

- SSL client policies and SSL server policies support cipher suites that contain DES, 3DES, MD5, RC4, and RC2.
- SSL client policies and SSL server policies support SSL protocol versions lower than TLS 1.1.
- SSL session renegotiation can be enabled.

Examples

Set the security enhanced level to 1 for the device.

```
<Sysname> system-view
[Sysname] security-enhanced level 1
```

MEMO:

security-enhanced level command is supported from later software, including Version 7.4.30. The security level specifications are the same as before Version 7.4.27.

10.1.5. ssl server-policy

Use **ssl server-policy** to create an SSL server policy and enter its view, or enter the view of an existing SSL server policy.

Use **undo ssl server-policy** to delete an SSL server policy.

Syntax

ssl server-policy *policy-name*

undo ssl server-policy *policy-name*

Default

No SSL server policies exist.

Views

System view

Predefined user roles

network-admin

Parameters

policy-name: Specifies a name for the SSL server policy, a case-insensitive string of 1 to 31 characters.

Usage guidelines

This command creates an SSL server policy for which you can configure SSL parameters such as a PKI domain and supported cipher suits. An SSL server policy takes effect only after it is associated with an application such as HTTPS.

Examples

Create an SSL server policy named **policy1** and enter its view.

```
<Switch> system-view
[Switch] ssl server-policy policy1
[Switch-ssl-server-policy-policy1]
```

Related commands

display ssl server-policy

10.1.6. ssl version disable

Use **ssl version disable** to disable the SSL server from using specific SSL protocol versions for session negotiation.

Use **undo ssl version disable** restore the default.

Syntax

ssl version { **ssl3.0 | tls1.0 | tls1.1 | tls1.2 | tls1.3** } **disable**

undo ssl version ssl3.0 disable

Default

The SSL server supports SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3.

Views

System view

Predefined user roles

network-admin

Parameters

ssl3.0: Specifies SSL 3.0.

tls1.0: Specifies TLS 1.0.

tls1.1: Specifies TLS 1.1.

tls1.2: Specifies TLS 1.2.

tls1.3: Specifies TLS 1.3.

Usage guidelines

To enhance system security, you can disable the SSL server from using specific SSL protocol versions (SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3) for session negotiation.

Examples

Disable SSL 3.0 for the SSL server.

```
<Switch> system-view
[Switch] ssl version ssl3.0 disable
```

Contents

A page of this section is **9-x-x**

11. Attack detection and prevention commands 11-1
11.1. Attack detection and prevention commands 11-1
11.1.1. attack-defense tcp fragment enable 11-1

11. Attack detection and prevention commands

11.1. Attack detection and prevention commands

11.1.1. attack-defense tcp fragment enable

Use **attack-defense tcp fragment enable** to enable TCP fragment attack prevention.

Use **undo attack-defense tcp fragment enable** to disable TCP fragment attack prevention.

Syntax

attack-defense tcp fragment enable

undo attack-defense tcp fragment enable

Default

TCP fragment attack prevention is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command enables the device to drop attack TCP fragments to prevent TCP fragment attacks that the packet filter cannot detect. As defined in RFC 1858, attack TCP fragments refer to the following TCP fragments:

- First fragments in which the TCP header is smaller than 20 bytes.
- Non-first fragments with a fragment offset of 8 bytes (FO=1).

The device supports verifying only TCP fragments forwarded through the CPU.

Examples

Enable TCP fragment attack prevention.

```
<Switch> System-view
[Switch] attack-defense tcp fragment enable
```

Contents

A page of this section is **9-x-x**

12. IP source guard commands 12-1
12.1. IP source guard commands 12-1
12.1.1. display ip source binding 12-1
12.1.2. display ipv6 source binding 12-2
12.1.3. ip source binding (interface view) 12-4
12.1.4. ip verify source 12-5
12.1.5. ipv6 source binding (interface view) 12-6
12.1.6. ipv6 verify source 12-7

12. IP source guard commands

12.1. IP source guard commands

12.1.1. display ip source binding

Use **display ip source binding** to display IPv4SG bindings.

Syntax

display ip source binding [**static** | [**vpn-instance** *vpn-instance-name*] [**arp-suppression** | **dhcp-relay** | **dhcp-server** | **dhcp-snooping**]] [**ip-address** *ip-address*] [**mac-address** *mac-address*] [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

static: Displays static IPv4SG bindings.

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. To display dynamic IPv4SG bindings for the public network, do not specify a VPN instance.

arp-suppression: Specifies the ARP flood suppression module.

dhcp-relay: Specifies the DHCP relay agent module.

dhcp-server: Specifies the DHCP server module.

dhcp-snooping: Specifies the DHCP snooping module.

ip-address *ip-address*: Specifies an IPv4 address.

mac-address *mac-address*: Specifies a MAC address in H-H-H format.

vlan *vlan-id*: Specifies a VLAN ID in the range of 1 to 4094.

interface *interface-type interface-number*: Specifies an interface by its type and number.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays IPv4SG bindings for the master device.

Examples

Display all IPSG bindings on the public network.

```
<Switch> display ip source binding
Total entries found: 5
IP Address      MAC Address    Interface               VLAN Type
10.1.0.5        040a-0000-4000 GE1/0/1                 1    DHCP snooping
10.1.0.6        040a-0000-3000 GE1/0/1                 1    DHCP snooping
```

```
10.1.0.7        040a-0000-2000 GE1/0/1                1    DHCP snooping
10.1.0.8        040a-0000-1000 GE1/0/2                N/A  DHCP relay
10.1.0.9        040a-0000-2000 GE1/0/2                N/A  Static
```

Table 12-1 Command output

Field	Description
Total entries found	Total number of IPv4SG bindings.
IP Address	IPv4 address in the IPv4SG binding. If no IP address is bound in the binding, this field displays **N/A**.
MAC Address	MAC address in the IPv4SG binding. If no MAC address is bound in the binding, this field displays **N/A**.
Interface	Interface of the binding. This field displays **N/A** for a global IPv4SG binding.
VLAN	VLAN information in the IPv4SG binding. If the binding contains no VLAN information, this field displays **N/A**.
Type	IPSG binding type: • **Static**—Manually configured by using the **ip source binding** command. Static bindings are for packet filtering in IPSG or used by other modules to provide security services. • **ARP snooping**—Dynamically generated based on ARP snooping. The binding is for packet filtering in IPSG. • **ARP suppression**—Dynamically generated based on ARP flood suppression. The binding is for packet filtering in IPSG. • **802.1X**—Dynamically generated based on 802.1X. The binding is for packet filtering in IPSG. • **DHCP relay**—Dynamically generated based on DHCP relay agent. The binding is for packet filtering in IPSG. • **DHCP server**—Dynamically generated based on DHCP server. The binding is used by other modules to provide security services. • **DHCP snooping**—Dynamically generated based on DHCP snooping. The binding is for packet filtering in IPSG.

Related commands

ip source binding

ip verify source

12.1.2. display ipv6 source binding

Use **display ipv6 source binding** to display IPv6SG address bindings.

Syntax

display ipv6 source binding [**static** | [**vpn-instance** *vpn-instance-name*] [**dhcpv6-snooping**]] [**ip-address** *ipv6-address*] [**mac-address** *mac-address*] [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

static: Displays static IPv6SG address bindings.

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. To display dynamic IPv6SG address bindings for the public network, do not specify a VPN instance.

dhcpv6-snooping: Specifies the DHCPv6 snooping module.

ip-address *ipv6-address*: Specifies an IPv6 address.

mac-address *mac-address*: Specifies a MAC address in H-H-H format.

vlan *vlan-id*: Specifies a VLAN ID in the range of 1 to 4094.

interface *interface-type interface-number*: Specifies an interface by its type and number.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays IPv6SG address bindings for the master device.

Examples

Display all IPv6SG address bindings on the public network.

```
<Switch> display ipv6 source binding
Total entries found: 2
IPv6 Address          MAC Address    Interface              VLAN Type
2012:1222:2012:1222:  000f-2202-0435 GE1/0/1                 1    DHCPv6 snooping
2012:1222:2012:1222
2012:1222:2012:1222:  000f-2202-0436 GE1/0/1                 N/A  Static
2012:1222:2012:1223
```

Table 12-2 Command output

Field	Description
Total entries found	Total number of IPv6SG address bindings.
IPv6 Address	IPv6 address in the IPv6SG address binding. If no IPv6 address is bound in the binding, this field displays **N/A**.
MAC Address	MAC address in the IPv6SG address binding. If no MAC address is bound in the binding, this field displays **N/A**.
Interface	Interface of the IPv6SG address binding. This field displays **N/A** for a global IPv6SG binding.
VLAN	VLAN information in the IPv6SG address binding. If the binding contains no VLAN information, this field displays **N/A**.
Type	Type of the IPv6SG address binding: • **Static**—Manually configured by using the **ipv6 source binding** command. Static bindings are for packet filtering in IPv6SG or used by other modules to provide security services.

Field	Description
	• **DHCPv6 relay**—Dynamically generated based on DHCPv6 relay agent. The binding is for packet filtering in IPv6SG. • **DHCPv6 snooping**—Dynamically generated based on DHCPv6 snooping. The binding is for packet filtering in IPv6SG. • **802.1X**—Dynamically generated based on 802.1X. The binding is for packet filtering in IPv6SG. • **ND suppression**—Dynamically generated based on ND suppression. The binding is for packet filtering in IPv6SG.

Related commands

ipv6 source binding

ipv6 verify source

12.1.3. ip source binding (interface view)

Use **ip source binding** to configure a static IPv4SG binding on an interface.

Use **undo ip source binding** to delete the static IPv4SG bindings configured on an interface.

Syntax

ip source binding { **ip-address** *ip-address* | **ip-address** *ip-address* **mac-address** *mac-address* | **mac-address** *mac-address* } [**vlan** *vlan-id*]

undo ip source binding { **all** | **ip-address** *ip-address* | **ip-address** *ip-address* **mac-address** *mac-address* | **mac-address** *mac-address* } [**vlan** *vlan-id*]

Default

No static IPv4SG bindings exist on an interface.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

VLAN interface view

Predefined user roles

network-admin

Parameters

all: Removes all static IPv4SG bindings on the interface.

ip-address *ip-address*: Specifies an IPv4 address for the static binding. The IPv4 address must be a class A, B, or C address, and cannot be 127.x.x.x or 0.0.0.0.

mac-address *mac-address*: Specifies a MAC address for the static binding. The MAC address must be in H-H-H format, and cannot be all 0s, all Fs (a broadcast MAC address), or a multicast MAC address.

vlan *vlan-id*: Specifies a VLAN ID for the static binding. The value range is 1 to 4094. This option is supported only in Layer 2 Ethernet interface view.

Usage guidelines

Static IPv4SG bindings on an interface implement the following functions:

- Filter incoming IPv4 packets on the interface.
- Check user validity by cooperating with the ARP attack detection feature.

Examples

Configure a static IPv4SG binding on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] ip source binding ip-address 192.168.0.1 mac-address
0001-0001-0001
```

Related commands

display ip source binding

12.1.4. ip verify source

Use **ip verify source** to enable IPv4SG on an interface.

Use **undo ip verify source** to disable IPv4SG on an interface.

Syntax

ip verify source { **ip-address** | **ip-address mac-address** | **mac-address** }

undo ip verify source

Default

The IPv4SG feature is disabled on an interface.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

VLAN interface view

VLAN view

MEMO:

VLAN View became practicable after v7.2.16.

Predefined user roles

network-admin

Parameters

ip-address: Filters incoming packets by source IPv4 addresses.

ip-address mac-address: Filters incoming packets by source IPv4 addresses and source MAC addresses.

mac-address: Filters incoming packets by source MAC addresses.

Usage guidelines

After you enable IPv4SG on an interface, this feature uses static and dynamic IPv4SG bindings to match incoming packets on the interface. Packets that match an IPv4SG binding are forwarded and packets that do not match any IPv4SG binding are discarded.

The matching criterion specified by this command applies only to dynamic IPSG. Static IPv4SG uses static bindings configured by using the **ip source binding** command.

Examples

Enable IPv4SG on Layer 2 Ethernet interface GigabitEthernet 1/0/1 and verify the source IPv4 address and MAC address for dynamic IPSG.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] ip verify source ip-address mac-address
```

Enable IPv4SG on VLAN-interface 100 and verify the source IPv4 address and MAC address for dynamic IPSG.

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ip verify source ip-address mac-address
```

Enable IPv4SG on Layer 3 Ethernet interface GigabitEthernet 1/0/2 and verify the source IPv4 address and MAC address for dynamic IPSG.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] ip verify source ip-address mac-address
```

Enable IPv4SG on Layer 3 Ethernet interface GigabitEthernet 1/0/2 and verify the source MAC address for dynamic IPSG.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] ip verify source mac-address
```

Related commands

display ip source binding

12.1.5. ipv6 source binding (interface view)

Use **ipv6 source binding** to configure a static IPv6SG binding.

Use **undo ipv6 source binding** to delete the static IPv6SG bindings configured on an interface.

Syntax

ipv6 source binding { **ip-address** *ipv6-address* | **ip-address** *ipv6-address* **mac-address** *mac-address* | **mac-address** *mac-address* } [**vlan** *vlan-id*]

undo ipv6 source binding { **all** | **ip-address** *ipv6-address* | **ip-address** *ipv6-address* **mac-address** *mac-address* | **mac-address** *mac-address* } [**vlan** *vlan-id*]

Default

No static IPv6SG bindings exist on an interface.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

VLAN interface view

Predefined user roles

network-admin

Parameters

all: Removes all the static IPv6SG bindings on the interface.

ip-address *ipv6-address*: Specifies an IPv6 address for the static binding. The IPv6 address cannot be an all-zero address, a multicast address, or a loopback address.

mac-address *mac-address*: Specifies a MAC address for the static binding. The MAC address must be in H-H-H format, and cannot be all 0s, all Fs (a broadcast MAC address), or a multicast MAC address.

vlan *vlan-id*: Specifies a VLAN ID for the static binding. The value range is 1 to 4094. This option is supported only in Layer 2 Ethernet interface view.

Usage guidelines

Static IPv6SG bindings on an interface filter incoming IPv6 packets.

Examples

Configure a static IPv6SG binding on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] ipv6 source binding ip-address 2001::1 mac-address
0002-0002-0002
```

Related commands

display ipv6 source binding

12.1.6. ipv6 verify source

Use **ipv6 verify source** to enable IPv6SG on an interface.

Use **undo ipv6 verify source** to disable IPv6SG on an interface.

Syntax

ipv6 verify source { **ip-address** | **ip-address mac-address** | **mac-address** }

undo ipv6 verify source

Default

The IPv6SG feature is disabled on an interface.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

VLAN interface view

VLAN view

MEMO:

VLAN View became practicable after v7.2.16.

Predefined user roles

network-admin

Parameters

ip-address: Filters incoming packets by source IPv6 addresses.

ip-address mac-address: Filters incoming packets by source IPv6 addresses and source MAC addresses.

mac-address: Filters incoming packets by source MAC addresses.

Usage guidelines

After you enable IPv6SG on an interface, this feature uses static and dynamic IPv6SG bindings to match incoming packets on the interface. Packets that match an IPv6SG binding are forwarded and packets that do not match any IPv6SG binding are discarded.

The matching criterion specified by this command applies only to dynamic IPv6SG. Static IPv6SG uses static bindings configured by using the **ipv6 source binding** command.

Examples

Enable IPv6SG on Layer 2 Ethernet interface GigabitEthernet 1/0/1 and verify the source IPv6 address and MAC address for dynamic IPv6SG.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] ipv6 verify source ip-address mac-address
```

Related commands

display ipv6 source binding

Contents

A page of this section is **9-x-x**

13. ARP attack protection commands 13-1
13.1. Unresolvable IP attack protection commands 13-1
13.1.1. arp resolving-route enable 13-1
13.1.2. arp resolving-route probe-count 13-1
13.1.3. arp resolving-route probe-interval 13-2
13.1.4. arp source-suppression enable 13-3
13.1.5. arp source-suppression limit 13-3
13.1.6. display arp source-suppression 13-4
13.2. ARP packet rate limit commands 13-4
13.2.1. arp rate-limit 13-4
13.2.2. arp rate-limit log enable 13-5
13.2.3. arp rate-limit log interval 13-6
13.2.4. snmp-agent trap enable arp 13-7
13.3. Source MAC-based ARP attack detection commands 13-7
13.3.1. arp source-mac 13-7
13.3.2. arp source-mac aging-time 13-8
13.3.3. arp source-mac exclude-mac 13-9
13.3.4. arp source-mac threshold 13-9
13.3.5. display arp source-mac 13-10
13.4. ARP packet source MAC consistency check commands 13-11
13.4.1. arp valid-check enable 13-11
13.5. ARP active acknowledgement commands 13-11
13.5.1. arp active-ack enable 13-11
13.6. ARP attack detection commands 13-12
13.6.1. arp detection enable 13-12
13.6.2. arp detection trust 13-13
13.6.3. arp detection validate 13-13
13.6.4. arp restricted-forwarding enable 13-14
13.6.5. display arp detection 13-15
13.6.6. display arp detection statistics attack-source 13-15
13.6.7. display arp detection statistics packet-drop 13-16
13.6.8. reset arp detection statistics attack-source 13-17
13.6.9. reset arp detection statistics packet-drop 13-18
13.7. ARP scanning commands 13-18
13.7.1. arp scan 13-18
13.8. ARP gateway protection commands 13-20
13.8.1. arp filter source 13-20
13.9. ARP filtering commands 13-20
13.9.1. arp filter binding 13-20

13. ARP attack protection commands

13.1. Unresolvable IP attack protection commands

13.1.1. arp resolving-route enable

Use **arp resolving-route enable** to enable ARP blackhole routing.

Use **undo arp resolving-route enable** to disable ARP blackhole routing.

Syntax

arp resolving-route enable

undo arp resolving-route enable

Default

ARP blackhole routing is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Configure this command on the gateways.

Examples

Enable ARP blackhole routing.

```
<Switch> system-view
[Switch] arp resolving-route enable
```

Related commands

arp resolving-route probe-count

arp resolving-route probe-interval

13.1.2. arp resolving-route probe-count

Use **arp resolving-route probe-count** to set the number of ARP blackhole route probes for each unresolved IP address.

Use **undo arp resolving-route probe-count** to restore the default.

Syntax

arp resolving-route probe-count *count*

undo arp resolving-route probe-count

Default

The device performs three ARP blackhole route probes for each unresolved IP address.

Views

System view

Predefined user roles

network-admin

Parameters

count: Sets the number of probes, in the range of 1 to 25.

Examples

Configure the device to perform five ARP blackhole route probes for each unresolved IP address.

```
<Switch> system-view
[Switch] arp resolving-route probe-count 5
```

Related commands

arp resolving-route enable

arp resolving-route probe-interval

13.1.3. arp resolving-route probe-interval

Use **arp resolving-route probe-interval** to set the interval at which the device probes ARP blackhole routes.

Use **undo arp resolving-route probe-interval** to restore the default.

Syntax

arp resolving-route probe-interval *interval*

undo arp resolving-route probe-interval

Default

The device probes ARP blackhole routes every 1 second.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the probe interval in the range of 1 to 5 seconds.

Examples

Configure the device to probe ARP blackhole routes every 3 seconds.

```
<Switch> system-view
[Switch] arp resolving-route probe-interval 3
```

Related commands

arp resolving-route enable

arp resolving-route probe-count

13.1.4. arp source-suppression enable

Use **arp source-suppression enable** to enable the ARP source suppression feature.

Use **undo arp source-suppression enable** to disable the ARP source suppression feature.

Syntax

arp source-suppression enable

undo arp source-suppression enable

Default

The ARP source suppression feature is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Configure this feature on the gateways.

Examples

Enable the ARP source suppression feature.

```
<Switch> system-view
[Switch] arp source-suppression enable
```

Related commands

display arp source-suppression

13.1.5. arp source-suppression limit

Use **arp source-suppression limit** to set the maximum number of unresolvable packets that can be processed per source IP address within 5 seconds.

Use **undo arp source-suppression limit** to restore the default.

Syntax

arp source-suppression limit *limit-value*

undo arp source-suppression limit

Default

The device can process a maximum of 10 unresolvable packets per source IP address within 5 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

limit-value: Specifies the limit in the range of 2 to 1024.

Usage guidelines

If unresolvable packets received from an IP address within 5 seconds exceed the limit, the device stops processing the packets from that IP address until the 5 seconds elapse.

Examples

Configure the device to process a maximum of 100 unresolvable packets per source IP address within 5 seconds.

```
<Switch> system-view
[Switch] arp source-suppression limit 100
```

Related commands

display arp source-suppression

13.1.6. display arp source-suppression

Use **display arp source-suppression** to display information about the current ARP source suppression configuration.

Syntax

display arp source-suppression

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display information about the current ARP source suppression configuration.

```
<Switch> display arp source-suppression
 ARP source suppression is enabled
 Current suppression limit: 100
```

Table 13-1 Command output

Field	Description
Current suppression limit	Maximum number of unresolvable packets that can be processed per source IP address within 5 seconds.

13.2. ARP packet rate limit commands

13.2.1. arp rate-limit

Use **arp rate-limit** to enable the ARP packet rate limit feature on an interface.

Use **undo arp rate-limit** to disable the ARP packet rate limit feature on an interface.

Syntax

arp rate-limit [*pps*]

undo arp rate-limit

Default

The ARP packet rate limit feature is enabled on an interface.

Before v7.1.6 100pps

After v7.2.16 600pps

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Layer 3 Ethernet interface view

Predefined user roles

network-admin

Parameters

Before v7.1.6

pps: Specifies the upper limit for ARP packet rate in pps. The value range for this argument is 5 to 200.

After v7.2.16

pps: Specifies the upper limit for ARP packet rate in pps. The value range for this argument is 5 to 600.

Usage guidelines

If you do not specify a value for the *pps* argument in the **arp rate-limit** command, the default rate limit value applies. Packets that exceed the rate limit are discarded.

Examples

Enable the ARP packet rate limit feature on GigabitEthernet 1/0/1, and set the maximum ARP packet rate to 50 pps.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] arp rate-limit 50
```

NOTE:

QX-S5600G series can be certified up to 100PPS.

13.2.2. arp rate-limit log enable

Use **arp rate-limit log enable** to enable logging for ARP packet rate limit.

Use **undo arp rate-limit log enable** to disable logging for ARP packet rate limit.

Syntax

arp rate-limit log enable

undo arp rate-limit log enable

Default

Logging for ARP packet rate limit is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

When logging for ARP packet rate limit is enabled, the device sends the highest threshold-crossed ARP packet rate within the sending interval in a log message to the information center. You can configure the information center module to set the log output rules. For more information about information center, see *Network Management and Monitoring Configuration Guide*.

Examples

Enable logging for ARP packet rate limit.

```
<Switch> system-view
[Switch] arp rate-limit log enable
```

13.2.3. arp rate-limit log interval

Use **arp rate-limit log interval** to set the notification and log message sending interval for ARP packet rate limit.

Use **undo arp rate-limit log interval** to restore the default.

Syntax

arp rate-limit log interval *interval*

undo arp rate-limit log interval

Default

The device sends notifications or log messages every 60 seconds when the rate of ARP packets received on an interface exceeds the limit.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies an interval in the range of 1 to 86400 seconds.

Usage guidelines

To change the default interval and activate it, you must enable ARP packet rate limit and enable sending notifications or log messages for ARP packet rate limit.

Examples

Set the device to send notifications and log messages every 120 seconds when the rate of ARP packets received on an interface exceeds the limit.

```
<Switch> system-view
[Switch] arp rate-limit log interval 120
```

Related commands

arp rate-limit

arp rate-limit log enable

snmp-agent trap enable arp

13.2.4. snmp-agent trap enable arp

Use **snmp-agent trap enable arp** to enable SNMP notifications for ARP.

Use **undo snmp-agent trap enable arp** to disable SNMP notifications for ARP.

Syntax

snmp-agent trap enable arp [**rate-limit**]

undo snmp-agent trap enable arp [**rate-limit**]

Default

SNMP notifications for ARP is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

rate-limit: Specifies the ARP packet rate limit feature.

Usage guidelines

After you enable SNMP notifications for ARP, the device generates a notification that includes the highest threshold-crossed ARP packet rate within the sending interval.

For ARP event notifications to be sent correctly, you must also configure SNMP on the device. For more information about SNMP configuration, see the network management and monitoring configuration guide for the device.

Examples

Enable SNMP notifications for ARP packet rate limit.

```
<Switch> system-view
[Switch] snmp-agent trap enable arp rate-limit
```

13.3. Source MAC-based ARP attack detection commands

13.3.1. arp source-mac

Use **arp source-mac** to enable the source MAC-based ARP attack detection feature and specify a handling method.

Use **undo arp source-mac** to disable the source MAC-based ARP attack detection feature.

Syntax

arp source-mac { **filter** | **monitor** }

undo arp source-mac [**filter** | **monitor**]

Default

The source MAC-based ARP attack detection feature is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

filter: Specifies the filter handling method.

monitor: Specifies the monitor handling method.

Usage guidelines

Configure this feature on the gateways.

This feature checks the number of ARP packets delivered to the CPU. If the number of packets from the same MAC address within 5 seconds exceeds a threshold, the device generates an ARP attack entry for the MAC address. Before the entry ages out, the device handles the attack by using either of the following methods:

- **Monitor**—Only generates log messages.
- **Filter**—Generates log messages and filters out subsequent ARP packets from the MAC address.

Make sure you have enabled the ARP logging feature before enabling the source MAC-based ARP attack detection feature. For information about the ARP logging feature, see *Layer 3—IP Services Configuration Guide*.

If you do not specify any handling method in the **undo arp source-mac** command, the command disables this feature.

Examples

Enable the source MAC-based ARP attack detection feature and specify the filter handling method.

```
<Switch> system-view
[Switch] arp source-mac filter
```

13.3.2. arp source-mac aging-time

Use **arp source-mac aging-time** to set the aging time for ARP attack entries.

Use **undo arp source-mac aging-time** to restore the default.

Syntax

arp source-mac aging-time *time*

undo arp source-mac aging-time

Default

The aging time for ARP attack entries is 300 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

time: Sets the aging time for ARP attack entries, in the range of 60 to 6000 seconds.

Examples

Set the aging time for ARP attack entries to 60 seconds.

```
<Switch> system-view
[Switch] arp source-mac aging-time 60
```

13.3.3. arp source-mac exclude-mac

Use **arp source-mac exclude-mac** to exclude specific MAC addresses from source MAC-based ARP attack detection.

Use **undo arp source-mac exclude-mac** to remove the excluded MAC addresses from source MAC-based ARP attack detection.

Syntax

arp source-mac exclude-mac *mac-address*&<1-10>

undo arp source-mac exclude-mac [*mac-address*&<1-10>]

Default

No MAC addresses are excluded from source MAC-based ARP attack detection.

Views

System view

Predefined user roles

network-admin

Parameters

mac-address&<1-10>: Specifies a MAC address list. The *mac-address* argument indicates an excluded MAC address in the format of H-H-H. &<1-10> indicates that you can configure a maximum of 10 excluded MAC addresses.

Usage guidelines

If you do not specify a MAC address, the **undo arp source-mac exclude-mac** command removes all excluded MAC addresses.

Examples

Exclude a MAC address from source MAC-based ARP attack detection.

```
<Switch> system-view
[Switch] arp source-mac exclude-mac 001e-1200-0213
```

13.3.4. arp source-mac threshold

Use **arp source-mac threshold** to set the threshold for source MAC-based ARP attack detection. If the number of ARP packets sent from a MAC address within 5 seconds exceeds this threshold, the device recognizes this as an attack.

Use **undo arp source-mac threshold** to restore the default.

Syntax

arp source-mac threshold *threshold-value*

undo arp source-mac threshold

Default

The threshold for source MAC-based ARP attack detection is 30.

Views

System view

Predefined user roles

network-admin

Parameters

threshold-value: Specifies the threshold for source MAC-based ARP attack detection. The value range for this argument is 1 to 5000.

Examples

Set the threshold for source MAC-based ARP attack detection to 30.

```
<Switch> system-view
[Switch] arp source-mac threshold 30
```

13.3.5. display arp source-mac

Use **display arp source-mac** to display ARP attack entries detected by source MAC-based ARP attack detection.

Syntax

display arp source-mac { **interface** *interface-type interface-number* | **slot** *slot-number* }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number.

slot *slot-number*: Specifies an IRF member device by its ID. If you do not specify a member device, this command displays ARP attack entries for the master device.

Examples

Display the ARP attack entries detected by source MAC-based ARP attack detection on GigabitEthernet 1/0/1.

```
<Switch> display arp source-mac interface gigabitethernet 1/0/1
Source-MAC          VLAN ID  Interface               Aging-time
23f3-1122-3344      4094     GE1/0/1                 10
```

Table 13-2 Command output

Field	Description
Source-MAC	Source MAC address of the attack.

Field	Description
VLAN ID	ID of the VLAN in which the attack was detected.
Interface	Interface on which the attack was detected.
Aging-time	Aging time for the ARP attack entry, in minutes.

13.4. ARP packet source MAC consistency check commands

13.4.1. arp valid-check enable

Use **arp valid-check enable** to enable ARP packet source MAC address consistency check.

Use **undo arp valid-check enable** to disable ARP packet source MAC address consistency check.

Syntax

arp valid-check enable

undo arp valid-check enable

Default

ARP packet source MAC address consistency check is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Configure this feature on gateways. The gateways can filter out ARP packets whose source MAC address in the Ethernet header is different from the sender MAC address in the message body.

Examples

Enable ARP packet source MAC address consistency check.

```
<Switch> system-view
[Switch] arp valid-check enable
```

13.5. ARP active acknowledgement commands

13.5.1. arp active-ack enable

Use **arp active-ack enable** to enable the ARP active acknowledgement feature.

Use **undo arp active-ack enable** to disable the ARP active acknowledgement feature.

Syntax

arp active-ack enable

undo arp active-ack enable

Default

The ARP active acknowledgement feature is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Configure this feature on gateways to prevent user spoofing.

Examples

Enable the ARP active acknowledgement feature.

```
<Switch> system-view
[Switch] arp active-ack enable
```

13.6. ARP attack detection commands

13.6.1. arp detection enable

Use **arp detection enable** to enable ARP attack detection.

Use **undo arp detection enable** to disable ARP attack detection.

Syntax

arp detection enable

undo arp detection enable

Default

ARP attack detection is disabled.

Views

VLAN view

VSI view

Predefined user roles

network-admin

Examples

Enable ARP attack detection for VLAN 2.

```
<Switch> system-view
[Switch] vlan 2
[Switch-vlan2] arp detection enable
```

Enable ARP attack detection for VSI **vsi1**.

```
<Switch> system-view
[Switch] vsi vsi1
[Switch-vsi-vsi1] arp detection enable
```

Related commands

display arp detection statistics attack-source

reset arp detection statistics attack-source

13.6.2. arp detection trust

Use **arp detection trust** to configure an interface as an ARP trusted interface or configure an AC as an ARP trusted AC.

Use **undo arp detection trust** to restore the default.

Syntax

arp detection trust

undo arp detection trust

Default

An interface is an ARP untrusted interface. An AC is an ARP untrusted AC.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Ethernet service instance view

Predefined user roles

network-admin

Examples

Configure GigabitEthernet 1/0/1 as an ARP trusted interface.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] arp detection trust
```

Configure Ethernet service instance 1 on Layer 2 Ethernet interface GigabitEthernet 1/0/1 as an ARP trusted AC.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] service-instance 1
[Switch-GigabitEthernet1/0/1-srv1] arp detection trust
```

13.6.3. arp detection validate

Use **arp detection validate** to enable ARP packet validity check.

Use **undo arp detection validate** to disable ARP packet validity check.

Syntax

arp detection validate { **dst-mac** | **ip** | **src-mac** } *

undo arp detection validate [**dst-mac** | **ip** | **src-mac**] *

Default

ARP packet validity check is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

dst-mac: Checks the target MAC address of ARP responses. If the target MAC address is all-zero, all-one, or inconsistent with the destination MAC address in the Ethernet header, the packet is considered invalid and discarded.

ip: Checks the sender and target IP addresses of ARP replies, and the sender IP address of ARP requests. All-one or multicast IP addresses are considered invalid and the corresponding packets are discarded.

src-mac: Checks whether the sender MAC address in the message body is identical to the source MAC address in the Ethernet header. If they are identical, the packet is forwarded. Otherwise, the packet is discarded.

Usage guidelines

You can specify more than one object to be checked in one command line.

If no keyword is specified, the **undo arp detection validate** command disables ARP packet validity check for all objects.

Examples

Enable ARP packet validity check by checking the MAC addresses and IP addresses of ARP packets.

```
<Switch> system-view
[Switch] arp detection validate dst-mac ip src-mac
```

13.6.4. arp restricted-forwarding enable

Use **arp restricted-forwarding enable** to enable ARP restricted forwarding.

Use **undo arp restricted-forwarding enable** to disable ARP restricted forwarding.

Syntax

arp restricted-forwarding enable

undo arp restricted-forwarding enable

Default

ARP restricted forwarding is disabled.

Views

VLAN view

Predefined user roles

network-admin

Examples

Enable ARP restricted forwarding in VLAN 2.

```
<Switch> system-view
[Switch] vlan 2
[Switch-vlan2] arp restricted-forwarding enable
```

13.6.5. display arp detection

Use **display arp detection** to display the VLANs and VSIs that are enabled with ARP attack detection.

Syntax

display arp detection

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display the VLANs and VSIs that are enabled with ARP attack detection.

```
<Switch> display arp detection
ARP detection is enabled in the following VLANs:
1-2, 4-5
 ARP detection is enabled in the following VSIs:
 vpna
 vsi-0000-0000-0031
 vpnb
 vpnc-vsi-0000-0000-00aa
```

Related commands

arp detection enable

13.6.6. display arp detection statistics attack-source

Use **display arp detection statistics attack-source** to display statistics for ARP attack sources.

Syntax

display arp detection statistics attack-source slot *slot-number*

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its ID. If you do not specify a member device, this command displays ARP attack source statistics for the master device.

Examples

Display statistics for ARP attack sources.

```
<Switch> display arp detection attack statistics attack-source
Interface              VLAN  MAC address    IP address      Number     Time
```

```
GE1/0/1                 1      0005-0001-0001 10.1.1.14       24          17:09:56
03-27-2017
```

Table 13-3 Command output

Field	Description
Interface	Receiving interface of ARP attack packets.
VLAN	VLAN to which ARP attack packets belong.
MAC address	Sender MAC address in ARP attack packets.
IP address	Sender IP address in ARP attack packets.
Number	Number of ARP attack packets dropped by ARP attack detection.
Time	The most recent time when ARP attack detection dropped an ARP attack packet.

Related commands

arp detection enable

13.6.7. display arp detection statistics packet-drop

Use **display arp detection statistics packet-drop** to display statistics for packets dropped by ARP attack detection.

Syntax

display arp detection statistics packet-drop [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays dropped packet statistics for all interfaces and all Ethernet service instances on the interfaces.

Usage guidelines

This command displays numbers of packets discarded by user validity check and ARP packet validity check on interfaces or Ethernet service instances on the interfaces.

Examples

Display statistics for packets dropped by ARP attack detection.

```
<Switch> display arp detection statistics packet-drop
State: U-Untrusted  T-Trusted
ARP packets dropped by ARP inspect checking:
Interface(State)            IP        Src-MAC   Dst-MAC   Inspect
GE1/0/1(U)                  40        0         0         78
GE1/0/2(U)                  0         0         0         0
```

```
GE1/0/3(T)                0          0          0          0
GE1/0/4(U)                0          0          30         0
GE1/0/5-srv1(U)           0          10         20         0
GE1/0/5-srv2(T)           10         0          20         22
```

Table 13-4 Command output

Field	Description
State	State of an interface: • **U**—ARP untrusted interface or AC. • **T**—ARP trusted interface or AC.
Interface(State)	Inbound interface or AC of ARP packets. State specifies the port state, **trusted** or **untrusted**.
IP	Number of ARP packets discarded due to invalid sender and target IP addresses.
Src-MAC	Number of ARP packets discarded due to invalid source MAC address.
Dst-MAC	Number of ARP packets discarded due to invalid destination MAC address.
Inspect	Number of ARP packets that failed to pass user validity check.

Related commands

reset arp detection statistics packet-drop

13.6.8. reset arp detection statistics attack-source

Use **reset arp detection statistics attack-source** to clear statistics for ARP attack sources.

Syntax

reset arp detection statistics attack-source [**slot** *slot-number*]

Views

User view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its ID. If you do not specify a member device, this command clears ARP attack source statistics for the master device.

Examples

Clear statistics for ARP attack sources.

```
<Switch> reset arp detection attack statistics attack-source
```

Related commands

arp detection enable

display arp detection statistics attack-source

13.6.9. reset arp detection statistics packet-drop

Use **reset arp detection statistics packet-drop** to clear statistics for packets dropped by ARP attack detection.

Syntax

reset arp detection statistics packet-drop [**interface** *interface-type interface-number*]

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command clears dropped packet statistics for all interfaces and all Ethernet service instances on the interfaces.

Examples

Clear statistics for packets dropped by ARP attack detection.

```
<Switch> reset arp detection statistics packet-drop
```

Related commands

display arp detection statistics packet-drop

13.7. ARP scanning commands

13.7.1. arp scan

Use **arp scan** to trigger an ARP scanning in an address range.

Syntax

arp scan [*start-ip-address* **to** *end-ip-address*] [**send-rate** { **ppm** *ppm* | *pps* }]

Views

Layer 3 Ethernet interface view

Layer 3 aggregate interface view

VLAN interface view

Predefined user roles

network-admin

Parameters

start-ip-address: Specifies the start IP address of the scanning range.

end-ip-address: Specifies the end IP address of the scanning range. The end IP address must be higher than or equal to the start IP address.

send-rate: Specifies the rate at which the device sends ARP requests for ARP scanning.

ppm *ppm*: Specifies the ARP packet sending rate, in packets per minute (ppm). The value range for the *ppm* argument is 10 to 600, and the value must be a multiple of 10.

ppm *pps*: Specifies the ARP packet sending rate, in packets per second (pps). The value range for the *pps* argument is 10 to 1000, and the value must be a multiple of 10.

Usage guidelines

ARP scanning automatically creates ARP entries for devices in the specified address range. IP addresses already in existing ARP entries are not scanned.

If the interface's primary and secondary IP addresses are in the address range, the sender IP address in the ARP request is the address on the smallest network segment.

If no address range is specified, the device learns ARP entries for devices on the subnet where the primary IP address of the interface resides. The sender IP address in the ARP requests is the primary IP address of the interface.

The start and end IP addresses must be on the same subnet as the primary IP address or secondary IP addresses of the interface.

ARP scanning will take some time. To stop an ongoing scan, press **Ctrl** + **C**. Dynamic ARP entries are created based on ARP replies received before the scan is terminated.

You can set the ARP packet sending rate if the scanning range has a large number of IP addresses. This setting can avoid high CPU usage and heavy network load caused by a burst of ARP traffic.

When you set the sending rate to a large value, the device might use a rate lower than the specified rate to ensure the device performance.

If you do not set the ARP packet sending rate, the device sends ARP requests to all IP addresses in the specified scanning range simultaneously.

Examples

Configure the device to scan the neighbors on the network where the primary IP address of VLAN-interface 2 resides.

```
<Switch> system-view
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] arp scan
```

Configure the device to scan neighbors in an address range.

```
<Switch> system-view
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] arp scan 1.1.1.1 to 1.1.1.20
```

Configure the device to scan neighbors in an address range on VLAN-interface 2 and set the ARP packet sending rate to 10 pps.

```
<Switch> system-view
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] arp scan 1.1.1.1 to 1.1.1.20 send-rate 10
```

MEMO:

arp scan command is supported from later software, including Version 7.2.23.

13.8. ARP gateway protection commands

13.8.1. arp filter source

Use **arp filter source** to enable ARP gateway protection for a gateway.

Use **undo arp filter source** to disable ARP gateway protection for a gateway.

Syntax

arp filter source *ip-address*

undo arp filter source *ip-address*

Default

ARP gateway protection is disabled.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the IP address of a protected gateway.

Usage guidelines

You can enable ARP gateway protection for a maximum of eight gateways on an interface.

You cannot configure both the **arp filter source** and **arp filter binding** commands on the same interface.

Examples

Enable ARP gateway protection for the gateway with IP address 1.1.1.1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] arp filter source 1.1.1.1
```

13.9. ARP filtering commands

13.9.1. arp filter binding

Use **arp filter binding** to enable ARP filtering and configure an ARP permitted entry.

Use **undo arp filter binding** to remove an ARP permitted entry.

Syntax

arp filter binding *ip-address mac-address*

undo arp filter binding *ip-address*

Default

ARP filtering is disabled.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

ip-address: Specifies a permitted sender IP address.

mac-address: Specifies a permitted sender MAC address.

Usage guidelines

If the sender IP and MAC addresses of an ARP packet match an ARP permitted entry, the ARP packet is permitted. If the sender IP and MAC addresses of an ARP packet do not match an ARP permitted entry, the ARP packet is discarded.

You can configure a maximum of eight ARP permitted entries on an interface.

You cannot configure both the **arp filter source** and **arp filter binding** commands on the same interface.

Examples

Enable ARP filtering and configure an ARP permitted entry.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] arp filter binding 1.1.1.1 0e10-0213-1023
```

Contents

A page of this section is **9-x-x**

14. IPv4 uRPF commands ····· 14-1
14.1. IPv4 uRPF commands ····· 14-1
14.1.1. display ip urpf ····· 14-1
14.1.2. ip urpf ····· 14-1

14. IPv4 uRPF commands

14.1. IPv4 uRPF commands

14.1.1. display ip urpf

Use **display ip urpf** to display uRPF configuration.

Syntax

display ip urpf [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays uRPF configuration for all member devices.

Examples

Display uRPF configuration for the specified slot.

```
<Switch> display ip urpf slot 1
Global uRPF configuration information(failed):
   Check type: strict
   Allow default route
```

Table 14-1 Command output

Field	Description
(failed)	The system failed to deliver the uRPF configuration to the forwarding chip because of insufficient chip resources. This field is not displayed if the delivery is successful.
Check type	uRPF check mode: loose or strict.
Allow default route	Using the default route is allowed.

14.1.2. ip urpf

Use **ip urpf** to enable uRPF.

Use **undo ip urpf** to disable uRPF.

Syntax

ip urpf { **loose** | **strict** }

undo ip urpf

Default

uRPF is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

loose: Enables loose uRPF check. To pass loose uRPF check, the source address of a packet must match the destination address of a FIB entry.

strict: Enables strict uRPF check. To pass strict uRPF check, the source address and receiving interface of a packet must match the destination address and output interface of a FIB entry.

Usage guidelines

uRPF can be deployed on a PE connected to a CE or an ISP, or on a CE.

Examples

Enable strict uRPF check globally.

```
<Switch> system-view
[Switch] ip urpf strict
```

Related commands

display ip urpf

QX-S5600G Series Ethernet Switches

Command References

10.High Availability

This manual is including the following chapters.

01-Ethernet OAM commands

02-CFD commands

03-DLDP commands

04-RRPP commands

05-Smart Link commands

06-Monitor Link commands

07-VRRP commands

08-BFD commands

09-Track commands

Contents

A page of this section is **10-x-x**

1. Ethernet OAM commands ····· 1-1
1.1. Ethernet OAM commands ····· 1-1
1.1.1. display oam ····· 1-1
1.1.2. display oam configuration ····· 1-5
1.1.3. display oam critical-event ····· 1-7
1.1.4. display oam link-event ····· 1-7
1.1.5. oam enable ····· 1-10
1.1.6. oam errored-frame threshold ····· 1-11
1.1.7. oam errored-frame window ····· 1-12
1.1.8. oam errored-frame-period threshold ····· 1-13
1.1.9. oam errored-frame-period window ····· 1-13
1.1.10. oam errored-frame-seconds threshold ····· 1-14
1.1.11. oam errored-frame-seconds window ····· 1-15
1.1.12. oam errored-symbol-period threshold ····· 1-16
1.1.13. oam errored-symbol-period window ····· 1-17
1.1.14. oam global errored-frame threshold ····· 1-17
1.1.15. oam global errored-frame window ····· 1-18
1.1.16. oam global errored-frame-period threshold ····· 1-19
1.1.17. oam global errored-frame-period window ····· 1-20
1.1.18. oam global errored-frame-seconds threshold ····· 1-20
1.1.19. oam global errored-frame-seconds window ····· 1-21
1.1.20. oam global errored-symbol-period threshold ····· 1-22
1.1.21. oam global errored-symbol-period window ····· 1-23
1.1.22. oam global timer hello ····· 1-23
1.1.23. oam global timer keepalive ····· 1-24
1.1.24. oam mode ····· 1-25
1.1.25. oam remote-failure action ····· 1-26
1.1.26. oam remote-loopback ····· 1-26
1.1.27. oam remote-loopback interface ····· 1-27
1.1.28. oam remote-loopback reject-request ····· 1-28
1.1.29. oam timer hello ····· 1-29
1.1.30. oam timer keepalive ····· 1-30
1.1.31. reset oam ····· 1-30

1. Ethernet OAM commands

1.1. Ethernet OAM commands

1.1.1. display oam

Use **display oam** to display Ethernet OAM connection information.

Syntax

display oam { **local** | **remote** } [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

local: Specifies the local end.

remote: Specifies the remote end.

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, the command displays Ethernet OAM connection information for all interfaces.

Examples

Display Ethernet OAM connection information for all local interfaces.

```
<Switch> display oam local
----------- [GigabitEthernet1/0/1] -----------
 Enable status      : Enable
 Loopback status    : No loopback
 Link status        : UP
 OAM mode           : Active
 PDU                : ANY
 Mux action         : FWD
 Par action         : FWD
```

Display Ethernet OAM connection information for the local interface GigabitEthernet 1/0/1.

```
<Switch> display oam local interface gigabitethernet 1/0/1
 Enable status      : Enable
 Loopback status    : No loopback
 Link status        : UP
 OAM mode           : Active
 PDU                : ANY
 Mux action         : FWD
 Par action         : FWD
 Flags
```

```
  Link fault        : Not occurred
  Dying gasp        : Not occurred
  Critical event    : Not occurred
  Local evaluating  : COMPLETE
  Remote evaluating : COMPLETE
Packets statistics
  Packet type                        Sent                    Received
  ------------------------------------------------------------------
  OAMPDU                              100                      80
  OAMInformation                     64                       60
  OAMEventNotification              36                       20
  OAMUniqueEventNotification      36                       10
  OAMDuplicateEventNotification   0                        10
```

Table 1-1 Command output

Field	Description
GigabitEthernet1/0/1	Information on GigabitEthernet 1/0/1.
Enable status	Ethernet OAM state: • **Enable**. • **Disable**.
Loopback status	Ethernet OAM loopback state: • **No loopback**—Remote loopback is disabled. • **Remote loopback**—Controlling end of remote loopback. • **Local loopback**—Controlled end of remote loopback.
Link status	Link physical state: • **UP** • **DOWN**.
OAM mode	Local Ethernet OAM mode: • **Active**—The interface operates in active Ethernet OAM mode. • **Passive**—The interface operates in passive Ethernet OAM mode.
PDU	The way in which the local end processes Ethernet OAMPDUs: • **RX_INFO**—The interface receives only Information OAMPDUs and does not send any Ethernet OAMPDUs. • **LF_INFO**—The interface sends only Information OAMPDUs without Information TLV triplets and with their link error flag bits being set. • **INFO**—The interface sends and receives only Information OAMPDUs. • **ANY**—The interface sends and receives Ethernet OAMPDUs of any type.
Mux action	Operating mode of the local transmitter: • **FWD**—The interface can send any packets. • **DISCARD**—The interface only sends Ethernet OAMPDUs.

Field	Description
Par action	Operating mode of the local receiver: • **FWD**—The interface can receive any packets. • **DISCARD**—The interface only receives Ethernet OAMPDUs. • **LB**—The local receiver is in loopback state. All the packets, other than Ethernet OAMPDUs, received on the local receiver are returned to their sources along their original routes.
Flags	Local flags inserted in the local flag fields of the sent Ethernet OAMPDUs.
Link fault	Indicates whether an Ethernet OAM link error is present.
Dying gasp	Indicates whether a fatal error is present.
Critical event	Indicates whether a critical error is present.
Local evaluating	Indicates whether the local-to-remote configuration negotiation is complete: • **COMPLETE**—The negotiation is completed. • **NOTCOMPLETE**—The negotiation is uncompleted.
Remote evaluating	Indicates whether the remote-to-local configuration negotiation is complete: • **COMPLETE**—The negotiation is completed. • **NOTCOMPLETE**—The negotiation is uncompleted. • **RESERVED**—The field is reserved and the negotiation is uncompleted. • **UNSATISFIED**—The remote end is not satisfied with the local configuration and the negotiation is uncompleted.
Packets statistics	Statistics about Ethernet OAMPDUs.
OAMPDU	Total number of sent or received Ethernet OAMPDUs.
OAMInformation	Number of sent or received Information OAMPDUs.
OAMEventNotification	Number of sent or received Event notification OAMPDUs.
OAMUniqueEventNotification	Number of unduplicated sent or received Event notification OAMPDUs.
OAMDuplicateEventNotification	Number of duplicate sent or received Event notification OAMPDUs.

Display Ethernet OAM connection information for all remote interfaces.

```
<Switch> display oam remote
---------- [GigabitEthernet1/0/1] ----------
 OAM mode           : Active
 MAC address        : 3822-d6a2-a800
 MTU size           : 1500
 Mux action         : FWD
 Par action         : FWD
```

Display Ethernet OAM connection information for the peer interface GigabitEthernet 1/0/1.

```
<Switch> display oam remote interface gigabitethernet 1/0/1
 OAM mode           : Active
```

```
MAC address       : 3822-d6a2-a800
MTU size          : 1500
Mux action        : FWD
Par action        : FWD
Configuration
  Unidirectional    : Not supported
  Remote loopback   : Supported
  Link events       : Supported
  MIB retrieval     : Not supported
Flags
  Link fault        : Not occurred
  Dying gasp        : Not occurred
  Critical event    : Not occurred
  Local evaluating  : COMPLETE
  Remote evaluating : COMPLETE
```

Table 1-2 Command output

Field	Description
GigabitEthernet1/0/1	Information on GigabitEthernet 1/0/1.
OAM mode	Ethernet OAM mode on the remote end: • **Active**—The interface operates in active Ethernet OAM mode. • **Passive**—The interface operates in passive Ethernet OAM mode.
MAC address	MAC address of the remote end.
MTU size	MTU size, in bytes.
Mux action	Operating mode of the remote transmitter: • **FWD**—The interface can send any packets. • **DISCARD**—The interface only sends Ethernet OAMPDUs.
Par action	Operating mode of the remote receiver: • **FWD**—The interface can receive any packets. • **DISCARD**—The interface only receives Ethernet OAMPDUs. • **LB**—The local receiver is in loopback state. All the packets, other than Ethernet OAMPDUs, received on the local receiver are returned to their sources along their original routes.
Configuration	Configuration of the remote Ethernet OAM entity.
Unidirectional	Indicates whether unidirectional transmission is supported.
Remote loopback	Indicates whether Ethernet OAM remote loopback is supported.
Link events	Indicates whether Ethernet OAM link error events are supported.
MIB retrieval	Indicates whether MIB variable retrieval is supported.
Flags	Values of the peer Ethernet OAM flag fields in OAM packets.
Link fault	Indicates whether an Ethernet OAM link error is present.

Field	Description
Dying gasp	Indicates whether a fatal error is present.
Critical event	Indicates whether a critical error is present.
Local evaluating	Indicates whether the local-to-remote configuration negotiation is complete: • **COMPLETE**—The negotiation is completed. • **NOTCOMPLETE**—The negotiation is uncompleted. • **RESERVED**—The field is reserved and the negotiation is uncompleted. • **UNSATISFIED**—The remote end is not satisfied with the local configuration and the negotiation is uncompleted.
Remote evaluating	Indicates whether the remote-to-local configuration negotiation is complete: • **COMPLETE**—The negotiation is completed. • **NOTCOMPLETE**—The negotiation is uncompleted. • **UNSATISFIED**—The remote end is not satisfied with the local configuration and the negotiation is uncompleted.

Related commands

reset oam

1.1.2. display oam configuration

Use **display oam configuration** to display Ethernet OAM configuration information.

Syntax

display oam configuration [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, the command displays Ethernet OAM configuration globally and for interfaces that do not use the default configuration.

Examples

Display Ethernet OAM configuration globally and for interfaces that do not use the default configuration.

```
<Switch> display oam configuration
---------------- [Global] ----------------
 OAM timers
   Hello timer         : 1000 milliseconds
   Keepalive timer     : 5000 milliseconds
 Link monitoring
   Errored symbol period
```

```
    Window           : 100 x 1000000 symbols
    Threshold        : 1 error symbols
  Errored frame
    Window           : 10 x 100 milliseconds
    Threshold        : 1 error frames
  Errored frame period
    Window           : 1000 x 10000 frames
    Threshold        : 1 error frames
  Errored frame seconds
    Window           : 600 x 100 milliseconds
    Threshold        : 1 error seconds

----------- [GigabitEthernet1/0/1] -----------
 OAM timers
   Hello timer       : 500 milliseconds
   Keepalive timer   : 5000 milliseconds
 Link monitoring
   Errored symbol period
     Window          : 100 x 1000000 symbols
     Threshold       : 1 error symbols
   Errored frame
     Window          : 10 x 100 milliseconds
     Threshold       : 1 error frames
   Errored frame period
     Window          : 1000 x 10000 frames
     Threshold       : 1 error frames
   Errored frame seconds
     Window          : 600 x 100 milliseconds
     Threshold       : 1 error seconds
```

Table 1-3 Command output

Field	Description
Global	Global information.
GigabitEthernet1/0/1	Information on GigabitEthernet 1/0/1.
OAM timers	Ethernet OAM connection detection timers.
Hello timer	Ethernet OAM handshake packet transmission interval.
Keepalive timer	Ethernet OAM connection timeout timer.
Link monitoring	Link event detection window and threshold.
Errored symbol period	Errored symbol event.
Errored frame	Errored frame event.
Errored frame period	Errored frame period event.
Errored frame seconds	Errored frame seconds event.
Window	Detection window configured for link events.
Threshold	Triggering threshold configured for link events.

1.1.3. display oam critical-event

Use **display oam critical-event** to display statistics for critical Ethernet OAM link events.

Syntax

display oam critical-event [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, the command displays statistics for the critical Ethernet OAM link events for all interfaces.

Examples

Display statistics for critical Ethernet OAM link events on all interfaces.

```
<Switch> display oam critical-event
---------- [GigabitEthernet1/0/1] ----------
 Local link status   : UP
 Event statistics
   Link fault        : Not occurred
   Dying gasp        : Not occurred
   Critical event    : Not occurred
```

Table 1-4 Command output

Field	Description
GigabitEthernet1/0/1	Information on GigabitEthernet 1/0/1.
Local link status	Local link status, up or down.
Event statistics	Statistics for critical Ethernet OAM link events.
Link fault	Indicates whether a link fault is present.
Dying Gasp	Indicates whether a fatal fault is present.
Critical Event	Indicates whether a critical fault is present.

1.1.4. display oam link-event

Use **display oam link-event** to display statistics for Ethernet OAM link error events for local or peer interfaces.

Syntax

display oam link-event { **local** | **remote** } [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

local: Specifies the local end.

remote: Specifies the peer end.

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, the command displays statistics for Ethernet OAM link error events for all local or peer interfaces.

Usage guidelines

Ethernet OAM link error events include errored symbol events, errored frame events, errored frame period events, and errored frame seconds events.

Examples

Display statistics for Ethernet OAM link error events for all local interfaces.

```
<Switch> display oam link-event local
----------- [GigabitEthernet1/0/1] -----------
 Link status: UP
 OAM local errored symbol event
   Event time stamp         : 35498 x 100 milliseconds
   Errored symbol window    : 100000000 symbols
   Errored symbol threshold : 1 error symbols
   Errored symbol           : 1 error symbols
   Error running total      : 4 error symbols
   Event running total      : 4 events
 OAM local errored frame event
   Event time stamp        : 49582 x 100 milliseconds
   Errored frame window    : 10 x 100 milliseconds
   Errored frame threshold : 1 error frames
   Errored frame           : 1 error frames
   Error running total     : 6 error frames
   Event running total     : 6 events
 OAM local errored frame period event
   Event time stamp                : 16382 x 100 milliseconds
   Errored frame period window     : 10000000 frames
   Errored frame period threshold  : 1 error frames
   Errored frame period            : 1 error frames
   Error running total             : 5 error frames
   Event running total             : 5 events
 OAM local errored frame seconds summary event
   Event time stamp                : 50022 x 100 milliseconds
   Errored frame seconds window    : 600 x 100 milliseconds
   Errored frame seconds threshold : 1 error seconds
   Errored frame seconds           : 1 error seconds
```

```
  Error running total             : 1 error seconds
  Event running total             : 1 events
```

Display statistics for Ethernet OAM link error events for all peer interfaces.

```
<Switch> display oam link-event remote
---------- [GigabitEthernet1/0/1] ----------
 Link status: UP
 OAM remote errored symbol event
   Event time stamp         : 35498 x 100 milliseconds
   Errored symbol window    : 100000000  symbols
   Errored symbol threshold : 1 error symbols
   Errored symbol           : 1 error symbols
   Error running total      : 4 error symbols
   Event running total      : 4 events
 OAM remote errored frame event
   Event time stamp         : 49582 x 100 milliseconds
   Errored frame window     : 10 x 100 milliseconds
   Errored frame threshold  : 1 error frames
   Errored frame            : 1 error frames
   Error running total      : 6 error frames
   Event running total      : 6 events
 OAM remote errored frame period event
   Event time stamp                 : 16382 x 100 milliseconds
   Errored frame period window      : 10000000 frames
   Errored frame period threshold   : 1 error frames
   Errored frame period             : 1 error frames
   Error running total              : 5 error frames
   Event running total              : 5 events
 OAM remote errored frame seconds summary event
   Event time stamp                 : 50022 x 100 milliseconds
   Errored frame seconds window     : 600 x 100 milliseconds
   Errored frame seconds threshold  : 1 error seconds
   Errored frame seconds            : 1 error seconds
   Error running total              : 1 error seconds
   Event running total              : 1 events
```

Table 1-5 Command output

Field	Description
GigabitEthernet1/0/1	Information on GigabitEthernet 1/0/1.
Link status	Link status, up or down.
OAM local/remote errored symbol event	Information about local/remote errored symbol events (available only when remote errored symbol events occur): • **Event time stamp**—Time when an errored symbol event occurred. • **Errored symbol window**—Errored symbol detection interval. • **Errored symbol threshold**—Errored threshold that triggers an errored symbol event. • **Errored symbol**—Number of detected errored symbols in the

Field	Description
	most recent errored symbol event. • **Error running total**—Total number of errored symbols. • **Event running total**—Total number of errored symbol events that have occurred.
OAM local/remote errored frame event	Information about local/remote end errored frame events (available only when local/remote end errored frame events occur): • **Event time stamp**—Time when an errored frame event occurred. • **Errored frame window**—Errored frame detection interval. • **Errored frame threshold**—Errored threshold that triggers an errored frame event. • **Errored frame**—Number of detected errored frames in the most recent errored frame event. • **Error running total**—Total number of errored frames. • **Event running total**—Total number of errored frame events that have occurred.
OAM local/remote errored frame period event	Information about local or remote errored frame period events (available only when local/remote errored frame period events occur): • **Event time stamp**—Time when an errored frame period event occurred. • **Errored frame period window**—Errored frame period detection interval. • **Errored frame period threshold**—Errored threshold that triggers an errored frame period event. • **Errored frame period**—Number of detected errored frames in the most recent errored frame period event. • **Error running total**—Total number of errored frames that have detected. • **Event running total**—Total number of errored frame period events.
OAM local/remote errored frame seconds summary event	Information about local/remote end errored frame seconds events (available only when local/remote end errored frame seconds events occur): • **Event time stamp**—Time when an errored frame seconds event occurred. • **Errored frame second window**—Errored frame second detection interval. • **Errored Frame seconds threshold**—Errored threshold that triggers an errored frame seconds event. • **Errored frame seconds**—Number of detected errored frame seconds in the most recent errored frame seconds event. • **Error running total**—Total number of errored frame seconds. • **Event running total**—Total number of errored frame seconds events that have occurred.

Related commands

`reset oam`

1.1.5. oam enable

Use **`oam enable`** to enable Ethernet OAM.

Use **undo oam enable** to disable Ethernet OAM.

Syntax

oam enable

undo oam enable

Default

Ethernet OAM is disabled.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Predefined user roles

network-admin

Examples

Enable OAM on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] oam enable
```

1.1.6. oam errored-frame threshold

Use **oam errored-frame threshold** to set the errored frame event triggering threshold for an interface.

Use **undo oam errored-frame threshold** to restore the default.

Syntax

oam errored-frame threshold *threshold-value*

undo oam errored-frame threshold

Default

An interface uses the global setting.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Predefined user roles

network-admin

Parameters

threshold-value: Specifies the errored frame event triggering threshold in number of errored frame events, in the range of 0 to 4294967295.

Usage guidelines

The configuration in interface view takes effect only on the specified interface. For an interface, the configuration in interface view takes precedence.

Examples

Set the errored frame event triggering threshold to 100 on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] oam errored-frame threshold 100
```

Related commands

display oam configuration

display oam link-event

oam global errored-frame threshold

1.1.7. oam errored-frame window

Use **oam errored-frame window** to set the errored frame event detection window.

Use **undo oam errored-frame window** to restore the default.

Syntax

oam errored-frame window *window-value*

undo oam errored-frame window

Default

An interface uses the global setting.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Predefined user roles

network-admin

Parameters

window-value: Specifies the errored frame event detection window in the range of 10 to 600, in steps of 10, in 100 milliseconds.

Usage guidelines

The configuration in interface view takes effect only on the specified interface. For an interface, the configuration in interface view takes precedence.

Examples

Set the errored frame event detection window to 2000 milliseconds on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] oam errored-frame window 20
```

Related commands

display oam configuration

display oam link-event

oam global errored-frame window

1.1.8. oam errored-frame-period threshold

Use **oam errored-frame-period threshold** to set the errored frame period event triggering threshold on an interface.

Use **undo oam errored-frame-period threshold** to restore the default.

Syntax

oam errored-frame-period threshold *threshold-value*

undo oam errored-frame-period threshold

Default

An interface uses the global setting.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Predefined user roles

network-admin

Parameters

threshold-value: Specifies the errored frame period event triggering threshold in the range of 0 to 4294967295.

Usage guidelines

The configuration in interface view takes effect only on the specified interface. For an interface, the configuration in interface view takes precedence.

Examples

Set the errored frame period event triggering threshold to 100 on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] oam errored-frame-period threshold 100
```

Related commands

display oam configuration

display oam link-event

oam global errored-frame-period threshold

1.1.9. oam errored-frame-period window

Use **oam errored-frame-period window** to set the errored frame period event detection window.

Use **undo oam errored-frame-period window** to restore the default.

Syntax

oam errored-frame-period window *window-value*

undo oam errored-frame-period window

Default

An interface uses the global setting.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Predefined user roles

network-admin

Parameters

window-value: Specifies the errored frame period event detection window in the range of 1 to 65535. The value of this argument must be a multiple of 10000.

Usage guidelines

The configuration in interface view takes effect only on the specified interface. For an interface, the configuration in interface view takes precedence.

Examples

Set the errored frame period event detection window to 20000000 on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] oam errored-frame-period window 2000
```

Related commands

display oam configuration

display oam link-event

oam global errored-frame-period window

1.1.10. oam errored-frame-seconds threshold

Use **oam errored-frame-seconds threshold** to set the errored frame seconds event triggering threshold on an interface.

Use **undo oam errored-frame-seconds threshold** to restore the default.

Syntax

oam errored-frame-seconds threshold *threshold-value*

undo oam errored-frame-seconds threshold

Default

An interface uses the global setting.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Predefined user roles

network-admin

Parameters

threshold-value: Specifies the errored frame seconds event triggering threshold in the range of 0 to 900.

Usage guidelines

The value of the errored frame seconds event triggering threshold cannot be greater than the value of the errored frame seconds event detection window (in seconds). Otherwise, errored frame seconds events cannot be generated.

The configuration in interface view takes effect only on the specified interface. For an interface, the configuration in interface view takes precedence.

Examples

Set the errored frame seconds event triggering threshold to 100 on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] oam errored-frame-seconds threshold 100
```

Related commands

display oam configuration

display oam link-event

oam errored-frame-seconds window

oam global errored-frame-seconds threshold

1.1.11. oam errored-frame-seconds window

Use **oam errored-frame-seconds window** to set the errored frame seconds event detection window.

Use **undo oam errored-frame-seconds window** to restore the default.

Syntax

oam errored-frame-seconds window *window-value*

undo oam errored-frame-seconds window

Default

An interface uses the global setting.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Predefined user roles

network-admin

Parameters

window-value: Specifies the errored frame seconds event detection window in the range of 100 to 9000, in steps of 10, in 100 milliseconds.

Usage guidelines

The value of the errored frame seconds event triggering threshold cannot be greater than the value of the errored frame seconds event detection window (in seconds). Otherwise, errored frame seconds events cannot be generated.

The configuration in interface view takes effect only on the specified interface. For an interface, the configuration in interface view takes precedence.

Examples

Set the errored frame seconds event detection window to 10000 milliseconds on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] oam errored-frame-seconds window 100
```

Related commands

display oam configuration

display oam link-event

oam errored-frame-seconds threshold

oam errored-frame-seconds period

1.1.12. oam errored-symbol-period threshold

Use **oam errored-symbol-period threshold** to set the errored symbol event triggering threshold.

Use **undo oam errored-symbol-period threshold** to restore the default.

Syntax

oam errored-symbol-period threshold *threshold-value*

undo oam errored-symbol-period threshold

Default

An interface uses the global setting.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Predefined user roles

network-admin

Parameters

threshold-value: Specifies the errored symbol event triggering threshold in the range of 0 to 4294967295.

Usage guidelines

The configuration in interface view takes effect only on the specified interface. For an interface, the configuration in interface view takes precedence.

Examples

Set the errored symbol event triggering threshold to 100 on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] oam errored-symbol-period threshold 100
```

Related commands

display oam configuration

display oam link-event

oam global errored-symbol-period threshold

1.1.13. oam errored-symbol-period window

Use **oam errored-symbol-period window** to set the errored symbol event detection window.

Use **undo oam errored-symbol-period window** to restore the default.

Syntax

oam errored-symbol-period window *window-value*

undo oam errored-symbol-period window

Default

An interface uses the global setting.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Predefined user roles

network-admin

Parameters

window-value: Specifies the errored symbol event detection window in the range of 1 to 65535. The value of this argument must be a multiple of 1000000.

Usage guidelines

The configuration in interface view takes effect only on the specified interface. For an interface, the configuration in interface view takes precedence.

Examples

Set the errored symbol event detection window to 200000000 on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] oam errored-symbol-period window 200
```

Related commands

display oam configuration

display oam link-event

oam global errored-symbol-period window

1.1.14. oam global errored-frame threshold

Use **oam global errored-frame threshold** to set the global errored frame event triggering threshold.

Use **undo oam global errored-frame threshold** to restore the default.

Syntax

oam global errored-frame threshold *threshold-value*

undo oam global errored-frame threshold

Default

The errored frame event triggering threshold is 1.

Views

System view

Predefined user roles

network-admin

Parameters

threshold-value: Specifies the errored frame event triggering threshold in the range of 0 to 4294967295.

Usage guidelines

The configuration in system view takes effect on all interfaces, but has a lower precedence than the configuration in interface view.

Examples

Set the errored frame event triggering threshold to 100.

```
<Switch> system-view
[Switch] oam global errored-frame threshold 100
```

Related commands

display oam configuration

display oam link-event

oam errored-frame threshold

1.1.15. oam global errored-frame window

Use **oam global errored-frame window** to set the global errored frame event detection window.

Use **undo oam global errored-frame window** to restore the default.

Syntax

oam global errored-frame window *window-value*

undo oam global errored-frame window

Default

The global errored frame event detection window is 1000 milliseconds.

Views

System view

Predefined user roles

network-admin

Parameters

window-value: Specifies the errored frame event detection window in the range of 10 to 600, in steps of 10, in 100 milliseconds.

Usage guidelines

The configuration in system view takes effect on all interfaces, but has a lower precedence than the configuration in interface view.

Examples

Set the errored frame event detection window to 2000 milliseconds.

```
<Switch> system-view
[Switch] oam global errored-frame window 20
```

Related commands

display oam configuration

display oam link-event

oam errored-frame window

1.1.16. oam global errored-frame-period threshold

Use **oam global errored-frame-period threshold** to set the global errored frame period event triggering threshold.

Use **undo oam global errored-frame-period threshold** to restore the default.

Syntax

oam global errored-frame-period threshold *threshold-value*

undo oam global errored-frame-period threshold

Default

The errored frame period event triggering threshold is 1.

Views

System view

Predefined user roles

network-admin

Parameters

threshold-value: Specifies the errored frame period event triggering threshold in the range of 0 to 4294967295.

Usage guidelines

The configuration in system view takes effect on all interfaces, but has a lower precedence than the configuration in interface view.

Examples

Set the errored frame period event triggering threshold to 100.

```
<Switch> system-view
[Switch] oam global errored-frame-period threshold 100
```

Related commands

display oam configuration

display oam link-event

oam errored-frame-period threshold

1.1.17. oam global errored-frame-period window

Use **oam global errored-frame-period window** to set the global errored frame period event detection window.

Use **undo oam global errored-frame-period window** to restore the default.

Syntax

oam global errored-frame-period window *window-value*

undo oam global errored-frame-period window

Default

The global errored frame period event detection window is 10000000.

Views

System view

Predefined user roles

network-admin

Parameters

window-value: Specifies the errored frame period event detection window in the range of 1 to 65535. The value of this argument must be a multiple of 10000.

Usage guidelines

The configuration in system view takes effect on all interfaces, but has a lower precedence than the configuration in interface view.

Examples

Set the errored frame period event detection window to 20000000.

```
<Switch> system-view
[Switch] oam global errored-frame-period window 2000
```

Related commands

display oam configuration

display oam link-event

oam errored-frame-period window

1.1.18. oam global errored-frame-seconds threshold

Use **oam global errored-frame-seconds threshold** to set the global errored frame seconds event triggering threshold.

Use **undo oam global errored-frame-seconds threshold** to restore the default.

Syntax

oam global errored-frame-seconds threshold *threshold-value*

undo oam global errored-frame-seconds threshold

Default

The global errored frame seconds event detection interval is 1.

Views

System view

Predefined user roles

network-admin

Parameters

threshold-value: Specifies the errored frame seconds event triggering threshold in the range of 0 to 900.

Usage guidelines

The value of the errored frame seconds event triggering threshold cannot be greater than the value of the errored frame seconds event detection window (in seconds). Otherwise, errored frame seconds events cannot be generated.

The configuration in system view takes effect on all interfaces, but has a lower precedence than the configuration in interface view.

Examples

Set the errored frame seconds event triggering threshold to 100.

```
<Switch> system-view
[Switch] oam global errored-frame-seconds threshold 100
```

Related commands

display oam configuration

display oam link-event

oam errored-frame-seconds threshold

oam global errored-frame-seconds window

1.1.19. oam global errored-frame-seconds window

Use **oam global errored-frame-seconds window** to set the global errored frame seconds event detection window.

Use **undo oam global errored-frame-seconds window** to restore the default.

Syntax

oam global errored-frame-seconds window *window-value*

undo oam global errored-frame-seconds window

Default

The global errored frame seconds event detection window is 60000 milliseconds.

Views

System view

Predefined user roles

network-admin

Parameters

window-value: Specifies the errored frame seconds event detection window in the range of 100 to 9000, in steps of 10, in 100 milliseconds.

Usage guidelines

The value of the errored frame seconds event triggering threshold cannot be greater than the value of the errored frame seconds event detection window (in seconds). Otherwise, errored frame seconds events cannot be generated.

The configuration in system view takes effect on all interfaces, but has a lower precedence than the configuration in interface view.

Examples

Set the errored frame seconds event detection window to 10000 milliseconds.

```
<Switch> system-view
[Switch] oam global errored-frame-seconds window 100
```

Related commands

display oam configuration

display oam link-event

oam errored-frame-seconds period

oam global errored-frame-seconds threshold

1.1.20. oam global errored-symbol-period threshold

Use **oam global errored-symbol-period threshold** to set the global errored symbol event triggering threshold.

Use **undo oam global errored-symbol-period threshold** to restore the default.

Syntax

oam global errored-symbol-period threshold *threshold-value*

undo oam global errored-symbol-period threshold

Default

The global errored symbol event triggering threshold is 1.

Views

System view

Predefined user roles

network-admin

Parameters

threshold-value: Specifies the errored symbol event triggering threshold in the range of 0 to 4294967295.

Usage guidelines

The configuration in system view takes effect on all interfaces, but has a lower precedence than the configuration in interface view.

Examples

Set the errored symbol event triggering threshold to 100.

```
<Switch> system-view
[Switch] oam global errored-symbol-period threshold 100
```

Related commands

display oam configuration

display oam link-event

oam errored-symbol-period threshold

1.1.21. oam global errored-symbol-period window

Use **oam global errored-symbol-period window** to set the global errored symbol event detection window.

Use **undo oam global errored-symbol-period window** to restore the default.

Syntax

oam global errored-symbol-period window *window-value*

undo oam global errored-symbol-period window

Default

The global errored symbol event detection window is 100000000.

Views

System view

Predefined user roles

network-admin

Parameters

window-value: Specifies the errored symbol event detection window in the range of 1 to 65535. The value of this argument must be a multiple of 1000000.

Usage guidelines

The configuration in system view takes effect on all interfaces, but has a lower precedence than the configuration in interface view.

Examples

Set the errored symbol event detection window to 200000000.

```
<Switch> system-view
[Switch] oam global errored-symbol-period window 200
```

Related commands

display oam configuration

display oam link-event

oam global errored-symbol-period window

1.1.22. oam global timer hello

Use **oam global timer hello** to configure the global Ethernet OAM handshake packet transmission interval.

Use **undo oam global timer hello** to restore the default.

Syntax

oam global timer hello *interval*

undo oam global timer hello

Default

The global Ethernet OAM handshake packet transmission interval is 1000 milliseconds.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the Ethernet OAM handshake packet transmission interval, in steps of 100, in milliseconds. The value range for the *interval* argument is 500 to 5000.

Usage guidelines

After the timeout timer of an Ethernet OAM connection expires, the local OAM entity ages out and terminates its connection with the peer OAM entity. To keep the Ethernet OAM connections stable, set the connection timeout timer to be a minimum of five times the handshake packet transmission interval.

The configuration in system view takes effect on all interfaces, but has a lower precedence than the configuration in interface view.

Examples

Set the Ethernet OAM handshake packet transmission interval to 600 milliseconds.

```
<Switch> system-view
[Switch] oam global timer hello 600
```

Related commands

display oam configuration

oam timer hello

1.1.23. oam global timer keepalive

Use **oam global timer keepalive** to configure the global Ethernet OAM connection timeout timer.

Use **undo oam global timer keepalive** to restore the default.

Syntax

oam global timer keepalive *interval*

undo oam global timer keepalive

Default

The global Ethernet OAM connection timeout timer is 5000 milliseconds.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the Ethernet OAM connection timeout timer, in steps of 100, in milliseconds. The value range for the *interval* argument is 1000 to 25000.

Usage guidelines

After the timeout timer of an Ethernet OAM connection expires, the local OAM entity ages out and terminates its connection with the peer OAM entity. To keep the Ethernet OAM connections stable, set the connection timeout timer to be a minimum of five times the handshake packet transmission interval.

The configuration in system view takes effect on all interfaces, but has a lower precedence than the configuration in interface view.

Examples

Set the Ethernet OAM connection timeout timer to 6000 milliseconds.

```
<Switch> system-view
[Switch] oam global timer keepalive 6000
```

Related commands

display oam configuration

oam timer keepalive

1.1.24. oam mode

Use **oam mode** to set the Ethernet OAM mode.

Use **undo oam mode** to restore the default.

Syntax

oam mode { **active** | **passive** }

undo oam mode

Default

An Ethernet OAM-enabled Ethernet interface operates in active Ethernet OAM mode.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Predefined user roles

network-admin

Parameters

active: Specifies the active Ethernet OAM mode.

passive: Specifies the passive Ethernet OAM mode.

Usage guidelines

To change the Ethernet OAM mode of an Ethernet OAM-enabled Ethernet interface, first disable Ethernet OAM on the interface.

Examples

Disable Ethernet OAM on GigabitEthernet 1/0/1, and then configure GigabitEthernet 1/0/1 to operate in passive Ethernet OAM mode.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] undo oam enable
[Switch-GigabitEthernet1/0/1] oam mode passive
```

Related commands

oam enable

1.1.25. oam remote-failure action

Use **oam remote-failure action** to configure the action an interface takes after it receives an Ethernet OAM event from the remote end.

Use **undo oam remote-failure action** to remove the configuration.

Syntax

oam remote-failure { **connection-expired** | **critical-event** | **dying-gasp** | **link-fault** } **action error-link-down**

undo oam remote-failure { **connection-expired** | **critical-event** | **dying-gasp** | **link-fault** } **action error-link-down**

Default

An interface only logs the Ethernet OAM event it receives from the remote end.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Predefined user roles

network-admin

Parameters

connection-expired: Specifies a connection timeout event.

critical-event: Specifies a critical event.

dying-gasp: Specifies a fatal event.

link-fault: Specifies a link fault event.

error-link-down: Terminates the OAM connection, and sets the link state of the interface to down.

Examples

Configure GigabitEthernet 1/0/1 to terminate the OAM connection after it receives a critical event from the remote end, and set the link state of the interface to down.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] oam remote-failure critical-event action error-link-down
```

1.1.26. oam remote-loopback

Use **oam remote-loopback start** to enable Ethernet OAM remote loopback on an interface.

Use **oam remote-loopback stop** to disable Ethernet OAM remote loopback on an interface.

Syntax

oam remote-loopback start

oam remote-loopback stop

Default

Ethernet OAM remote loopback is disabled on an interface.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

Ethernet OAM remote loopback is available only after the Ethernet OAM connection is established. It can be performed only by the Ethernet OAM entities operating in active Ethernet OAM mode.

You can enable Ethernet OAM remote loopback on a specified interface in user view or system view. You can also enable it on the current interface in interface view. The configurations have the same effect.

Examples

Configure active Ethernet OAM mode and enable Ethernet OAM on GigabitEthernet 1/0/1. Enable Ethernet OAM remote loopback on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] oam mode active
[Switch-GigabitEthernet1/0/1] oam enable
[Switch-GigabitEthernet1/0/1] oam remote-loopback start
```

Related commands

oam enable

oam mode

oam remote-loopback interface

1.1.27. oam remote-loopback interface

Use **oam remote-loopback start interface** to enable Ethernet OAM remote loopback on an interface.

Use **oam remote-loopback stop interface** to disable Ethernet OAM remote loopback on an interface.

Syntax

oam remote-loopback start interface *interface-type interface-number*

oam remote-loopback stop interface *interface-type interface-number*

Default

Ethernet OAM remote loopback is disabled on an interface.

Views

User view

System view

Predefined user roles

network-admin

Parameters

interface-type interface-number: Specifies an interface by its type and number.

Usage guidelines

Ethernet OAM remote loopback is available only after the Ethernet OAM connection is established. It can be performed only by the Ethernet OAM entities operating in active Ethernet OAM mode.

You can enable Ethernet OAM remote loopback on a specified interface in user view or system view. You can also enable it on the current interface in interface view. The configurations have the same effect.

Examples

Configure the active Ethernet OAM mode and enable Ethernet OAM on GigabitEthernet 1/0/1. Enable Ethernet OAM remote loopback on GigabitEthernet 1/0/1 in system view.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] oam mode active
[Switch-GigabitEthernet1/0/1] oam enable
[Switch-GigabitEthernet1/0/1] quit
[Switch] oam remote-loopback start interface gigabitethernet 1/0/1
```

Related commands

oam enable

oam mode

oam remote-loopback

1.1.28. oam remote-loopback reject-request

Use **oam remote-loopback reject-request** to configure an interface to reject the Ethernet OAM remote loopback request from a remote interface.

Use **undo oam remote-loopback reject-request** to restore the default.

Syntax

oam remote-loopback reject-request

undo oam remote-loopback reject-request

Default

An interface does not reject the Ethernet OAM remote loopback request from a remote interface.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

If an interface is in loopback state when you execute the **oam remote-loopback reject-request** command, the configuration takes effect when the next loopback starts.

Examples

Configure GigabitEthernet 1/0/1 to reject the Ethernet OAM remote loopback request from a remote interface.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] oam remote-loopback reject-request
```

1.1.29. oam timer hello

Use **oam timer hello** to configure the Ethernet OAM handshake packet transmission interval.

Use **undo oam timer hello** to restore the default.

Syntax

oam timer hello *interval*

undo oam timer hello

Default

An interface uses the global setting.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Predefined user roles

network-admin

Parameters

interval: Specifies the Ethernet OAM handshake packet transmission interval, in steps of 100, in milliseconds. The value range for the *interval* argument is 500 to 5000.

Usage guidelines

After the timeout timer of an Ethernet OAM connection expires, the local OAM entity ages out and terminates its connection with the peer OAM entity. To keep the Ethernet OAM connections stable, set the connection timeout timer to be at least five times the handshake packet transmission interval.

The configuration in interface view takes effect only on the specified interface. For an interface, the configuration in interface view takes precedence.

Examples

Set the Ethernet OAM handshake packet transmission interval to 600 milliseconds on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] oam timer hello 600
```

Related commands

display oam configuration

oam global timer hello

1.1.30. oam timer keepalive

Use **oam timer keepalive** to configure the Ethernet OAM connection timeout timer.

Use **undo oam timer keepalive** to restore the default.

Syntax

oam timer keepalive *interval*

undo oam timer keepalive

Default

An interface uses the global setting.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Predefined user roles

network-admin

Parameters

interval: Specifies the Ethernet OAM connection timeout timer, in steps of 100, in milliseconds. The value range for the *interval* argument is 1000 to 25000.

Usage guidelines

After the timeout timer of an Ethernet OAM connection expires, the local OAM entity ages out and terminates its connection with the peer OAM entity. To keep the Ethernet OAM connections stable, set the connection timeout timer to be a minimum of five times the handshake packet transmission interval.

The configuration in interface view takes effect only on the specified interface. For an interface, the configuration in interface view takes precedence.

Examples

Set the Ethernet OAM connection timeout timer to 6000 milliseconds on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] oam timer keepalive 6000
```

Related commands

display oam configuration

oam global timer keepalive

1.1.31. reset oam

Use **reset oam** to clear statistics for Ethernet OAM packets and Ethernet OAM link error events.

Syntax

reset oam [**interface** *interface-type interface-number*]

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, the command clears statistics for Ethernet OAM packets and Ethernet OAM link error events for all interfaces.

Examples

Clear statistics for Ethernet OAM packets and Ethernet OAM link error events for all interfaces.

```
<Switch> reset oam
```

Related commands

display oam

display oam link-event

Contents

A page of this section is **10-x-x**

2. CFD commands 2-1
2.1. CFD commands 2-1
2.1.1. cfd cc enable 2-1
2.1.2. cfd cc interval 2-2
2.1.3. cfd enable 2-3
2.1.4. cfd linktrace 2-3
2.1.5. cfd linktrace auto-detection 2-4
2.1.6. cfd loopback 2-5
2.1.7. cfd md 2-6
2.1.8. cfd mep 2-7
2.1.9. cfd meplist 2-8
2.1.10. cfd mip-rule 2-9
2.1.11. cfd service-instance 2-10
2.1.12. display cfd linktrace-reply 2-11
2.1.13. display cfd linktrace-reply auto-detection 2-13
2.1.14. display cfd md 2-14
2.1.15. display cfd mep 2-15
2.1.16. display cfd meplist 2-18
2.1.17. display cfd mp 2-18
2.1.18. display cfd remote-mep 2-20
2.1.19. display cfd service-instance 2-21
2.1.20. display cfd status 2-22

2. CFD commands

2.1. CFD commands

2.1.1. cfd cc enable

Use **cfd cc enable** to enable CCM sending on a specified MEP.

Use **undo cfd cc enable** to disable CCM sending on a specified MEP.

Syntax

cfd cc service-instance *instance-id* **mep** *mep-id* **enable**

undo cfd cc service-instance *instance-id* **mep** *mep-id* **enable**

Default

The CCM sending feature is disabled.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

service-instance *instance-id*: Specifies the Ethernet service instance ID in the range of 1 to 32767.

mep *mep-id*: Specifies a MEP by its ID in the range of 1 to 8191.

Usage guidelines

Follow these guidelines when you use the command:

- Configurations in Ethernet interface view take effect only on the current interface.
- Configurations in aggregate interface view take effect only on the current aggregate interface.
- If the MEP belongs to an MA that does not carry the VLAN attribute, configurations on a member port of an aggregation group view take effect only on the current member port.
- If the MEP belongs to an MA that carries the VLAN attribute, configurations on a member port of an aggregation group take effect only when the member port leaves the aggregation group.

Examples

On port GigabitEthernet 1/0/1, enable CCM sending on MEP 3 in Ethernet service instance 5.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] cfd cc service-instance 5 mep 3 enable
```

Related commands

cfd cc interval

2.1.2. cfd cc interval

Use **cfd cc interval** to set the value of the interval field in the CCM messages.

Use **undo cfd cc interval** to remove the value of the interval field in the CCM messages.

Syntax

cfd cc interval *interval-value* **service-instance** *instance-id*

undo cfd cc interval [*interval-value*] **service-instance** *instance-id*

Default

The value of this field is 4 for all CCM messages sent.

Views

System view

Predefined user roles

network-admin

Parameters

interval *interval-value*: Specifies the value of the interval field in CCM messages. The value range for the interval field is 1 to 7. If you set the value to 1 or 2, the continuity check might work incorrectly due to hardware restrictions.

service-instance *instance-id*: Specifies the Ethernet service instance ID in the range of 1 to 32767.

Usage guidelines

When setting the CCM interval, use the settings described in Table 2-1 .

Table 2-1 CCM interval field encoding

CCM interval field	Transmission interval	Maximum CCM lifetime
1	10/3 milliseconds	35/3 milliseconds
2	10 milliseconds	35 milliseconds
3	100 milliseconds	350 milliseconds
4	1 second	3.5 seconds
5	10 seconds	35 seconds
6	60 seconds	210 seconds
7	600 seconds	2100 seconds

Examples

Set the value of the interval field to 3 in CCM messages sent by MEPs in Ethernet service instance 2.

```
<Switch> system-view
[Switch] cfd cc interval 3 service-instance 2
```

Related commands

cfd cc enable

2.1.3. cfd enable

Use **cfd enable** to enable CFD.

Use **undo cfd enable** to disable CFD.

Syntax

cfd enable

undo cfd enable

Default

CFD is disabled.

Views

System view

Predefined user roles

network-admin

Examples

Enable CFD.

```
<Switch> system-view
[Switch] cfd enable
```

2.1.4. cfd linktrace

Use **cfd linktrace** to identify the path between the source MEP and target MP.

Syntax

cfd linktrace service-instance *instance-id* **mep** *mep-id* { **target-mac** *mac-address* | **target-mep** *target-mep-id* } [**ttl** *ttl-value*] [**hw-only**]

Views

Any view

Predefined user roles

network-admin

Parameters

service-instance *instance-id*: Specifies an Ethernet service instance by its ID in the range of 1 to 32767.

mep *mep-id*: Specifies the source MEP by its ID in the range of 1 to 8191.

target-mac *mac-address*: Specifies the destination MAC address, in the format of H-H-H.

target-map *target-mep-id*: Specifies the destination MEP by its ID in the range of 1 to 8191.

ttl *ttl-value*: Specifies the TTL value in the range of 1 to 255. The default value is 64.

hw-only: Sets the hw-only bits of the LTMs sent. If you specify this keyword, the MIP does not flood LTMs that have an unknown destination MAC address.

Usage guidelines

This command identifies the path between the source MEP and target MP by using LTMs and LTRs.

Examples

Identify the path between source MEP 1101 and target MEP 2001 in Ethernet service instance 1.

```
<Switch> cfd linktrace service-instance 1 mep 1101 target-mep 2001
Linktrace to MEP 2001 with the sequence number 1101-43361:
MAC address               TTL     Last MAC         Relay action
0010-fc00-6512            63      0010-fc00-6500   Hit
```

Table 2-2 Command output

Field	Description
Linktrace to MEP 2001 with the sequence number 1101-43361	Linktrace to target MEP 2001 with the sequence number 1101-43361.
MAC address	Source MAC address in the LTRs.
TTL	TTL of the LTM when it passes the device.
Last MAC	MAC address of the last-hop device the LTM passes.
Relay action	Indicates whether the forwarding device found the destination MAC address in its MAC address table. When the standard version (IEEE 802.1ag) of CFD is used: • **Hit**—The current device is the destination device. • **FDB**—The forwarding device found the destination MAC address. • **MPDB**—The destination MAC address is not found, or the destination MAC address is found in the MEP or MIP database.

Related commands

cfd linktrace auto-detection

display cfd linktrace-reply

2.1.5. cfd linktrace auto-detection

Use **cfd linktrace auto-detection** to enable automatic sending of LTMs.

Use **undo cfd linktrace auto-detection** to disable automatic sending of LTMs.

Syntax

cfd linktrace auto-detection [**size** *size-value*]

undo cfd linktrace auto-detection

Default

Automatic sending of LTMs is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

size *size-value*: Specifies the size of the buffer used to store the auto-detection result, in the range of 1 to 100 (in terms of auto-detection times). The default value is 5, which means the buffer stores the results of the recent five auto-detections.

Usage guidelines

This command enables the source MEP to send LTMs when it fails to receive CCMs from the target MEP within 3.5 times the sending interval. The destination of the LTMs is the target MEP, and the TTL field value is 255. Based on the returned LTRs, the fault source can be located on the faulty link.

If you disable automatic LTM sending, the content stored in the buffer will be removed.

Examples

Enable automatic LTM sending, and set the size of the buffer used to store the auto-detection result to 100 (in terms of auto-detection times).

```
<Switch> system-view
[Switch] cfd linktrace auto-detection size 100
```

Related commands

cfd linktrace

display cfd linktrace-reply auto-detection

2.1.6. cfd loopback

Use **cfd loopback** to enable loopback (LB).

Syntax

cfd loopback service-instance *instance-id* **mep** *mep-id* { **target-mac** *mac-address* | **target-mep** *target-mep-id* } [**number** *number*]

Views

Any view

Predefined user roles

network-admin

Parameters

service-instance *instance-id*: Specifies an Ethernet service instance by its ID in the range of 1 to 32767.

mep *mep-id*: Specifies the source MEP by its ID in the range of 1 to 8191.

target-mac *mac-address*: Specifies the destination MAC address of the MP, in the format of H-H-H.

target-mep *target-mep-id*: Specifies the target MEP by its ID in the range of 1 to 8191.

number *number*: Specifies the number of the sent LBMs packets. The value is in the range of 1 to 10. The default value is 5.

Usage guidelines

The LB function verifies link connectivity between the source MEP and the target MP by using LBMs and LBRs.

Examples

Enable LB for the link between MEP 1101 and MEP 2001 in Ethernet service instance 1 (assume that the link status is normal).

```
<Switch> cfd loopback service-instance 1 mep 1101 target-mep 2001
Loopback to MEP 2001 with the sequence number start from 1101-43404:
Reply from 0010-fc00-6512: sequence number=1101-43404 Time=5ms
Reply from 0010-fc00-6512: sequence number=1101-43405 Time=5ms
Reply from 0010-fc00-6512: sequence number=1101-43406 Time=5ms
Reply from 0010-fc00-6512: sequence number=1101-43407 Time=5ms
Reply from 0010-fc00-6512: sequence number=1101-43408 Time=5ms
Sent: 5        Received: 5        Lost: 0
```

Enable LB for the link between MEP 1101 and MEP 2001 in Ethernet service instance 1 (assume that the link status is abnormal).

```
<Switch> cfd loopback service-instance 1 mep 1101 target-mep 2001
Loopback to MEP 2001 with the sequence number start from 1101-43404:
Sent: 5        Received: 0        Lost: 5
```

Table 2-3 Command output

Field	Description
Loopback to MEP 2001 with the sequence number start from 1101-43404	Sends LBMs to remote MEP 2001 with the sequence number starting with 1101-43404.
Reply from 0010-fc00-6512	Reply from the MP with the MAC address 0010-FC00-6512.
sequence number	Sequence number in the LBR messages.
Time=5ms	The interval between the sending of LBMs and receiving of LBRs is 5 milliseconds.
Sent	Number of sent LBMs.
Received	Number of received LBRs.
Lost	Number of lost LBRs.

2.1.7. cfd md

Use **cfd md** to create an MD.

Use **undo cfd md** to delete an MD.

Syntax

cfd md *md-name* [**index** *index-value*] **level** *level-value* [**md-id** { **dns** *dns-name* | **mac** *mac-address subnumber* | **none** }]

undo cfd md *md-name*

Default

No MDs exist.

Views

System view

Predefined user roles

network-admin

Parameters

md *md-name*: Specifies the name of an MD, which is a string of 1 to 43 characters that can contain letters, numbers, and special characters such as grave accent (`), tilde (~), exclamation mark (!), at sign (@), number sign (#), dollar sign ($), percent (%), caret (^), ampersand (&), asterisk (*), brackets ({ } , ( ), [ ] , < >), hyphen (-), underscore (_), plus (+), equal sign (=), vertical bar (|), colon (:), semicolon (;), quotation mark ('), comma (,), period (.), and slash (/).

index *index-value*: Specifies an MD index in the range of 1 to 4294967295. If you do not specify this option, the system automatically assigns the smallest index number that is not in use. As a best practice, use the index automatically assigned by the system.

level *level-value*: Specifies an MD level in the range of 0 to 7.

md-id: Specifies the MD name carried by packets sent by the MEP. If you do not provide this keyword, the MD name is represented by *md-name*.

dns *dns-name*: Specifies an MD name in the format of DNS name, where *dns-name* represents the DNS name.

mac *mac-address subnumber*: Specifies an MD name containing the MAC address and an integer. The *mac-address* argument represents the MAC address of the MD, and the *subnumber* argument is in the range of 0 to 65535.

none: Specifies that no MD name is carried in the packets sent by the MEP.

Usage guidelines

An MD name must be in compliant with the specifications in IEEE802.1ag-2007.

You can create only one MD with a specific level. MD cannot be created if you enter an invalid MD name or an existing MD name or the MD index is in use.

When deleting an MD, you will also delete the configurations related to that MD.

Examples

Create an MD named **test_md1**, with its level being 3.

```
<Switch> system-view
[Switch] cfd md test_md1 level 3
```

Create an MD named **test_md2**, and the MD name carried in the packet sent by the MEP comprises the MAC address 1-1-1 and integer 1.

```
<Switch> system-view
[Switch] cfd md test_md2 level 5 md-id mac 1-1-1 1
```

2.1.8. cfd mep

Use **cfd mep** to create a MEP.

Use **undo cfd mep** to delete a MEP.

Syntax

cfd mep *mep-id* **service-instance** *instance-id* { **inbound** | **outbound** }

undo cfd mep *mep-id* **service-instance** *instance-id*

Default

No MEPs exist.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

mep *mep-id*: Specifies the MEP ID, in the range of 1 to 8191.

service-instance *instance-id*: Specifies an Ethernet service instance by its ID in the range of 1 to 32767.

inbound: Creates an inward-facing MEP.

outbound: Creates an outward-facing MEP.

Usage guidelines

In creating a MEP, the Ethernet service instance you specified defines the MD and MA to which the MEP belongs.

You cannot create a MEP if the MEP ID is not included in the MEP list of the relevant Ethernet service instance.

Follow these guidelines when you use the command:

- Configurations in Ethernet interface view take effect only on the current interface.
- Configurations in aggregate interface view take effect only on the current aggregate interface.
- If the MEP belongs to an MA that does not carry the VLAN attribute, configurations on a member port of an aggregation group take effect only on the current member port.
- If the MEP belongs to an MA that carries the VLAN attribute, configurations on a member port of an aggregation group take effect only when the member port leaves the aggregation group.

Examples

Configure a MEP list in Ethernet service instance 5, and create inward-facing MEP 3 in Ethernet service instance 5 on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] cfd md test_md level 3
[Switch] cfd service-instance 5 ma-id vlan-based md test_md vlan 100
[Switch] cfd meplist 3 service-instance 5
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] cfd mep 3 service-instance 5 outbound
```

Related commands

cfd meplist

2.1.9. cfd meplist

Use **cfd meplist** to create a MEP list.

Use **undo cfd meplist** to delete a MEP list.

Syntax

cfd meplist *mep-list* **service-instance** *instance-id*

undo cfd meplist *mep-list* **service-instance** *instance-id*

Default

No MEP list is created.

Views

System view

Predefined user roles

network-admin

Parameters

meplist *mep-list*: Specifies a space-separated list of up to 10 MEP items. Each item specifies a MEP ID or a range of MEP IDs in the form of *mep-id 1* **to** *mep-id 2*. The value range for the MEP ID is 1 to 8191. The *mep-id 2* must be equal to or greater than *mep-id 1*.

service-instance *instance-id*: Specifies an Ethernet service instance by its ID in the range of 1 to 32767.

Usage guidelines

A MEP list is a collection of local MEPs allowed to be configured and the remote MEPs to be monitored in the same MA.

Before creating a MEP list, create the relevant MD and Ethernet service instance.

After you delete a MEP list, all local MEP configurations based on this list are deleted.

Examples

Create a MEP list that includes MEP 9 through MEP 15 in Ethernet service instance 5.

```
<Switch> system-view
[Switch] cfd md test_md level 3
[Switch] cfd service-instance 5 ma-id vlan-based md test_md vlan 100
[Switch] cfd meplist 9 to 15 service-instance 5
```

Related commands

cfd md

cfd service-instance

2.1.10. cfd mip-rule

Use **cfd mip-rule** to configure the rules for generating MIPs.

Use **undo cfd mip-rule** to remove the rules for generating MIPs and the MIPs created in a service instance.

Syntax

cfd mip-rule { **default** | **explicit** } **service-instance** *instance-id*

undo cfd mip-rule [**default** | **explicit**] **service-instance** *instance-id*

Default

No rules for generating MIPs are configured and the system does not automatically generate any MIPs.

Views

System view

Predefined user roles

network-admin

Parameters

default: Specifies the default rule. If no lower-level MIP exists on an interface, a MIP is created on the current level. A MIP can be created even if no MEP is configured on the interface.

explicit: Specifies the explicit rule. If no lower-level MIP exists and a lower-level MEP exists on an interface, a MIP is created at the current level. A MIP can be created only when a lower-level MEP is created on the interface.

service-instance *instance-id*: Specifies an Ethernet service instance by its ID in the range of 1 to 32767.

Usage guidelines

The system automatically generates MIPs on each port according to the rules configured.

Examples

Configure the MIP generation rule as default in Ethernet service instance 5.

```
<Switch> system-view
[Switch] cfd mip-rule default service-instance 5
```

2.1.11. cfd service-instance

Use **cfd service-instance** to create an Ethernet service instance.

Use **undo cfd service-instance** to remove an Ethernet service instance.

Syntax

cfd service-instance *instance-id* **ma-id** { **icc-based** *ma-name* | **integer** *ma-num* | **string** *ma-name* | **vlan-based** [*vlan-id*] } [**ma-index** *index-value*] **md** *md-name* **vlan** *vlan-id*

undo cfd service-instance *instance-id*

Default

No Ethernet service instances exist.

Views

System view

Predefined user roles

network-admin

Parameters

service-instance *instance-id*: Specifies the Ethernet service instance ID in the range of 1 to 32767.

ma-id: Creates an MA.

icc-based *ma-name*: Specifies that an MA is identified by an ICC. The *ma-name* argument is a string of 1 to 13 characters.

integer *ma-num*: Specifies that an MA is identified by an integer, where the *ma-num* argument is in the range of 0 to 65535.

string *ma-name*: Specifies that an MA is identified by a string, where the *ma-name* argument is string of 1 to 45 characters that can contain letters, numbers, and special characters such as grave

accent (`), tilde (~), exclamation mark (!), at sign (@), number sign (#), dollar sign ($), percent (%), caret (^), ampersand (&), asterisk (*), brackets ({ }, ( ), [ ], < >), hyphen (-), underscore (_), plus (+), equal sign (=), vertical bar (|), colon (:), semicolon (;), quotation mark ('), comma (,), period (.), and slash (/).

vlan-based [*vlan-id*]: Specifies that an MA is identified by a VLAN ID, where the *vlan-id* argument is in the range of 1 to 4094. If you do not provide the *vlan-id* argument, the VLAN ID specified by **vlan** *vlan-id* is used. If the **vlan** *vlan-id* option is not provided, you must specify the *vlan-id* argument for the **vlan-based** [*vlan-id*] option.

ma-index *index-value*: Specifies an MA index in the range of 1 to 4294967295. If you do not specify this option, the system automatically assigns the smallest index number that is not in use. As a best practice, use the index automatically assigned by the system.

md *md-name*: Specifies the name of an MD. The *md-name* argument is a string of 1 to 43 characters that can contain letters, numbers, and special characters such as grave accent (`), tilde (~), exclamation mark (!), at sign (@), number sign (#), dollar sign ($), percent (%), caret (^), ampersand (&), asterisk (*), brackets ({ }, ( ), [ ], < >), hyphen (-), underscore (_), plus (+), equal sign (=), vertical bar (|), colon (:), semicolon (;), quotation mark (’), comma (,), period (.), and slash (/).

vlan *vlan-id*: Specifies the VLAN that the MA serves. The value range for the *vlan-id* argument is 1 to 4094.

Usage guidelines

An Ethernet service instance is indicated by an integer to represent an MA in an MD. An MA index uniquely identifies a specific MA in an MD. An MA index can be used in different MDs.

An MD name must be in compliant with the specifications in IEEE802.1ag-2007.

With the **vlan-based** [*vlan-id*] or **vlan** *vlan-id* option, the command creates an MA carrying the VLAN attribute. If you do not specify the option, the command creates an MA carrying no VLAN attribute.

You must create the relevant MD before creating an Ethernet service instance with the MD name.

Deleting an Ethernet service instance also deletes the configurations related to that Ethernet service instance.

Deleting an Ethernet service instance not only removes the connection between the Ethernet service instance and the relevant MA, but also deletes the MA.

Examples

Create a level-3 MD named **test_md** and create Ethernet service instance 5, in which the MA is identified by a VLAN and serves VLAN 100.

```
<Switch> system-view
[Switch] cfd md test_md level 3
[Switch] cfd service-instance 5 ma-id vlan-based md test_md vlan 100
```

Related commands

cfd md

2.1.12. display cfd linktrace-reply

Use **display cfd linktrace-reply** to display information about the LTRs received by a MEP.

Syntax

display cfd linktrace-reply [**service-instance** *instance-id* [**mep** *mep-id*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

service-instance *instance-id*: Specifies the Ethernet service instance ID in the range of 1 to 32767. If you do not specify this option, the command displays the LTR information for all Ethernet service instances.

mep *mep-id*: Specifies the ID of a MEP, in the range of 1 to 8191. If you do not specify this option, the command displays the LTR information for all MEPs.

Usage guidelines

This command displays only information about LTRs received by execution of the **cfd linktrace** command.

Examples

Display the LTR information saved on all the MEPs in every Ethernet service instance.

```
[Switch] display cfd linktrace-reply
Service instance: 1       MEP ID: 1003
MAC address               TTL     Last MAC          Relay action
0000-fc00-6505            63      0000-fc00-6504    MPDB
000f-e269-a852            62      0000-fc00-6505    FDB
0000-fc00-6508            61      000f-e269-a852    Hit
Service instance: 2       MEP ID: 1023
MAC address               TTL     Last MAC          Relay action
0000-fc00-6508            61      000f-e269-a852    Hit
```

Table 2-4 Command output

Field	Description
Service instance	Ethernet service instance to which the MEPs that send LTMs belong.
MEP ID	ID of the MEP that sends LTMs.
MAC address	Source MAC address in the LTR.
TTL	TTL of the LTM when it passes the device.
Last MAC	MAC address of the last-hop device the LTM passes.
Relay action	Indicates whether the forwarding device found the destination MAC address in its MAC address table. When the standard version (IEEE 802.1ag) of CFD is used: • **Hit**—The current device is the destination device. • **FDB**—The forwarding device found the destination MAC address. • **MPDB**—The destination MAC address is not found, or the destination MAC address is found in the MEP or MIP database.

Related commands

cfd linktrace

2.1.13. display cfd linktrace-reply auto-detection

Use **display cfd linktrace-reply auto-detection** to display information about the LTRs received as responses to the automatically sent LTMs.

Syntax

display cfd linktrace-reply auto-detection [**size** *size-value*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

size *size-value*: Specifies the times of recent auto-detections, in the range of 1 to 100. If you do not specify this option, the command displays all information in the buffer.

Usage guidelines

This command displays only information about LTRs received by execution of the **cfd linktrace auto-detection** command.

Examples

Display the contents of the LTRs received as responses to the LTMs automatically sent.

```
<Switch> display cfd linktrace-reply auto-detection
Service instance: 1       MEP ID: 1003    Time: 2013/05/22 10:43:57
Target MEP ID: 2005       TTL: 64
MAC address               TTL     Last MAC          Relay action
0000-fc00-6505            63      0000-fc00-6504    MPDB
000f-e269-a852            62      0000-fc00-6505    FDB
0000-fc00-6508            61      000f-e269-a852    Hit
Service instance: 2       MEP ID: 1023    Time: 2013/05/22 10:44:06
Target MEP ID: 2025       TTL: 64
MAC address               TTL     Last MAC          Relay action
0000-fc00-6508            61      000f-e269-a852    Hit
```

Table 2-5 Command output

Field	Description
Service instance	Ethernet service instance to which the MEPs that sent LTMs belong.
MEP ID	ID of the MEP that sends LTMs.
Time	Time of the LTMs automatically sent.
Target MEP ID	ID of the target MEP.
TTL	Initial TTL of the automatically sent LTMs.

Field	Description
MAC address	Source MAC address in the LTRs.
TTL	TTL of the LTM when it passes the device.
Last MAC	MAC address of the last-hop device the LTM passes.
Relay action	Indicates whether the forwarding device found the destination MAC address in its MAC address table. When the standard version (IEEE 802.1ag) of CFD is used: • **Hit**—The current device is the destination device. • **FDB**—The forwarding device found the destination MAC address. • **MPDB**—The destination MAC address is not found, or the destination MAC address is found in the MEP or MIP database.

Related commands

cfd linktrace auto-detection

2.1.14. display cfd md

Use **display cfd md** to display the MD configuration information.

Syntax

display cfd md

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display the MD configuration information.

```
<Switch> display cfd md
CFD is enabled.
Maintenance domains configured: 4 in total
Level   Index      Maintenance domain                          MD format  MD ID
0       1          md_0                                        CHARSTRING md_0
1       2          md_1                                        DNS        dns1
2       3          md_2                                        MAC        0001-00
01-0001-1
3       4          md_3                                        NONE       Without
 ID
```

Table 2-6 Command output

Field	Description
Maintenance domains configured	Number of MDs configured.
Level	Level of MD.

Field	Description
Index	MD index.
Maintenance domain	Name of MD.
MD format	MD name format: • **CHARSTRING**—Character string. • **DNS**—DNS name. • **MAC**—MAC address and an integer. • **NONE**—No MD name is carried.
MD ID	MD ID value: • A character string if the MD format is **CHARSTRING**. • A DNS name if the MD format is **DNS**. • A MAC address-subnumber if the MD format is **MAC**. • No ID if the MD format is **NONE**.

2.1.15. display cfd mep

Use **display cfd mep** to display the attribute and operating information for a MEP.

Syntax

display cfd mep *mep-id* **service-instance** *instance-id*

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

mep *mep-id*: Specifies a MEP by its ID in the range of 1 to 8191.

service-instance *instance-id*: Specifies an Ethernet service instance by its ID in the range of 1 to 32767.

Examples

Display the attribute and operating information for MEP 50 in Ethernet service instance 1.

```
<Switch> display cfd mep 50 service-instance 1
Interface: GigabitEthernet1/0/2
Maintenance domain: md_0
Maintenance domain index: 1
Maintenance association: ma_0
Maintenance association index: 1
Level: 0        VLAN: 1         Direction: Outbound
Current state: Active          CCM send: Enabled
FNG state: FNG_DEFECT_REPORTED

CCM:
```

```
Current state: CCI_WAITING
Interval: 1s        SendCCM: 12018

Loopback:
NextSeqNumber: 8877
SendLBR: 0          ReceiveInOrderLBR: 0          ReceiveOutOrderLBR: 0

Linktrace:
NextSeqNumber: 8877
SendLTR: 0          ReceiveLTM: 0

No CCM received from some remote MEPs.

One or more streams of error CCMs is received. The last received CCM:
Maintenance domain: (Without ID)
Maintenance association: matest1
MEP ID: 5      Sequence Number:0x50A
MAC Address: 0011-2233-4402
Received Time: 2013/03/06 13:01:34

One or more streams of cross-connect CCMs is received. The last received CCM:
Maintenance domain: mdtest1
Maintenance association:matest1
MEP ID: 6      Sequence Number:0x63A
MAC Address: 0011-2233-4401
Received Time: 2013/03/06 13:01:34

Some other MEPs are transmitting the RDI bit.
```

Table 2-7 Command output

Field	Description
Interface	Interface on which the MEP is configured.
Maintenance domain	MD to which the MEP belongs. (If the MD does not have a name, this field is displayed as **Without ID**.)
Maintenance domain index	Index of the MD to which the MEP belongs..
Maintenance association	MA to which the MEP belongs.
Maintenance association index	Index of the MA to which the MEP belongs.
Level	Level of the MD.
VLAN	VLAN to which the MA belongs.
Direction	Direction of the MEPs.
Current state	State of MEP: • **Active**. • **Inactive**.
CCM send	Whether the MEP sends CCM.

Field	Description
FNG state	State of FNG (Fault Notification Generator): • **FNG_RESET**—A fault has been cleared. • **FNG_DEFECT**—A fault has been detected. • **FNG_REPORT_DEFECT**—Report a fault. • **FNG_DEFECT_REPORTED**—A fault has been reported. • **FNG_DEFECT_CLEARING**—A fault is being cleared. If this field is not supported, a hyphen (-) is displayed.
CCM	Information related to CCM.
Current state	State of CCMs sent: • **CCI_IDLE**—Initial state. • **CCI_WAITING**—Sending state. If this field is not supported, a hyphen (-) is displayed.
Interval	Interval to send CCM. **Not supported** means the MEP does not support CCM sending.
SendCCM	Number of CCMs that have been sent by the MEPs. If this field is not supported, a hyphen (-) is displayed.
Loopback	Information related to Loopback.
NextSeqNumber	Sequence number of the next LBM to be sent.
SendLBR	Number of LBRs that have been sent. If the MEP is inward-facing, the number of LBRs will not be counted.
ReceiveInOrderLBR	Number of LBRs received in correct sequence.
ReceiveOutOrderLBR	Number of LBRs received out of order.
Linktrace	Information related to linktrace.
NextSeqNumber	Sequence number of the next LTM to be sent.
SendLTR	Number of LTRs sent. If the MEP is inward-facing, the number of LTRs will not be counted.
ReceiveLTM	Number of LTMs received.
No CCM received from some remote MEPs.	Failure to receive CCMs from some remote MEPs. (This information is displayed only when some CCMs are lost.)
One or more streams of error CCMs is received. The last received CCM:	Display the content of the last error CCM when one or more error CCMs are received. (This information is displayed only when error CCMs are received.)
Maintenance domain	MD of the last error CCM. If this field is not supported, a hyphen (-) is displayed.
Maintenance association	MA of the last error CCM. If this field is not supported, a hyphen (-) is displayed.
MEP	ID of the MEP that sent the last error CCM. If this field is not supported, a hyphen (-) is displayed.
Sequence Number	Sequence number of the last error CCM. If this field is not supported, a hyphen (-) is displayed.
Received Time	Time when the last error CCM is received.

Field	Description
	If this field is not supported, a hyphen (-) is displayed.
One or more streams of cross-connect CCMs is received. The last received CCM:	Cross-connect CCMs are received, and the content of the last cross-connect CCM is displayed. (This information is displayed only when cross-connect CCMs are received.)
Some other MEPs are transmitting the RDI bit.	CCMs with the RDI flag bits set are received from other MEPs. (This information is displayed only when this type of CCMs are received.)

2.1.16. display cfd meplist

Use **display cfd meplist** to display the MEP list in an Ethernet service instance.

Syntax

display cfd meplist [**service-instance** *instance-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

service-instance *instance-id*: Specifies an Ethernet service instance by its ID in the range of 1 to 32767. If you do not specify this option, the command displays MEP lists in all Ethernet service instances.

Examples

Display the MEP list in Ethernet service instance 5.

```
<Switch> display cfd meplist service-instance 5
Service instance: 5
MEP list: 1 to 20, 30, 50.
```

2.1.17. display cfd mp

Use **display cfd mp** to display the MP information.

Syntax

display cfd mp [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number. If you do not specify this option, the command displays MP information for all ports.

Usage guidelines

The output is arranged by port name. On a port, the output shows MPs that serve VLANs, and then shows MPs that do not serve any VLANs. The MPs that serve VLANs are displayed in the ascending VLAN ID order. Within the same VLAN, the output is in the order of MIPs and MEPs (from high to low level). The MEPs that do not serve any VLANs are displayed by level (from high to low).

Examples

Display the MP information on all ports.

```
<Switch> display cfd mp
Interface GigabitEthernet1/0/1   VLAN 100
MIP              Level: 2    Service instance: 102
Maintenance domain: md_2
Maintenance domain index: 3
Maintenance association: ma_2
Maintenance association index: 3

MEP ID: 101      Level: 1    Service instance: 101    Direction: Inbound
Maintenance domain: md_1
Maintenance domain index: 2
Maintenance association: ma_1
Maintenance association index: 2

MEP ID: 100      Level: 0    Service instance: 100    Direction: Outbound
Maintenance domain: md_0
Maintenance domain index: 1
Maintenance association: ma_0
Maintenance association index: 1
```

Table 2-8 Command output

Field	Description
Interface GigabitEthernet1/0/1 VLAN 100	MP configuration of VLAN 100 on GigabitEthernet 1/0/1.
MIP	A MIP in the MP.
Level	MD level to which the MP belongs.
Service instance	Ethernet service instance to which the MP belongs.
Maintenance domain	MD to which the MP belongs.
Maintenance domain index	Index of the MD to which the MP belongs.
Maintenance association	MA to which the MP belongs.
Maintenance association index	Index of the MA to which the MP belongs.
Direction	Direction of the MEP, inbound or outbound.

2.1.18. display cfd remote-mep

Use **display cfd remote-mep** to display information about a remote MEP.

Syntax

display cfd remote-mep service-instance *instance-id* **mep** *mep-id*

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

service-instance *instance-id*: Specifies an Ethernet service instance by its ID in the range of 1 to 32767.

mep *mep-id*: Specifies a MEP by its ID in the range of 1 to 8191.

Examples

Display remote MEP information for MEP 10 in Ethernet service instance 4.

```
<Switch> display cfd remote-mep service-instance 4 mep 10
MEP ID   MAC address      State        Time                 MAC status
20       f474-8800-6565   OK           2013/03/06 02:36:38  UP
30       f474-8827-6502   OK           2013/03/06 02:36:38  DOWN
40       f474-8800-6510   FAILED       2013/03/06 02:36:39  DOWN
50       f474-8852-baa0   OK           2013/03/06 02:36:44  DOWN
60       0010-fc00-6502   OK           2013/03/06 02:36:42  DOWN
```

Table 2-9 Command output

Field	Description
MEP ID	ID of the remote MED.
MAC address	MAC address of the remote MEP device. If this field is not supported, a hyphen (-) is displayed.
State	Running state of the remote MEP: • **OK**. • **FAILED**.
Time	Time when the remote MEP entered the **FAILED** or **OK** state for the last time. If this field is not supported, a hyphen (-) is displayed.
MAC status	State of the interface indicated by the last CCM received from the remote MEP: • **UP**—The interface is ready to pass packets. • **DOWN**—The interface cannot pass packets. • **TESTING**—The interface is in some test mode. • **UNKNOWN**—The interface status cannot be determined. • **DORMANT**—The interface is not in a state to pass packets. Instead, it is in a pending state, waiting for some external event.

Field	Description
	• **NOT-PRESENT**—Some component of the interface is missing. • **LLD**—The interface is down due to state of the lower layer interfaces. If this field is not supported, a hyphen (-) is displayed.

2.1.19. display cfd service-instance

Use **display cfd service-instance** to display the configuration information of Ethernet service instance.

Syntax

display cfd service-instance [*instance-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

instance-id: Specifies an Ethernet service instance ID in the range of 1 to 32767. If you do not specify this argument, the command displays configuration information for all Ethernet service instances.

Examples

Display the configuration information of all Ethernet service instances.

```
<Switch> display cfd service-instance
Service instances configured (2 in total):
Service instance 5:
Maintenance domain: md_5
Maintenance domain index: 5
Maintenance association: ma_5
Maintenance association index: 5
Level: 5  VLAN: 5   MIP rule: NONE   CCM interval: 1s   Direction: Inbound
MEP ID: 730  Interface: GigabitEthernet1/0/1

Service instance 6:
Maintenance domain: (Without ID)
Maintenance domain index: 6
Maintenance association: ma_6
Maintenance association index: 6
Level: 6  VLAN: 6   MIP rule: NONE   CCM interval: 1s   Direction: Outbound
MEP ID: 731  Interface: GigabitEthernet1/0/2
```

Table 2-10 Command output

Field	Description
Service instances are configured.	Number of Ethernet service instances configured.
Service instance	Ethernet service instance ID.
Maintenance domain	MD of the Ethernet service instances. (If the MD does not have a name, this field displays **Without ID**.)
Maintenance domain index	Index of the MD to which the Ethernet service instances belong.
Maintenance association:	MA of the Ethernet service instances.
Maintenance association index	Index of the MA to which the Ethernet service instances belong.
Level	MD level.
VLAN	VLAN to which the MA belongs.
MIP rule	MIP generation rules configured on Ethernet service instance.
CCM interval	Interval to send CCMs.
Direction	Direction of the MEPs configured on the Ethernet service instance.
MEP ID	ID of MEPs configured on the Ethernet service instance.
Interface	Interface of the MEP configured on the Ethernet service instance.

2.1.20. display cfd status

Use **display cfd status** to display the CFD and AIS status.

Syntax

display cfd status

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display the CFD and AIS status.

```
<Switch> display cfd status
CFD is enabled.
AIS is disabled.
```

Contents

A page of this section is **10-x-x**

3. DLDP commands 3-1
3.1. DLDP commands 3-1
3.1.1. display dldp 3-1
3.1.2. display dldp statistics 3-3
3.1.3. dldp authentication-mode 3-4
3.1.4. dldp authentication-password 3-5
3.1.5. dldp delaydown-timer 3-6
3.1.6. dldp enable 3-6
3.1.7. dldp global enable 3-7
3.1.8. dldp interval 3-7
3.1.9. dldp port unidirectional-shutdown 3-8
3.1.10. dldp unidirectional-shutdown 3-9
3.1.11. reset dldp statistics 3-10

3. DLDP commands

3.1. DLDP commands

3.1.1. display dldp

Use **display dldp** to display DLDP configuration.

Syntax

display dldp [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify this option, the command displays global and port-specific DLDP configuration.

Examples

Display global and port-specific DLDP configuration.

```
<Switch> display dldp
 DLDP global status: Enabled
 DLDP advertisement interval: 5s
 DLDP authentication-mode: Simple
 DLDP authentication-password: ******
 DLDP unidirectional-shutdown mode: Auto
 DLDP delaydown-timer value: 1s
 Number of enabled ports: 2

Interface GigabitEthernet1/0/1
 DLDP port state: Bidirectional
 DLDP port unidirectional-shutdown mode: None
 Number of the port's neighbors: 1
  Neighbor MAC address: 0023-8956-3600
  Neighbor port index: 79
  Neighbor state: Confirmed
  Neighbor aged time: 13s

Interface GigabitEthernet1/0/2
 DLDP port state: Inactive
 DLDP port unidirectional-shutdown mode: None
 Number of the port's neighbors: 0 (Maximum number ever detected: 1)
```

Display the DLDP configuration of GigabitEthernet 1/0/1.

```
<Switch> display dldp interface gigabitethernet 1/0/1
Interface GigabitEthernet1/0/1
 DLDP port state: Bidirectional
 DLDP port unidirectional-shutdown mode: None
 Number of the port's neighbors: 1
  Neighbor MAC address: 0023-8956-3600
  Neighbor port index: 79
  Neighbor state: Confirmed
  Neighbor aged time: 13s
```

Table 3-1 Command output

Field	Description
DLDP global status	Global DLDP state (Enabled or Disabled).
DLDP advertisement interval	Interval for sending Advertisement packets (in seconds) to maintain neighbor relations.
DLDP authentication-mode	DLDP authentication mode (None, Simple, or MD5).
DLDP authentication-password	Password for DLDP authentication: • ******—The password has been configured. • **Not configured**—The authentication mode has been configured but no password is configured.
DLDP unidirectional-shutdown mode	Global port shutdown mode (auto, manual, or hybrid) after unidirectional links are detected.
DLDP port unidirectional-shutdown mode	Port shutdown mode for the interface (auto, manual, or hybrid) after unidirectional links are detected. If no port shutdown mode is configured for an interface, this field displays **None**.
DLDP delaydown-timer value	Setting of the DelayDown timer, in seconds.
Number of enabled ports	Number of the DLDP-enabled ports.
Interface	Index of a DLDP-enabled port.
DLDP port state	DLDP state on a port: • **Bidirectional.** • **Inactive.** • **Initial.** • **Unidirectional.**
Number of the port's neighbors	Current number of neighbors.
Maximum number ever detected	Maximum number of neighbors once detected on the port. This field appears only when the current number of neighbors is different from the maximum number of neighbors once detected.
Neighbor MAC address	MAC address of the neighbor.
Neighbor port index	Neighbor port index.
Neighbor state	Neighbor state (Confirmed or Unconfirmed).
Neighbor aged time	Neighbor aging time.

3.1.2. display dldp statistics

Use **display dldp statistics** to display DLDP packet statistics.

Syntax

display dldp statistics [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify this option, the command displays DLDP packet statistics for all interfaces.

Examples

Display DLDP packet statistics for all interfaces.

```
<Switch> display dldp statistics
Interface GigabitEthernet1/0/1
 Packets sent: 6
 Packets received: 5
 Invalid packets received: 2
 Loopback packets received: 0
 Authentication-failed packets received: 0
 Valid packets received: 3

Interface GigabitEthernet1/0/2
 Packets sent: 7
 Packets received: 7
 Invalid packets received: 3
 Loopback packets received: 0
 Authentication-failed packets received: 0
 Valid packets received: 4
```

Table 3-2 Command output

Field	Description
Interface	Port index.
Packets sent	Total number of DLDP packets sent.
Packets received	Total number of DLDP packets received.
Invalid packets received	Number of the invalid packets received.
Loop packets received	Number of the loopback packets received.
Authentication failed packets received	Number of the received packets that failed to pass the authentication.
Valid packets received	Number of the valid packets received.

Related commands

reset dldp statistics

3.1.3. dldp authentication-mode

Use **dldp authentication-mode** to configure DLDP authentication.

Use **undo dldp authentication-mode** to restore the default.

Syntax

dldp authentication-mode { **md5** | **none** | **simple** }

undo dldp authentication-mode

Default

DLDP authentication mode is **none**.

Views

System view

Predefined user roles

network-admin

Parameters

md5: Specifies the MD5 authentication mode.

none: Specifies not to perform authentication.

simple: Specifies the plaintext authentication mode.

Usage guidelines

To enable DLDP to operate correctly, make sure the DLDP authentication modes and the passwords configured on the two ends of a link are the same.

If you do not configure the authentication password after you configure the authentication mode, the authentication mode is **none** no matter which authentication mode you configure.

Examples

Configure to perform plaintext authentication and set the password to **abc** (assuming that Device A and Device B are connected by a DLDP link).

- Configure Device A:

```
<DeviceA> system-view
[DeviceA] dldp authentication-mode simple
[DeviceA] dldp authentication-password simple abc
```

- Configure Device B:

```
<DeviceB> system-view
[DeviceB] dldp authentication-mode simple
[DeviceB] dldp authentication-password simple abc
```

Related commands

display dldp

dldp authentication-password

3.1.4. dldp authentication-password

Use **dldp authentication-password** to configure the password for DLDP authentication.

Use **undo dldp authentication-password** to restore the default.

Syntax

dldp authentication-password { **cipher** | **simple** } *string*

undo dldp authentication-password

Default

No DLDP authentication password is configured.

Views

System view

Predefined user roles

network-admin

Parameters

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 16 characters. Its encrypted form is a case-sensitive string of 1 to 53 characters.

Usage guidelines

To enable DLDP to operate correctly, make sure the DLDP authentication modes and the passwords configured on the two ends of a link are the same.

If you do not configure the authentication password after you configure the authentication mode, the authentication mode is **none** no matter which authentication mode you configure.

Examples

Configure to perform plaintext authentication and set the password to **abc** (assuming that Device A and Device B are connected by a DLDP link).

- Configure Device A:

```
<DeviceA> system-view
[DeviceA] dldp authentication-mode simple
[DeviceA] dldp authentication-password simple abc
```

- Configure Device B:

```
<DeviceB> system-view
[DeviceB] dldp authentication-mode simple
[DeviceB] dldp authentication-password simple abc
```

Related commands

display dldp

dldp authentication-mode

3.1.5. dldp delaydown-timer

Use **dldp delaydown-timer** to set the DelayDown timer.

Use **undo dldp delaydown-timer** to restore the default.

Syntax

dldp delaydown-timer *time*

undo dldp delaydown-timer

Default

The setting of the DelayDown timer is 1 second.

Views

System view

Predefined user roles

network-admin

Parameters

time: Specifies the DelayDown timer in the range of 1 to 5 seconds.

Usage guidelines

The DelayDown timer configured by using this command applies to all DLDP-enabled ports.

Examples

Set the DelayDown timer to 2 seconds.

```
<Switch> system-view
[Switch] dldp delaydown-timer 2
```

Related commands

display dldp

3.1.6. dldp enable

Use **dldp enable** to enable DLDP on a port.

Use **undo dldp enable** to disable DLDP on a port.

Syntax

dldp enable

undo dldp enable

Default

DLDP is disabled on a port.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

DLDP can take effect only after you enable it globally and on a port.

Examples

Enable DLDP globally, and then enable DLDP on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] dldp global enable
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] dldp enable
```

Related commands

display dldp

dldp global enable

3.1.7. dldp global enable

Use **dldp global enable** to enable DLDP globally.

Use **undo dldp global enable** to disable DLDP globally.

Syntax

dldp global enable

undo dldp global enable

Default

DLDP is disabled globally.

Views

System view

Predefined user roles

network-admin

Usage guidelines

DLDP can take effect only after you enable it globally and on a port.

Examples

Enable DLDP globally.

```
<Switch> system-view
[Switch] dldp global enable
```

Related commands

display dldp

dldp enable

3.1.8. dldp interval

Use **dldp interval** to set the interval for sending Advertisement packets.

Use **undo dldp interval** to restore the default.

Syntax

dldp interval *interval*

undo dldp interval

Default

The interval for sending Advertisement packets is 5 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies Advertisement packets sending interval in the range of 1 to 100 seconds.

Usage guidelines

This command applies to all DLDP-enabled ports.

To enable DLDP to operate correctly, make sure the intervals for sending Advertisement packets configured on the two ends of a link are the same.

Examples

Set the interval for sending Advertisement packets to 20 seconds.

```
<Switch> system-view
[Switch] dldp interval 20
```

Related commands

display dldp

3.1.9. dldp port unidirectional-shutdown

Use **dldp port unidirectional-shutdown** to set the port shutdown mode for an interface.

Use **undo dldp port unidirectional-shutdown** to restore the default.

Syntax

dldp port unidirectional-shutdown { **auto** | **hybrid**|**manual** }

undo dldp port unidirectional-shutdown

Default

The global setting is used.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Predefined user roles

network-admin

Parameters

auto: Specifies the auto mode. In this mode, when DLDP detects a unidirectional link, it shuts down the unidirectional port. When the link becomes bidirectional, DLDP brings up the port that was shut down.

hybrid: Specifies the hybrid mode. In this mode, when DLDP detects a unidirectional link, it shuts down the unidirectional port and stops link detection. To verify the link status, use the **undo shutdown** command to bring up the port. If the link becomes bidirectional, the port becomes bidirectional.

manual: Specifies the manual mode. In this mode, when DLDP detects a unidirectional link, it does not shut down the involved port. You must manually shut it down. To verify the link status, use the **undo shutdown** command to bring up the port. If the link becomes bidirectional, the port becomes bidirectional.

Usage guidelines

If DLDP detects a unidirectional link, you must troubleshoot the interface and cabling faults.

The port shutdown mode setting for an interface takes effect only on the current interface and has priority over the global port shutdown mode setting.

Examples

Set the port shutdown mode to **manual** for GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] dldp port unidirectional-shutdown manual
```

Related commands

display dldp

dldp unidirectional-shutdown

3.1.10. dldp unidirectional-shutdown

Use **dldp unidirectional-shutdown** to set the global port shutdown mode.

Use **undo dldp unidirectional-shutdown** to restore the default.

Syntax

dldp unidirectional-shutdown { **auto** | **manual** }

undo dldp unidirectional-shutdown

Default

The global port shutdown mode is auto mode.

Views

System view

Predefined user roles

network-admin

Parameters

auto: Specifies the auto mode. In this mode, when DLDP detects a unidirectional link, it shuts down the unidirectional port. When the link becomes bidirectional, DLDP brings up the port that was shut down.

manual: Specifies the manual mode. In this mode, when DLDP detects a unidirectional link, it does not shut down the involved port. You must manually shut it down. To verify the link status, use the **undo shutdown** command to bring up the port. If the link becomes bidirectional, the port becomes bidirectional.

Usage guidelines

If DLDP detects a unidirectional link, you must troubleshoot the interface and cabling faults.

The global port shutdown mode setting takes effect on all interfaces and has lower priority than the port shutdown mode setting for an interface.

Examples

Set the global port shutdown mode to manual mode.

```
<Switch> system-view
[Switch] dldp unidirectional-shutdown manual
```

Related commands

display dldp

dldp port unidirectional-shutdown

3.1.11. reset dldp statistics

Use **reset dldp statistics** to clear DLDP packet statistics.

Syntax

reset dldp statistics [**interface** *interface-type interface-number*]

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify this option, the command clears DLDP packet statistics for all interfaces.

Examples

Clear DLDP packet statistics for all interfaces.

```
<Switch> reset dldp statistics
```

Related commands

display dldp statistics

Contents

A page of this section is **10-x-x**

4. RRPP commands 4-1
4.1. RRPP commands 4-1
4.1.1. control-vlan 4-1
4.1.2. display rrpp brief 4-1
4.1.3. display rrpp ring-group 4-4
4.1.4. display rrpp statistics 4-5
4.1.5. display rrpp verbose 4-8
4.1.6. domain ring 4-10
4.1.7. fast-detection enable 4-11
4.1.8. fast-timer 4-12
4.1.9. protected-vlan 4-13
4.1.10. reset rrpp statistics 4-14
4.1.11. ring 4-14
4.1.12. ring enable 4-16
4.1.13. rrpp domain 4-17
4.1.14. rrpp enable 4-17
4.1.15. rrpp ring-group 4-18
4.1.16. snmp-agent trap enable rrpp 4-19
4.1.17. timer 4-19

4. RRPP commands

4.1. RRPP commands

4.1.1. control-vlan

Use **control-vlan** to configure the primary control VLAN for an RRPP domain.

Use **undo control-vlan** to restore the default.

Syntax

control-vlan *vlan-id*

undo control-vlan

Default

No control VLANs exist in an RRPP domain.

Views

RRPP domain view

Predefined user roles

network-admin

Parameters

vlan-id: Specifies the primary control VLAN by its ID in the range of 2 to 4093.

Usage guidelines

When you configure control VLANs for an RRPP domain, you only need to configure the primary control VLAN. The system automatically configures the secondary control VLAN. It uses the primary control VLAN ID plus 1 as the secondary control VLAN ID. For the control VLAN configuration to succeed, make sure the IDs of the two control VLANs are consecutive and have not been assigned yet.

Do not configure the default VLAN of a port accessing an RRPP ring as the control VLAN.

To ensure correct forwarding of RRPPDUs, do not enable QinQ or VLAN mapping on the control VLANs.

After you configure RRPP rings for an RRPP domain, you cannot delete or modify the primary control VLAN of the domain. To do so, use the **undo control-vlan** command.

Examples

Configure VLAN 100 as the primary control VLAN of RRPP domain 1 (assume that VLAN 100 and VLAN 101 have not been created yet).

```
<Switch> system-view
[Switch] rrpp domain 1
[Switch-rrpp-domain1] control-vlan 100
```

4.1.2. display rrpp brief

Use **display rrpp brief** to display brief RRPP information.

Syntax

display rrpp brief

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display brief RRPP information.

```
<Switch> display rrpp brief
 Flags for node mode: M -- Master, T -- Transit, E -- Edge, A -- Assistant-edge

 RRPP protocol status: Enabled

 Domain ID     : 1
 Control VLAN  : Primary 5, Secondary 6
 Protected VLAN: Reference instance 0 to 2, 4
 Hello timer   : 1 seconds, Fail timer: 3 seconds
 Fast detection status: Disabled
 Fast-Hello timer: 20 ms, Fast-Fail timer: 60 ms
 Fast-Edge-Hello timer: 10 ms, Fast-Edge-Fail timer: 30 ms
  Ring  Ring   Node  Primary/Common            Secondary/Edge            Enable
  ID    level  mode  port                      port                      status
 ------------------------------------------------------------------------------
  1     1      M     GE1/0/1                   GE1/0/2                   Yes

 Domain ID     : 2
 Control VLAN  : Primary 10, Secondary 11
 Protected VLAN: Reference instance 0 to 2, 4
 Hello timer   : 1 seconds, Fail timer: 3 seconds
 Fast detection status: Disabled
 Fast-Hello timer: 20 ms, Fast-Fail timer: 60 ms
 Fast-Edge-Hello timer: 10 ms, Fast-Edge-Fail timer: 30 ms
  Ring  Ring   Node  Primary/Common            Secondary/Edge            Enable
  ID    level  mode  port                      port                      status
 ------------------------------------------------------------------------------
  1     0      T     GE1/0/3                   GE1/0/4                   Yes
  2     1      E     GE1/0/3                   GE1/0/5                   Yes
                     GE1/0/4
```

Table 4-1 Command output

Field	Description
Flags for node mode	RRPP node mode: • **M**—Master node. • **T**—Transit node.

Field	Description
	• **E**—Edge node. • **A**—Assistant edge node.
RRPP protocol status	RRPP status: • **Enabled**—Globally enabled. • **Disabled**—Globally disabled.
Domain ID	RRPP domain ID.
Control VLAN	Primary and secondary control VLANs of the RRPP domain.
Protected VLAN	MSTIs corresponding to the VLANs protected by the RRPP domain. To view the VLAN-to-instance mappings, use the **display stp region-configuration** command (see *Layer 2—LAN Switching Command Reference*).
Hello timer	Hello timer value in seconds.
Fail timer	Fail timer value in seconds.
Fast detection status	This field is not supported in the current software version. Fast detection status: **Enabled** or **Disabled**.
Fast-Hello timer	This field is not supported in the current software version. Fast-Hello timer value in milliseconds.
Fast-Fail timer	This field is not supported in the current software version. Fast-Fail timer value in milliseconds.
Fast-Edge-Hello timer	This field is not supported in the current software version. Fast-Edge-Hello timer value in milliseconds.
Fast-Edge-Fail timer	This field is not supported in the current software version. Fast-Edge-Fail timer value in milliseconds.
Ring ID	RRPP ring ID.
Ring level	RRPP ring level: • **0**—Primary ring. • **1**—Subring.
Primary/Common port	This field displays primary ports when the node mode is master node or transit node. This field displays common ports when the node mode is edge node or assistant edge node. A hyphen (-) appears when one of the following cases occurs: • The port is not configured on the ring. • The interface expansion card to which the port belongs has not started up. • The port is a member of a link aggregation group.
Secondary/Edge port	This field displays secondary ports when the node mode is master node or transit node. This field displays edge ports when the node mode is edge node or assistant edge node. A hyphen (-) appears when one of the following cases occurs: • The port is not configured on the ring. • The interface expansion card to which the port belongs has not started up. • The port is a member of a link aggregation group.

Field	Description
Enable status	RRPP ring status: • **Yes**—Enabled. • **No**—Disabled.

4.1.3. display rrpp ring-group

Use **display rrpp ring-group** to display the RRPP ring group configuration.

Syntax

display rrpp ring-group [*ring-group-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ring-group-id: Specifies an RRPP ring group by its ID in the range of 1 to 64 If you do not specify this argument, the command displays the configuration of all ring groups.

Usage guidelines

For an edge node RRPP ring group, this command also displays the subring sending Edge-Hello packets.

Examples

Display the configuration of all RRPP ring groups.

```
<Switch> display rrpp ring-group
 Ring group 1:
  Domain 1 ring 1 to 3, 5
  Domain 2 ring 1 to 3, 5
  Domain 1 ring 1 is the sending ring

 Ring group 2:
  Domain 1 ring 4, 6 to 7
  Domain 2 ring 4, 6 to 7
```

Table 4-2 Command output

Field	Description
Ring group 1	RRPP ring group 1.
Domain 1 ring 1 to 3, 5	Subrings in the ring group, including rings 1, 2, 3, and 5 in RRPP domain 1.
Domain 1 ring 1 is the sending ring	The sending ring of the ring group is ring 1 in RRPP domain 1.

4.1.4. display rrpp statistics

Use **display rrpp statistics** to display RRPPDU statistics.

Syntax

display rrpp statistics domain *domain-id* [**ring** *ring-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

domain *domain-id*: Specifies an RRPP domain by its ID in the range of 1 to 128.

ring *ring-id*: Specifies an RRPP ring by its ID in the range of 1 to 128. If you do not specify this option, the command displays the RRPPDU statistics for all rings in the specified RRPP domain.

Usage guidelines

If a port belongs to more than one ring, this command collects and displays RRPPDU statistics of the port by ring.

When a ring transits from inactive status to active status, packet counting for the ring restarts.

Examples

Display RRPPDU statistics for all rings in RRPP domain 2.

```
<Switch> display rrpp statistics domain 2
 Ring ID       : 1
 Ring level    : 0
 Node mode     : Master
 Active status : Yes
 Primary port  : GE1/0/3
 Fast-Hello packets: 0 Sent, 0 Received
 Fast-Edge-Hello packets: 0 Sent, 0 Received
  Direct Hello     Link      Common     Complete   Edge      Major     Total
                   down      flush FDB  flush FDB  hello     fault
 ------------------------------------------------------------------------------
  Out    16924     0         0          1          0         0         16925
  In     0         0         0          0          0         0         0
 Secondary port: GE1/0/4
 Fast-Hello packets: 0 Sent, 0 Received
 Fast-Edge-Hello packets: 0 Sent, 0 Received
  Direct Hello     Link      Common     Complete   Edge      Major     Total
                   down      flush FDB  flush FDB  hello     fault
 ------------------------------------------------------------------------------
  Out    0         0         0          0          0         0         0
  In     16878     0         0          1          0         0         16879

 Ring ID       : 2
```

```
Ring level    : 1
Node mode     : Edge
Active status : No
Common port   : GE1/0/3
Fast-Hello packets: 0 Sent, 0 Received
Fast-Edge-Hello packets: 0 Sent, 0 Received
 Direct Hello     Link     Common     Complete   Edge      Major     Total
                  down     flush FDB  flush FDB  hello     fault
--------------------------------------------------------------------------------
 Out    0         0        0          0          0         0         0
 In     0         0        0          0          0         0         0
Common port   : GE1/0/4
Fast-Hello packets: 0 Sent, 0 Received
Fast-Edge-Hello packets: 0 Sent, 0 Received
 Direct Hello     Link     Common     Complete   Edge      Major     Total
                  down     flush FDB  flush FDB  hello     fault
--------------------------------------------------------------------------------
 Out    0         0        0          0          0         0         0
 In     0         0        0          0          0         0         0
Edge port     : GE1/0/5
 Direct Hello     Link     Common     Complete   Edge      Major     Total
                  down     flush FDB  flush FDB  hello     fault
--------------------------------------------------------------------------------
 Out    0         0        0          0          0         0         0
 In     0         0        0          0          0         0         0
```

Table 4-3 Command output

Field	Description
Ring ID	RRPP ring ID.
Ring level	RRPP ring level: • **0**—Primary ring. • **1**—Subring.
Node mode	Node mode: • Master node. • Transit node. • Edge node. • Assistant edge node.
Active status	RRPP ring status: • **Yes**—Active. • **No**—Inactive.
Primary port	The primary port field means the node mode is master node or transit node. A hyphen (-) appears when one of the following cases occurs: • The port is not configured on the ring. • The interface expansion card to which the port belongs has not started up. • The port is a member of a link aggregation group.

Field	Description
Secondary port	The secondary port field means the node mode is master node or transit node. A hyphen (-) appears when one of the following cases occurs: • The port is not configured on the ring. • The interface expansion card to which the port belongs has not started up. • The port is a member of a link aggregation group.
Common port	The common port field means the node mode is edge node or assistant edge node. A hyphen (-) appears when one of the following cases occurs: • The port is not configured on the ring. • The interface expansion card to which the port belongs has not started up. • The port is a member of a link aggregation group.
Edge port	The edge port field means the node mode is edge node or assistant edge node. A hyphen (-) appears when one of the following cases occurs: • The port is not configured on the ring. • The interface expansion card to which the port belongs has not started up. • The port is a member of a link aggregation group.
Fast-Hello packets	This field is not supported in the current software version. Fast-Hello packet statistics on the port: • **Sent**—Number of Fast-Hello packets sent out of the port. • **Received**—Number of Fast-Hello packets received on the port.
Fast-Edge-Hello packets	This field is not supported in the current software version. Fast-Edge-Hello packet statistics on the port: • **Sent**—Number of Fast-Edge-Hello packets sent out of the port. • **Received**—Number of Fast-Edge-Hello packets received on the port.
Packet direct	Packet transmission direction on the port: • **Out**—Packet sending direction. • **In**—Packet receiving direction.
Hello	Statistics of Hello packets received/sent on the port.
Link down	Statistics of Link-Down packets received/sent on the port.
Common flush FDB	Statistics of Common-Flush-FDB packets received/sent on the port.
Complete flush FDB	Statistics of Complete-Flush-FDB packets received/sent on the port.
Edge hello	Statistics of Edge-Hello packets received/sent on the port.
Major fault	Statistics of Major-Fault packets received/sent on the port.
Total	Total number of packets received/sent on the port. Only Hello, Link-Down, Common-Flush-FDB, Complete-Flush-FDB, Edge-Hello, and Major-Fault packets of RRPP are counted.

Related commands

reset rrpp statistics

4.1.5. display rrpp verbose

Use **display rrpp verbose** to display detailed RRPP information.

Syntax

display rrpp verbose domain *domain-id* [**ring** *ring-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

domain *domain-id*: Specifies an RRPP domain by its ID in the range of 1 to 128.

ring *ring-id*: Specifies an RRPP ring by its ID in the range of 1 to 128. If you do not specify this option, the command displays detailed information for all rings in the specified RRPP domain.

Examples

Display detailed information for all rings in RRPP domain 2.

```
<Switch> display rrpp verbose domain 2
 Domain ID      : 2
 Control VLAN   : Primary 10, Secondary 11
 Protected VLAN: Reference instance 3, 5 to 7
 Hello timer    : 1 seconds, Fail timer: 3 seconds
 Fast detection status: Disabled
 Fast-Hello timer: 20 ms, Fast-Fail timer: 60 ms
 Fast-Edge-Hello timer: 10 ms, Fast-Edge-Fail timer: 30 ms

 Ring ID        : 1
 Ring level     : 0
 Node mode      : Master
 Ring state     : Completed
 Enable status  : Yes, Active status: Yes
 Primary port   : GE1/0/4                    Port status: UP
 Secondary port: GE1/0/5                     Port status: BLOCKED

 Ring ID        : 2
 Ring level     : 1
 Node mode      : Edge
 Ring state     : -
 Enable status  : No, Active status: No
 Common port    : GE1/0/4                    Port status: -
                  GE1/0/5                    Port status: -
 Edge port      : GE1/0/3                    Port status: -
```

Table 4-4 Command output

Field	Description
Domain ID	RRPP domain ID.
Control VLAN	Control VLANs of the RRPP domain: • **Primary**—Primary control VLAN. • **Secondary**—Secondary control VLAN.
Protected VLAN	MSTIs corresponding to the VLANs protected by the RRPP domain. To view the VLAN-to-instance mappings, use the **display stp region-configuration** command (see *Layer 2—LAN Switching Command Reference*).
Hello timer	Hello timer value in seconds.
Fail timer	Fail timer value in seconds.
Fast detection status	This field is not supported in the current software version. Fast detection mechanism status: **Enabled** or **Disabled**.
Fast-Hello timer	This field is not supported in the current software version. Fast-Hello timer value in milliseconds.
Fast-Fail timer	This field is not supported in the current software version. Fast-Fail timer value in milliseconds.
Fast-Edge-Hello timer	This field is not supported in the current software version. Fast-Edge-Hello timer value in milliseconds.
Fast-Edge-Fail timer	This field is not supported in the current software version. Fast-Edge-Fail timer value in milliseconds.
Ring ID	RRPP ring ID.
Ring level	RRPP ring level: • **0**—Primary ring. • **1**—Subring.
Node mode	Node mode: • Master node. • Transit node. • Edge node. • Assistant edge node.
Ring state	RRPP ring state: • **Completed**—The ring is healthy. • **Failed**—The ring is not closed. If the ring is not enabled on the device operating as the master node or the device is not the master node of the ring, a hyphen (-) is displayed.
Enable status	RRPP ring status: • **Yes**—Enabled. • **No**—Disabled.
Active status	RRPP ring status: • **Yes**—Active. • **No**—Inactive. An RRPP ring can be active only when RRPP and the RRPP ring are both enabled. This field also helps you identify whether RRPP is

Field	Description
	enabled.
Primary port	The primary port field means the node mode is master node or transit node. A hyphen (-) appears when one of the following cases occurs: • The port is not configured on the ring. • The interface expansion card to which the port belongs has not started up. • The port is a member of a link aggregation group.
Secondary port	The secondary port field means the node mode is master node or transit node. A hyphen (-) appears when one of the following cases occurs: • The port is not configured on the ring. • The interface expansion card to which the port belongs has not started up. • The port is a member of a link aggregation group.
Common port	The common port field means the node mode is edge node or assistant edge node. A hyphen (-) appears when one of the following cases occurs: • The port is not configured on the ring. • The interface expansion card to which the port belongs has not started up. • The port is a member of a link aggregation group.
Edge port	The edge port field means the node mode is edge node or assistant edge node. A hyphen (-) appears when one of the following cases occurs: • The port is not configured on the ring. • The interface expansion card to which the port belongs has not started up. • The port is a member of a link aggregation group.
Port status	Port status: Down, up, or blocked. A hyphen (-) appears when one of the following cases occurs: • The ring is inactive. • The port is not configured on the ring. • The interface expansion card to which the port belongs has not started up. • The port is a member of a link aggregation group.

4.1.6. domain ring

Use **domain ring** to configure subrings for an RRPP ring group.

Use **undo domain ring** to remove subrings from the RRPP ring group.

Syntax

domain *domain-id* **ring** *ring-id-list*

undo domain *domain-id* [**ring** *ring-id-list*]

Default

No subrings exist in an RRPP ring group.

Views

RRPP ring group view

Predefined user roles

network-admin

Parameters

domain-id: Specifies an RRPP domain by its ID in the range of 1 to 128.

ring *ring-id-list*: Specifies a space-separated list of up to 10 RRPP subring ID items. Each item specifies an RRPP subring ID or a range of RRPP subring IDs. The value range for RRPP subring IDs is 1 to 128. If you do not specify this option, the command removes all subrings from the ring group in the specified domain.

Usage guidelines

Follow these guidelines when you configure an RRPP ring group on the edge node and the assistant edge node:

- When you assign an active ring to a ring group, assign it on the assistant edge node first and then on the edge node.
- To remove an active ring from a ring group, remove it on the edge node first and then on the assistant edge node.
- To remove a ring group, remove it on the edge node first and then on the assistant edge node.
- When you activate rings in a ring group, activate them on the edge node first and then on the assistant edge node.
- When you deactivate rings in a ring group, deactivate them on the assistant edge node first and then on the edge node.

If you do not follow these guidelines, the assistant edge node might fail to receive Edge-Hello packets and consider the primary ring failed even if it did not.

Examples

Create RRPP ring group 1, and add subrings 1, 2, 3, and 5 to domain 1 and domain 2.

```
<Switch> system-view
[Switch] rrpp ring-group 1
[Switch-ring-group1] domain 1 ring 1 to 3 5
[Switch-ring-group1] domain 2 ring 1 to 3 5
```

Related commands

display rrpp ring-group

rrpp ring-group

4.1.7. fast-detection enable

NOTE:

This command is only supported when used in combination with UNIVERGE Network Operation Engine Overlay Network Extension.

Use **fast-detection enable** to enable fast detection for the RRPP domain.

Use **undo fast-detection enable** to disable fast detection for the RRPP domain.

Syntax

fast-detection enable

undo fast-detection enable

Default

Fast detection is disabled for an RRPP domain.

Views

RRPP domain view

Predefined user roles

network-admin

Usage guidelines

To make fast detection take effect in an RRPP domain, enable fast detection, RRPP, and the RRPP rings in the RRPP domain.

Examples

Enable fast detection for RRPP domain 1.

```
<Sysname> system-view
[Sysname] rrpp domain 1
[Sysname-rrpp-domain1] fast-detection enable
```

Related commands

ring enable

rrpp enable

4.1.8. fast-timer

NOTE:

This command is only supported when used in combination with UNIVERGE Network Operation Engine Overlay Network Extension.

Use **fast-timer** to set the Fast-Hello timer and the Fast-Fail timer.

Use **undo fast-timer** to restore the default.

Syntax

fast-timer hello-timer *hello-value* **fail-timer** *fail-value*

undo fast-timer

Default

The Fast-Hello timer is 20 milliseconds and the Fast-Fail timer is 60 milliseconds.

Views

RRPP domain view

Predefined user roles

network-admin

Parameters

hello-timer *hello-value*: Specifies the Fast-Hello timer in the range of 10 to 500 milliseconds.

fail-timer *fail-value*: Specifies the Fast-Fail timer in the range of 30 to 1500 milliseconds.

Usage guidelines

The Fast-Fail timer must be greater than or equal to three times the Fast-Hello timer.

Examples

Set the Fast-Hello timer to 20 milliseconds and the Fast-Fail timer to 70 milliseconds for RRPP domain 1.

```
<Sysname> system-view
[Sysname] rrpp domain 1
[Sysname-rrpp-domain1] fast-timer hello-timer 20 fail-timer 70
```

4.1.9. protected-vlan

Use **protected-vlan** to configure the protected VLANs for an RRPP domain.

Use **undo protected-vlan** to remove the protected VLANs from an RRPP domain.

Syntax

protected-vlan reference-instance *instance-id-list*

undo protected-vlan [**reference-instance** *instance-id-list*]

Default

No protected VLANs exist in an RRPP domain.

Views

RRPP domain view

Predefined user roles

network-admin

Parameters

reference-instance *instance-id-list*: Specifies the Multiple Spanning Tree Instances (MSTIs) you want to reference in the form of *instance-id-list* = { *instance-id* [**to** *instance-id*] }&<1-10>. The *instance-id* argument is an MSTI ID in the range of 0 to 4094. You can specify up to 10 MSTI IDs or ID ranges. You can use the **display stp region-configuration** command to display the VLAN-to-instance mappings. If you do not specify this option, the command removes all MSTIs referenced by the RRPP domain.

Usage guidelines

When the device's spanning tree operation mode is PVST mode, the MSTI ID value is only 0.

You can delete or modify the protected VLANs configured for an RRPP domain before and after you configure rings for the domain. However, after you configure rings for the RRPP domain, you cannot delete configurations of all the protected VLANs configured for the domain.

When the VLAN-to-instance mappings change, the protected VLANs of an RRPP domain also change.

Examples

Map VLANs 1 through 30 to MSTI 1, and activate the MST region configuration. Configure VLAN 100 as the control VLAN of RRPP domain 1. Configure VLANs mapped to MSTI 1 as the primary control VLANs of RRPP domain 1.

```
<Switch> system-view
[Switch] stp region-configuration
[Switch-mst-region] instance 1 vlan 1 to 30
```

```
[Switch-mst-region] active region-configuration
[Switch-mst-region] quit
[Switch] rrpp domain 1
[Switch-rrpp-domain1] control-vlan 100
[Switch-rrpp-domain1] protected-vlan reference-instance 1
```

Related commands

display stp region-configuration (*Layer 2—LAN Switching Command Reference*)

rrpp domain

4.1.10. reset rrpp statistics

Use **reset rrpp statistics** to clear RRPPDU statistics.

Syntax

reset rrpp statistics domain *domain-id* [**ring** *ring-id*]

Views

User view

Predefined user roles

network-admin

Parameters

domain *domain-id*: Specifies an RRPP domain by its ID in the range of 1 to 128.

ring *ring-id*: Specifies an RRPP ring by its ID in the range of 1 to 128. If you do not specify this option, the command clears RRPPDU statistics of all RRPP rings in the specified RRPP domain.

Examples

Clear the RRPPDU statistics of ring 10 in RRPP domain 1.

```
<Switch> reset rrpp statistics domain 1 ring 10
```

Related commands

display rrpp statistics

4.1.11. ring

Use **ring** to configure the node mode of the device, the role of the specified RRPP port, and the level of the RRPP ring.

Use **undo ring** to delete the RRPP ring.

Syntax

ring *ring-id* **node-mode** { { **master** | **transit** } [**primary-port** *interface-type interface-number*] [**secondary-port** *interface-type interface-number*] **level** *level-value* | { **assistant-edge** | **edge** } [**edge-port** *interface-type interface-number*] }

undo ring *ring-id*

Default

The device is not a node of the RRPP ring.

Views

RRPP domain view

Predefined user roles

network-admin

Parameters

ring-id: Specifies an RRPP ring by its ID in the range of 1 to 128.

master: Specifies the device as the master node of the RRPP ring.

transit: Specifies the device as the transit node of the RRPP ring.

primary-port: Specifies the port as a primary port.

interface-type interface-number: Specifies a port by its type and number.

secondary-port: Specifies the port as a secondary port.

level *level-value*: Specifies an RRPP ring level, 0 for the primary ring and 1 for the subring.

assistant-edge: Specifies the device as the assistant edge node of the RRPP ring.

edge: Specifies the device as the edge node of the RRPP ring.

edge-port: Specifies the edge port for the node.

Usage guidelines

The ID of an RRPP ring in a domain must be unique.

When an RRPP ring is activated, you cannot configure its RRPP ports.

When you configure the edge node and the assistant edge node, first configure the primary ring, and then the subrings.

The node mode, RRPP port role, and ring level settings of an RRPP ring cannot be modified after they are configured. To modify the settings, first remove the current settings.

Remove all subring configurations before you delete the primary ring configuration of the edge node or the assistant edge node. However, an active RRPP ring cannot be deleted.

When RRPP is enabled on a device, you must disable the RRPP ring before you can delete it. When RRPP is disabled on the device, you can directly delete the RRPP ring, as well as the setting of the **ring enable** command.

Examples

Specify the device as the master node of primary ring 10 in RRPP domain 1. Specify GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port.

```
<Switch> system-view
[Switch] rrpp domain 1
[Switch-rrpp-domain1] control-vlan 100
[Switch-rrpp-domain1] protected-vlan reference-instance 0 1 2
[Switch-rrpp-domain1] ring 10 node-mode master primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
```

Specify the device as the transit node of primary ring 10 in RRPP domain 1. Specify GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port. Specify the device as the edge node of subring 20 in RRPP domain 1, and specify GigabitEthernet 1/0/3 as the edge port.

```
<Switch> system-view
[Switch] rrpp domain 1
```

```
[Switch-rrpp-domain1] control-vlan 100
[Switch-rrpp-domain1] protected-vlan reference-instance 0 1 2
[Switch-rrpp-domain1] ring 10 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[Switch-rrpp-domain1] ring 20 node-mode edge edge-port gigabitethernet 1/0/3
```

Related commands

ring enable

4.1.12. ring enable

Use **ring enable** to enable an RRPP ring.

Use **undo ring enable** to disable the RRPP ring.

Syntax

ring *ring-id* **enable**

undo ring *ring-id* **enable**

Default

An RRPP ring is disabled.

Views

RRPP domain view

Predefined user roles

network-admin

Parameters

ring-id: Specifies an RRPP ring by its ID in the range of 1 to 128.

Usage guidelines

To activate an RRPP ring, you must enable RRPP and the RRPP ring.

Before you enable subrings on a device, you must enable the primary ring. Before you disable the primary ring on the device, you must disable all subrings. Otherwise, the system displays error prompts.

Examples

Enable RRPP ring 10 in RRPP domain 1.

```
<Switch> system-view
[Switch] rrpp domain 1
[Switch-rrpp-domain1] control-vlan 100
[Switch-rrpp-domain1] protected-vlan reference-instance 0 1 2
[Switch-rrpp-domain1] ring 10 node-mode master primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[Switch-rrpp-domain1] ring 10 enable
```

Related commands

rrpp enable

4.1.13. rrpp domain

Use **rrpp domain** to create an RRPP domain and enter its view, or enter the view of an existing RRPP domain.

Use **undo rrpp domain** to remove an RRPP domain.

Syntax

rrpp domain *domain-id*

undo rrpp domain *domain-id*

Default

No RRPP domains exist.

Views

System view

Predefined user roles

network-admin

Parameters

domain-id: Specifies an RRPP domain by its ID in the range of 1 to 128.

Usage guidelines

When you delete an RRPP domain, configurations of the control VLANs and protected VLANs are deleted at the same time.

To delete an RRPP domain successfully, make sure it has no RRPP rings.

Examples

Create RRPP domain 1, and enter RRPP domain 1 view.

```
<Switch> system-view
[Switch] rrpp domain 1
[Switch-rrpp-domain1]
```

Related commands

control-vlan

protected-vlan

4.1.14. rrpp enable

Use **rrpp enable** to enable RRPP.

Use **undo rrpp enable** to disable RRPP.

Syntax

rrpp enable

undo rrpp enable

Default

RRPP is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

To activate an RRPP domain, enable RRPP and the RRPP rings for the RRPP domain.

Examples

Enable RRPP.

```
<Switch> system-view
[Switch] rrpp enable
```

Related commands

ring enable

4.1.15. rrpp ring-group

Use **rrpp ring-group** to create an RRPP ring group and enter its view, or enter the view of an existing RRPP ring group.

Use **undo rrpp ring-group** to remove an RRPP ring group.

Syntax

rrpp ring-group *ring-group-id*

undo rrpp ring-group *ring-group-id*

Default

No RRPP ring groups exist.

Views

System view

Predefined user roles

network-admin

Parameters

ring-group-id: Specifies an RRPP ring group ID in the range of 1 to 64.

Usage guidelines

When you remove a ring group, remove it on the edge node first and then on the assistant edge node. Otherwise, the assistant edge node might fail to receive Edge-Hello packets and consider the primary ring failed even if it is not.

After a ring group is removed, all subrings in the ring group do not belong to any ring group.

Examples

Create RRPP ring group 1 and enter its view.

```
<Switch> system-view
[Switch] rrpp ring-group 1
[Switch-ring-group1]
```

Related commands

display rrpp ring-group

domain ring

4.1.16. snmp-agent trap enable rrpp

Use **snmp-agent trap enable rrpp** to enable SNMP notifications for RRPP.

Use **undo snmp-agent trap enable rrpp** to disable SNMP notifications for RRPP.

Syntax

snmp-agent trap enable rrpp [**major-fault** | **multi-master** | **ring-fail** | **ring-recover**] *

undo snmp-agent trap enable rrpp [**major-fault** | **multi-master** | **ring-fail** | **ring-recover**] *

Default

SNMP notifications for RRPP are disabled.

Views

System view

Predefined user roles

network-admin

Parameters

major-fault: Generates notifications when an SRPT between the assistant edge node and edge node is disconnected.

multi-master: Generates notifications when multiple master nodes are configured for the RRPP ring.

ring-fail: Generates notifications when the state of the RRPP ring changes from Health to Disconnect.

ring-recover: Generates notifications when the state of the RRPP ring changes from Disconnect to Health.

Usage guidelines

To report critical RRPP events to an NMS, enable SNMP notifications for RRPP. For RRPP event notifications to be sent correctly, you must also configure SNMP on the device. For more information about SNMP configuration, see the network management and monitoring configuration guide for the device.

If you do not specify any keyword, this command enables or disables all SNMP notifications for RRPP.

Examples

Generate notifications when the state of the RRPP ring changes from Disconnect to Health.

```
<Switch> system-view
[Switch] snmp-agent trap enable rrpp ring-recover
```

4.1.17. timer

Use **timer** to set the Hello timer and the Fail timer.

Use **undo timer** to restore the default.

Syntax

timer hello-timer *hello-value* **fail-timer** *fail-value*

undo timer

Default

The Hello timer is 1 second and the Fail timer is 3 seconds.

Views

RRPP domain view

Predefined user roles

network-admin

Parameters

hello-timer *hello-value*: Specifies the Hello timer in the range of 1 to 10 seconds.

fail-timer *fail-value*: Specifies the Fail timer in the range of 3 to 30 seconds.

Usage guidelines

The Fail timer must be greater than or equal to three times the Hello timer.

Examples

Set the Hello timer to 2 seconds and the Fail timer to 7 seconds for RRPP domain 1.

```
<Switch> system-view
[Switch] rrpp domain 1
[Switch-rrpp-domain1] timer hello-timer 2 fail-timer 7
```

Contents

A page of this section is **10-x-x**

5. Smart Link commands 5-1
5.1. Smart Link commands 5-1
5.1.1. display smart-link flush 5-1
5.1.2. display smart-link group 5-1
5.1.3. flush enable 5-3
5.1.4. port 5-3
5.1.5. port smart-link group 5-4
5.1.6. port smart-link group track 5-5
5.1.7. preemption delay 5-7
5.1.8. preemption mode 5-7
5.1.9. protected-vlan 5-8
5.1.10. reset smart-link statistics 5-9
5.1.11. smart-link flush enable 5-10
5.1.12. smart-link group 5-10

5. Smart Link commands

5.1. Smart Link commands

5.1.1. display smart-link flush

Use **display smart-link flush** to display information about the received flush messages.

Syntax

display smart-link flush

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display information about the received flush messages.

```
<Switch> display smart-link flush
 Received flush packets                          : 10
 Receiving interface of the last flush packet    : GigabitEthernet1/0/1
 Receiving time of the last flush packet         : 19:19:03 2012/04/21
 Device ID of the last flush packet              : 000f-e200-8500
 Control VLAN of the last flush packet           : 1
```

Table 5-1 Command output

Field	Description
Received flush packets	Total number of received flush messages.
Receiving interface of the last flush packet	Port that received the last flush message.
Receiving time of the last flush packet	Time when the last flush message was received.
Device ID of the last flush packet	Device ID carried in the last flush message.
Control VLAN of the last flush packet	Control VLAN ID carried in the last flush message.

Related commands

reset smart-link statistics

5.1.2. display smart-link group

Use **display smart-link group** to display information about the specified or all smart link groups.

Syntax

display smart-link group { *group-id* | **all** }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

group-id: Specifies a smart link group by its ID. The value range for this argument is 1 to 48.

all: Displays information about all smart link groups.

Examples

Display information about smart link group 1.

```
<Switch> display smart-link group 1
Smart link group 1 information:
  Device ID       : 0011-2200-0001
  Preemption mode : None
  Preemption delay: 1(s)
  Control VLAN    : 1
  Protected VLAN  : Reference Instance 2, 4

  Member                  Role      State    Flush-count     Last-flush-time
  ------------------------------------------------------------------------------
  GE1/0/1                 PRIMARY   ACTIVE   1               16:45:20 2012/04/21
  GE1/0/2                 SECONDARY STANDBY  2               16:37:20 2012/04/21
```

Table 5-2 Command output

Field	Description
Preemption mode	Preemption mode: • **None**—Preemption disabled. • **Role**—Role preemption mode. • **Speed**—**Speed preemption mode.**
Preemption delay	Preemption delaytime, in seconds.
Control-VLAN	Control VLAN ID.
Protected VLAN	Protected VLANs of the smart link group. Referenced Multiple Spanning Tree Instances (MSTIs) are displayed. To view the VLANs mapped to the referenced MSTIs, use the **display stp region-configuration** command.
Member	Member port of the smart link group.
Role	Port role: primary or secondary.
State	Port state: active, down, or standby.
Flush-count	Number of transmitted flush messages.
Last-flush-time	Time when the last flush message was transmitted (NA indicates that no flush message has been transmitted).

5.1.3. flush enable

Use **flush enable** to enable flush update.

Use **undo flush enable** to disable flush update.

Syntax

flush enable [**control-vlan** *vlan-id*]

undo flush enable

Default

Flush update is enabled for smart link groups, and VLAN 1 is used for flush message transmission.

Views

Smart link group view

Predefined user roles

network-admin

Parameters

control-vlan *vlan-id*: Specifies the control VLAN used for transmitting flush messages. The *vlan-id* argument represents the control VLAN ID and is in the range of 1 to 4094.

Usage guidelines

You must configure different control VLANs for different smart link groups.

- Make sure the configured control VLAN already exists, and assign the smart link group member ports to the control VLAN.
- The control VLAN of a smart link group must also be one of its protected VLANs. Do not remove the control VLAN. Otherwise, flush messages cannot be sent correctly.

Examples

Disable flush update for smart link group 1.

```
<Switch> system-view
[Switch] smart-link group 1
[Switch-smlk-group1] undo flush enable
```

Related commands

smart-link flush enable

5.1.4. port

Use **port** to assign a port to a smart link group and specify the port role.

Use **undo port** to remove a port from a smart link group.

Syntax

port *interface-type interface-number* { **primary** | **secondary** }

undo port *interface-type interface-number*

Default

No member ports exist in a smart link group.

Views

Smart link group view

Predefined user roles

network-admin

Parameters

interface-type interface-number: Specifies a port by its type and number, which can be a Layer 2 Ethernet interface or Layer 2 aggregate interface.

primary: Specifies a port as the primary port.

secondary: Specifies a port as the secondary port.

Usage guidelines

Before configuring member ports for a smart link group, you must configure protected VLANs for the smart link group.

Disable the spanning tree feature, and RRPP on the ports you want to add to the smart link group. You cannot enable the spanning tree feature, or RRPP on a smart link group member port.

If you configure a port as both an aggregation group member and a smart link group member, only the aggregation group member configuration takes effect. The port is not shown in the output from the **display smart-link group** command. The smart link group member configuration takes effect after the port leaves the aggregation group.

You can also assign a port to a smart link group by using the **port smart-link group** command in interface view.

Examples

Configure GigabitEthernet 1/0/1 as the secondary port of smart link group 1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] undo stp enable
[Switch-GigabitEthernet1/0/1] quit
[Switch] smart-link group 1
[Switch-smlk-group1] protected-vlan reference-instance 0
[Switch-smlk-group1] port gigabitethernet 1/0/1 secondary
```

Related commands

port smart-link group

5.1.5. port smart-link group

Use **port smart-link group** to assign a port to a smart link group and specify the port role.

Use **undo port smart-link group** to remove a port from a smart link group.

Syntax

port smart-link group *group-id* { **primary** | **secondary** }

undo port smart-link group *group-id*

Default

A port is not a smart link group member.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

group-id: Specifies a smart link group by its ID. The value range for this argument is 1 to 48.

primary: Specifies the port as the primary port.

secondary: Specifies the port as the secondary port.

Usage guidelines

Before configuring member ports for a smart link group, you must configure protected VLANs for the smart link group.

Disable the spanning tree feature, and RRPP on the ports you want to add to the smart link group. You cannot enable the spanning tree feature, or RRPP on a smart link group member port.

If you configure a port as both an aggregation group member and a smart link group member, only the aggregation group member configuration takes effect. The port is not shown in the output from the **display smart-link group** command. The smart link group member configuration takes effect after the port leaves the aggregation group.

You can assign a port to a smart link group by using the **port** command in smart link group view.

Examples

Configure GigabitEthernet 1/0/1 as the primary port of smart link group 1.

```
<Switch> system-view
[Switch] smart-link group 1
[Switch-smlk-group1] protected-vlan reference-instance 0
[Switch-smlk-group1] quit
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] undo stp enable
[Switch-GigabitEthernet1/0/1] port smart-link group 1 primary
```

Configure Layer 2 aggregate interface 1 as the primary port of smart link group 1.

```
<Switch> system-view
[Switch] smart-link group 1
[Switch-smlk-group1] protected-vlan reference-instance 0
[Switch-smlk-group1] quit
[Switch] interface bridge-aggregation 1
[Switch-Bridge-Aggregation1] undo stp enable
[Switch-Bridge-Aggregation1] port smart-link group 1 primary
```

Related commands

port

5.1.6. port smart-link group track

Use **port smart-link group track** to configure the collaboration between a smart link group member port and a track entry.

Use **undo port smart-link group track** to remove the collaboration between a smart link group member port and a track entry.

Syntax

port smart-link group *group-id* **track** *track-entry-number*

undo port smart-link group *group-id* **track** *track-entry-number*

Default

Smart link group member ports do not collaborate with track entries.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

group-id: Specifies a smart link group by its ID. The value range for this argument is 1 to 48.

track-entry-number: Specifies the ID of a track entry that has been associated with the CC function of CFD.

Usage guidelines

Smart Link collaborates with link detection protocols through track entries. It supports only the CC function of CFD to implement link detection. To associate the CC function of CFD with a track entry, use the **track cfd** command.

Before configuring the collaboration between Smart Link and Track on a port, make sure the port has been added to the specified smart link group.

Examples

Configure the collaboration between GigabitEthernet 1/0/1, the primary port of smart link group 1, and the CC function of CFD through track entry 1 to detect the link status.

```
<Switch> system-view
[Switch] track 1 cfd cc service-instance 100 mep 2
[Switch-track-1] quit
[Switch] smart-link group 1
[Switch-smlk-group1] protected-vlan reference-instance 0
[Switch-smlk-group1] quit
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] undo stp enable
[Switch-GigabitEthernet1/0/1] port smart-link group 1 primary
[Switch-GigabitEthernet1/0/1] port smart-link group 1 track 1
```

Configure the collaboration between bridge-aggregation 1, the primary port of smart link group 1, and the CC function of CFD through track entry 1 to detect the link status.

```
<Switch> system-view
[Switch] track 1 cfd cc service-instance 100 mep 2
[Switch-track-1] quit
[Switch] smart-link group 1
[Switch-smlk-group1] protected-vlan reference-instance 0
[Switch-smlk-group1] quit
```

```
[Switch] interface bridge-aggregation 1
[Switch-Bridge-Aggregation1] undo stp enable
[Switch-Bridge-Aggregation1] port smart-link group 1 primary
[Switch-Bridge-Aggregation1] port smart-link group 1 track 1
```

Related commands

track cfd

5.1.7. preemption delay

Use **preemption delay** to set the preemption delay.

Use **undo preemption delay** to restore the default.

Syntax

preemption delay *delay*

undo preemption delay

Default

The preemption delay is 1 second.

Views

Smart link group view

Predefined user roles

network-admin

Parameters

delay: Specifies the preemption delay in the range of 0 to 300 seconds.

Usage guidelines

Preemption delay is the period of time that the primary port waits before taking over to collaborate with the switchover of upstream devices.

The preemption delay configuration takes effect only after a preemption mode is configured.

Examples

Enable role preemption and set the preemption delay to 10 seconds.

```
<Switch> system-view
[Switch] smart-link group 1
[Switch-smlk-group1] preemption mode role
[Switch-smlk-group1] preemption delay 10
```

Related commands

preemption mode

5.1.8. preemption mode

Use **preemption mode** to configure a preemption mode for a smart link group.

Use **undo preemption mode** to restore the default.

Syntax

preemption mode role

undo preemption mode

Default

No preemption mode is configured for a smart link group.

Views

Smart link group view

Predefined user roles

network-admin

Parameters

role: Specifies the role preemption mode, which enables the primary port to transition to forwarding state after the primary link recovers.

Examples

Configure the role preemption mode.

```
<Switch> system-view
[Switch] smart-link group 1
[Switch-smlk-group1] preemption mode role
```

5.1.9. protected-vlan

Use **protected-vlan** to configure protected VLANs for a smart link group.

Use **undo protected-vlan** to remove the protected VLAN of a smart link group.

Syntax

protected-vlan reference-instance *instance-id-list*

undo protected-vlan [**reference-instance** *instance-id-list*]

Default

A smart link group does not have protected VLANs.

Views

Smart link group view

Predefined user roles

network-admin

Parameters

reference-instance *instance-id-list*: Specifies a protected VLANs.

- When the spanning tree mode is MSTP, the *instance-id-list* argument is space-separated list of up to 10 MSTI items. Each item specifies an MSTI ID or a range of MSTI IDs in the form of *instance-id 1* **to** *instance-id 2*. The value range for MSTI IDs is 0 to 4094. 0 represents the common internal spanning tree (CIST). The *instance-id 2* must be equal to or greater than *instance-id 1*. You can use the **display stp region-configuration** command to display instance-to-VLAN mappings.
- When the spanning tree mode is PVST, the instance-id-list argument is a space-separated list of up to 10 VLAN items. Each item specifies a VLAN ID or a range of VLAN IDs in the form of instance-id 1 to instance-id 2. The value range for VLAN IDs is 1 to 4094.

Usage guidelines

You must configure all VLANs to which the member ports of a smart link group belongs as protected VLANs.

If the VLAN-to-MSTI mappings change, the protected VLANs change.

To remove protected VLAN configuration, follow these restrictions and guidelines:

- In MSTP mode, if you specify the **reference-instance** *instance-id-list* option, the **undo protected-vlan** command removes configuration of VLANs mapped to the specified MSTIs. If you do not specify the **reference-instance** *instance-id-list* option, the command removes configuration of all protected VLANs.
- In PVST mode, if you specify the **reference-instance** *instance-id-list* option, the **undo protected-vlan** command removes configuration of the specified VLANs. If you do not specify the **reference-instance** *instance-id-list* option, the command removes configuration of all protected VLANs.
- If a smart link group has member ports, you cannot remove protected VLAN configuration. If a smart link group does not have member ports, you can remove protected VLAN configuration.

Examples

Map VLANs 1 through 30 to MSTI 1, and activate the MST region configuration. Configure the VLANs mapped to MSTI 1 as the protected VLANs of smart link group 1.

```
<Switch> system-view
[Switch] stp region-configuration
[Switch-mst-region] instance 1 vlan 1 to 30
[Switch-mst-region] active region-configuration
[Switch-mst-region] quit
[Switch] smart-link group 1
[Switch-smlk-group1] protected-vlan reference-instance 1
```

Related commands

display stp region-configuration (*Layer 2—LAN Switching Command Reference*)

smart-link group

5.1.10. reset smart-link statistics

Use **reset smart-link statistics** to clear statistics about flush messages.

Syntax

reset smart-link statistics

Views

User view

Predefined user roles

network-admin

Examples

Clear statistics about flush messages.

```
<Switch> reset smart-link statistics
```

Related commands

display smart-link flush

5.1.11. smart-link flush enable

Use **smart-link flush enable** to enable flush message receiving.

Use **undo smart-link flush enable** to disable flush message receiving.

Syntax

smart-link flush enable [**control-vlan** *vlan-id-list*]

undo smart-link flush enable [**control-vlan** *vlan-id-list*]

Default

Flush message receiving is disabled.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

control-vlan *vlan-id-list*: Specifies a space-separated list of up to 10 control VLAN items. Each item specifies a control VLAN ID or a range of control VLAN IDs in the form of *vlan-id1* **to** *vlan-id2*. The value range for the *vlan-id* argument is 1 to 4094. The *vlan-id2* must be equal to or greater than *vlan-id1*. The default value for the *vlan-id-list* argument is 1.

Examples

Enable GigabitEthernet 1/0/1 to receive flush messages.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] smart-link flush enable
```

Enable Layer 2 aggregate interface 1 to receive flush messages.

```
<Switch> system-view
[Switch] interface bridge-aggregation 1
[Switch-Bridge-Aggregation1] smart-link flush enable
```

Related commands

flush enable

5.1.12. smart-link group

Use **smart-link group** to create a smart link group and enter its view, or enter the view of an existing smart link group.

Use **undo smart-link group** to remove a smart link group.

Syntax

smart-link group *group-id*

undo smart-link group *group-id*

Default

No smart link groups exist.

Views

System view

Predefined user roles

network-admin

Parameters

group-id: Specifies a smart link group ID. The value range for this argument is 1 to 48.

Usage guidelines

You cannot remove a smart link group with member ports.

Examples

Create smart link group 1 and enter its view.

```
<Switch> system-view
[Switch] smart-link group 1
[Switch-smlk-group1]
```

Contents

A page of this section is **10-x-x**

6. Monitor Link commands 6-1
6.1. Monitor Link commands 6-1
6.1.1. display monitor-link group 6-1
6.1.2. monitor-link group 6-2
6.1.3. port 6-3
6.1.4. port monitor-link group 6-3

6. Monitor Link commands

6.1. Monitor Link commands

6.1.1. display monitor-link group

Use **display monitor-link group** to display information about monitor link groups.

Syntax

display monitor-link group { *group-id* | **all** }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

group-id: Specifies a monitor link group by its ID. The value range for the *group-id* argument is 1 to 16.

all: Specifies all monitor link groups.

Usage guidelines

This command does not display information about ports that belong to a link aggregation group.

Examples

Display information about all monitor link groups.

```
<Switch> display monitor-link group all
Monitor link protocol status: Disabled
Monitor link group 1 information:
  Group status     : N/A
  Downlink up-delay: 0(s)
  Last-up-time     : -
  Last-down-time   : -
  Up-port-threshold: 1

  Member                    Role       Status
  ------------------------------------------
  GE1/0/1                   UPLINK     UP
  GE1/0/2                   DOWNLINK   UP
```

Table 6-1 Command output

Field	Description
Monitor link protocol status	Whether Monitor Link is enabled: • Enabled. • Disabled.

Field	Description
Group status	Monitor link group status: • **DOWN**. • **UP**. • **N/A**—Monitor Link is disabled globally. The monitor link group does not operate.
Downlink up-delay	Switchover delay of the downlink interfaces in the monitor link group, in seconds.
Last-up-time	Last time when the monitor link group came up.
Last-down-time	Last time when the monitor link group went down.
Up-port-threshold	Uplink interface threshold for triggering monitor link group state switchover.
Member	Member interfaces of the monitor link group.
Role	Interface role, which can be uplink interface or downlink interface.
Status	Member interface state, which can be up or down.

6.1.2. monitor-link group

Use **monitor-link group** to create a monitor link group and enter its view, or enter the view of an existing monitor link group.

Use **undo monitor-link group** to remove a monitor link group.

Syntax

monitor-link group *group-id*

undo monitor-link group *group-id*

Default

No monitor link groups exist.

Views

System view

Predefined user roles

network-admin

Parameters

group-id: Specifies a monitor link group ID. The value range for the *group-id* argument is 1 to 16.

Examples

Create monitor link group 1 and enter its view.

```
<Switch> system-view
[Switch] monitor-link group 1
[Switch-mtlk-group1]
```

6.1.3. port

Use **port** to assign an interface to a monitor link group.

Use **undo port** to remove an interface from a monitor link group.

Syntax

port *interface-type interface-number* { **downlink** | **uplink** }

undo port *interface-type interface-number*

Default

No member interfaces exist in a monitor link group.

Views

Monitor link group view

Predefined user roles

network-admin

Parameters

interface-type: Specifies an interface by its type.

interface-number: Specifies an interface by its number.

downlink: Specifies a downlink interface.

uplink: Specifies an uplink interface.

Usage guidelines

You can assign an interface to only one monitor link group.

You can also assign an interface to a monitor link group by using the **port monitor-link group** command in interface view.

If you have configured a Selected port of an aggregation group as the downlink interface of a monitor link group, do not configure an Unselected port of the aggregation group as the uplink interface of the monitor link group.

Do not assign an aggregate interface and member ports of the aggregate group to the same monitor link group.

Examples

Configure GigabitEthernet 1/0/1 as an uplink interface and GigabitEthernet 1/0/2 as a downlink interface for monitor link group 1.

```
<Switch> system-view
[Switch] monitor-link group 1
[Switch-mtlk-group1] port gigabitethernet 1/0/1 uplink
[Switch-mtlk-group1] port gigabitethernet 1/0/2 downlink
```

Related commands

port monitor-link group

6.1.4. port monitor-link group

Use **port monitor-link group** to assign an interface to a monitor link group.

Use **undo port monitor-link group** to remove an interface from a monitor link group.

Syntax

port monitor-link group *group-id* { **downlink** | **uplink** }

undo port monitor-link group *group-id*

Default

An interface is not a monitor link group member.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

group-id: Specifies a monitor link group by its ID. The value range for the *group-id* argument is 1 to 16.

downlink: Specifies a downlink interface.

uplink: Specifies an uplink interface.

Usage guidelines

You can assign an interface to only one monitor link group.

You can also assign an interface to a monitor link group by using the **port** command in monitor link group view.

If you have configured a Selected port of an aggregation group as the downlink interface of a monitor link group, do not configure an Unselected port of the aggregation group as the uplink interface of the monitor link group.

Do not assign an aggregate interface and member ports of the aggregate group to the same monitor link group.

Examples

Configure GigabitEthernet 1/0/1 as an uplink interface and GigabitEthernet 1/0/2 as a downlink interface for monitor link group 1.

```
<Switch> system-view
[Switch] monitor-link group 1
[Switch-mtlk-group1] quit
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port monitor-link group 1 uplink
[Switch-GigabitEthernet1/0/1] quit
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port monitor-link group 1 downlink
```

Related commands

port

Contents

A page of this section is **10-x-x**

7. VRRP commands 7-1
7.1. IPv4 VRRP commands 7-1
7.1.1. display vrrp 7-1
7.1.2. display vrrp statistics 7-4
7.1.3. reset vrrp statistics 7-6
7.1.4. snmp-agent trap enable vrrp 7-7
7.1.5. vrrp check-ttl enable 7-8
7.1.6. vrrp dscp 7-8
7.1.7. vrrp state-transition-delay 7-9
7.1.8. vrrp version 7-10
7.1.9. vrrp vrid 7-10
7.1.10. vrrp vrid authentication-mode 7-11
7.1.11. vrrp vrid preempt-mode 7-13
7.1.12. vrrp vrid priority 7-14
7.1.13. vrrp vrid timer advertise 7-15
7.1.14. vrrp vrid track 7-16
7.2. IPv6 VRRP commands 7-17
7.2.1. display vrrp ipv6 7-17
7.2.2. display vrrp ipv6 statistics 7-21
7.2.3. reset vrrp ipv6 statistics 7-22
7.2.4. vrrp ipv6 dscp 7-23
7.2.5. vrrp ipv6 state-transition-delay 7-24
7.2.6. vrrp ipv6 vrid 7-25
7.2.7. vrrp ipv6 vrid preempt-mode 7-26
7.2.8. vrrp ipv6 vrid priority 7-27
7.2.9. vrrp ipv6 vrid timer advertise 7-27
7.2.10. vrrp ipv6 vrid track 7-28

7. VRRP commands

VRRP does not take effect on member ports of aggregation groups.

7.1. IPv4 VRRP commands

7.1.1. display vrrp

Use **display vrrp** to display the states of IPv4 VRRP groups.

Syntax

display vrrp [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number.

vrid *virtual-router-id*: Specifies an IPv4 VRRP group by its virtual router ID in the range of 1 to 255.

verbose: Displays detailed IPv4 VRRP group information. If you do not specify the **verbose** keyword, the command displays brief IPv4 VRRP group information.

Usage guidelines

If no interface or VRRP group is specified, this command displays the states of all IPv4 VRRP groups.

If only an interface is specified, this command displays the states of all IPv4 VRRP groups on the specified interface.

If both an interface and an IPv4 VRRP group are specified, this command displays the states of the specified IPv4 VRRP group on the specified interface.

Examples

Display brief information about all IPv4 VRRP groups on the device when VRRP operates in standard mode.

```
<Switch> display vrrp
IPv4 Virtual Router Information:
 Running Mode      : Standard
 Gratuitous ARP sending interval : 120 sec
 Total number of virtual routers : 1
 Interface          VRID  State        Running Adver   Auth     Virtual
                                        Pri     Timer   Type        IP
 ------------------------------------------------------------------------
```

```
Vlan2              1      Master       150      100      Simple    1.1.1.1
```

Table 7-1 Command output (in standard mode)

Field	Description
Running Mode	VRRP operating mode (standard mode).
Gratuitous ARP sending interval	Sending interval for gratuitous ARP packets.
Total number of virtual routers	Total number of VRRP groups.
Interface	Interface where the VRRP group is configured.
VRID	Virtual router ID (VRRP group number).
State	State of the router in the VRRP group: • **Master**—The router is the master in the VRRP group. • **Backup**—The router is the backup in the VRRP group. • **Initialize**—The router is in **Initialize** state. • **Inactive**—The router is in **Inactive** state, for example, when the router is not assigned a virtual IP address by using the **vrrp vrid** command.
Running Pri	Current priority of the router. When a track entry is associated with a VRRP group on the router, the router's priority changes when the track entry's status changes.
Adver Timer	VRRP advertisement sending interval in centiseconds.
Auth Type	Authentication type: • **None**—No authentication. • **Simple**—Simple text authentication. • **MD5**—MD5 authentication.
Virtual IP	Virtual IP address of the VRRP group.

Display detailed information about all IPv4 VRRP groups on the device when VRRP operates in standard mode.

```
<Switch> display vrrp verbose
IPv4 Virtual Router Information:
 Running Mode      : Standard
 Gratuitous ARP sending interval : 120 sec
 Total number of virtual routers : 2
   Interface Vlan-interface2
     VRID              : 1                  Adver Timer   : 100
     Admin Status      : Up                 State         : Master
     Config Pri        : 150                Running Pri   : 150
     Preempt Mode      : Yes                Delay Time    : 5
     Auth Type         : Simple             Key           : ******
     Virtual IP        : 1.1.1.1
     Virtual MAC       : 0000-5e00-0101
     Master IP         : 1.1.1.2
     Config Role       : Master
     Name              : abc
```

```
VRRP Track Information:
  Track Object    : 1                    State : Positive    Pri Reduced : 50

Interface Vlan-interface2
  VRID             : 2                    Adver Timer   : 100
  Admin Status     : Up                   State         : Backup
  Config Pri       : 80                   Running Pri   : 80
  Preempt Mode     : Yes                  Delay Time    : 0
  Become Master    : 2370ms left
  Auth Type        : None
  Virtual IP       : 1.1.1.11
  Virtual MAC      : 0000-5e00-0102
  Master IP        : 1.1.1.12

Interface Vlan-interface2
  VRID             : 3                    Adver Timer : 100
  Admin Status     : Up                   State       : Master
  Config Pri       : 100                  Running Pri : 100
  Preempt Mode     : Yes                  Delay Time  : 0
  Auth Type        : None
  Pkt Sending Mode : v2-only
  Virtual IP       : 1.1.1.10
  Virtual MAC      : 0000-5e00-0103
  Master IP        : 1.1.1.2
  Config Role      : Subordinate
  Follow Name      : abc
```

Table 7-2 Command output (in standard mode)

Field	Description
Running Mode	VRRP operating mode (standard mode).
Gratuitous ARP sending interval	Sending interval for gratuitous ARP packets.
Total number of virtual routers	Total number of VRRP groups.
Interface	Interface where the VRRP group is configured.
VRID	Virtual router ID (VRRP group number).
Adver Timer	VRRP advertisement sending interval in centiseconds.
Admin Status	Administrative status: **Up** or **Down**.
State	State of the router in the VRRP group: • **Master**—The router is the master in the VRRP group. • **Backup**—The router is the backup in the VRRP group. • **Initialize**—The router is in **Initialize** state. • **Inactive**—The router is in **Inactive** state, for example, when the router is not assigned a virtual IP address by using the **vrrp vrid** command.
Config Pri	Configured priority of the router, which is configured by using

Field	Description
	the **vrrp vrid priority** command.
Running Pri	Current priority of the router. When a track entry is associated with a VRRP group on the router, the router's priority changes when the track entry's status changes.
Preempt Mode	Preemptive mode: • **Yes**. • **No**.
Delay Time	Preemption delay in centiseconds.
Become Master	Time (in milliseconds) that a backup router has to wait before it becomes the master. This field is displayed only when the router is a backup.
Auth Type	Authentication type: • **None**—No authentication. • **Simple**—Simple text authentication. • **MD5**—MD5 authentication.
Key	Authentication key, which is not displayed if no authentication is required.
Virtual IP	Virtual IP address of the VRRP group.
Virtual MAC	Virtual MAC address of the VRRP group's virtual IP address, which is displayed when the router is the master.
Master IP	Primary IP address of the interface where the master resides.
Config Role	The configured role of the VRRP group to which the router belongs. • **Master**. • **Subordinate**.
Name	Master group name assigned to the VRRP group.
Follow Name	Name of the master VRRP group that the VRRP group follows.
VRRP Track Information	Track entry information. This field is displayed only after you configure the **vrrp vrid track** command.
Track Object	Track entry which is associated with the VRRP group.
State	Track entry state: • **Negative**. • **Positive**. • **NotReady**.
Pri Reduced	Value by which the priority decreases when the status of the associated track entry changes to the Negative state.
Switchover	Switchover mode. When the status of the associated track entry changes to the Negative state, the backup immediately becomes the master.

7.1.2. display vrrp statistics

Use **display vrrp statistics** to display statistics for IPv4 VRRP groups.

Syntax

display vrrp statistics [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number.

vrid *virtual-router-id*: Specifies an IPv4 VRRP group by its virtual router ID in the range of 1 to 255.

Usage guidelines

If no interface or VRRP group is specified, this command displays statistics for all IPv4 VRRP groups.

If only an interface is specified, this command displays statistics for all IPv4 VRRP groups on the specified interface.

If both an interface and an IPv4 VRRP group are specified, this command displays statistics for the specified IPv4 VRRP group on the specified interface.

Examples

Display statistics for all IPv4 VRRP groups when VRRP operates in standard mode.

```
<Switch> display vrrp statistics
 Interface               : Vlan-interface2
 VRID                    : 1
 CheckSum Errors         : 0          Version Errors               : 0
 Invalid Pkts Rcvd  :      0          Unexpected Pkts Rcvd         : 0
 IP TTL Errors           : 0          Advertisement Interval Errors : 0
 Invalid Auth Type       : 0          Auth Failures                : 0
 Packet Length Errors    : 0          Auth Type Mismatch           : 0
 Become Master           : 1          Address List Errors          : 0
 Adver Rcvd              : 0          Priority Zero Pkts Rcvd      : 0
 Adver Sent              : 807        Priority Zero Pkts Sent      : 0
IP Owner Conflicts      : 0

 Global statistics
 CheckSum Errors         : 0
 Version Errors          : 0
 VRID Errors             : 0
```

Table 7-3 Command output (in standard mode)

Field	Description
Interface	Interface where the VRRP group is configured.
VRID	VRRP group number.

Field	Description
CheckSum Errors	Number of packets with checksum errors.
Version Errors	Number of packets with version errors.
Invalid Pkts Rcvd	Number of received packets of invalid packet types.
Unexpected Pkts Rcvd	Number of received unexpected packets.
Advertisement Interval Errors	Number of packets with advertisement interval errors.
IP TTL Errors	Number of packets with TTL errors.
Auth Failures	Number of packets with authentication failures.
Invalid Auth Type	Number of packets with authentication failures because of invalid authentication types.
Auth Type Mismatch	Number of packets with authentication failures because of mismatching authentication types.
Packet Length Errors	Number of packets with VRRP packet length errors.
Address List Errors	Number of packets with virtual IP address list errors.
Become Master	Number of times that the router has been elected as the master.
Priority Zero Pkts Rcvd	Number of received advertisements with the router priority of 0.
Adver Rcvd	Number of received advertisements.
Priority Zero Pkts Sent	Number of sent advertisements with the router priority of 0.
Adver Sent	Number of sent advertisements.
IP Owner Conflicts	Number of VRRP packets that the local router (IP address owner) has received from conflicting IP address owners.
Global statistics	Global statistics for all VRRP groups.
CheckSum Errors	Total number of packets with checksum errors.
Version Errors	Total number of packets with version errors.
VRID Errors	Total number of packets with VRID errors.

Related commands

reset vrrp statistics

7.1.3. reset vrrp statistics

Use **reset vrrp statistics** to clear statistics for IPv4 VRRP groups.

Syntax

reset vrrp statistics [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]]

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number.

vrid *virtual-router-id*: Specifies an IPv4 VRRP group by its virtual router ID in the range of 1 to 255.

Usage guidelines

If no interface or VRRP group is specified, this command clears statistics for all IPv4 VRRP groups.

If only an interface is specified, this command clears statistics for all IPv4 VRRP groups on the specified interface.

If both an interface and an IPv4 VRRP group are specified, this command clears statistics for the specified IPv4 VRRP group on the specified interface.

Examples

Clear statistics for all IPv4 VRRP groups on all interfaces.

```
<Switch> reset vrrp statistics
```

Related commands

display vrrp statistics

7.1.4. snmp-agent trap enable vrrp

Use **snmp-agent trap enable vrrp** to enable SNMP notifications for VRRP.

Use **undo snmp-agent trap enable vrrp** to disable SNMP notifications for VRRP.

Syntax

snmp-agent trap enable vrrp [**auth-failure** | **new-master**]

undo snmp-agent trap enable vrrp [**auth-failure** | **new-master**]

Default

SNMP notifications for VRRP are enabled.

Views

System view

Predefined user roles

network-admin

Parameters

auth-failure: Generates notifications as defined in RFC 2787 when the device in a VRRP group receives a VRRP advertisement with the authentication type or key not matching the local configuration.

new-master: Generates notifications as defined in RFC 2787 when the state of a device in a VRRP group changes from Initialize or Backup to Master.

Usage guidelines

To report critical VRRP events to an NMS, enable SNMP notifications for VRRP. For VRRP event notifications to be sent correctly, you must also configure SNMP on the device. For more information

about SNMP configuration, see the network management and monitoring configuration guide for the device.

Examples

Generate notifications as defined in RFC 2787 when the device in a VRRP group receives a VRRP advertisement with the authentication type or key not matching the local configuration.

```
<Switch> system-view
[Switch] snmp-agent trap enable vrrp auth-failure
```

7.1.5. vrrp check-ttl enable

Use **vrrp check-ttl enable** to enable TTL check for IPv4 VRRP packets.

Use **undo vrrp check-ttl enable** to disable TTL check for IPv4 VRRP packets.

Syntax

vrrp check-ttl enable

undo vrrp check-ttl enable

Default

TTL check for IPv4 VRRP packets is enabled.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

The master in an IPv4 VRRP group periodically sends VRRP advertisements to declare its presence. The VRRP advertisements are multicast in the local subnet and cannot be forwarded by routers, so the TTL value is not changed. When the master sends VRRP advertisements, it sets the TTL value to 255. If you enable TTL check, the backups drop the VRRP advertisements with TTL other than 255, preventing attacks from other subnets.

Devices from different vendors might implement VRRP differently. When the device is interoperating with devices of other vendors, TTL check on VRRP packets might result in unexpected dropping of packets. In this scenario, use the **undo vrrp check-ttl enable** command to disable TTL check on VRRP packets.

Examples

Disable TTL check for IPv4 VRRP packets.

```
<Switch> system-view
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] undo vrrp check-ttl enable
```

7.1.6. vrrp dscp

Use **vrrp dscp** to set a DSCP value for VRRP packets.

Use **undo vrrp dscp** to restore the default.

Syntax

vrrp dscp *dscp-value*

undo vrrp dscp

Default

The DSCP value for VRRP packets is 48.

Views

System view

Predefined user roles

network-admin

Parameters

dscp-value: Specifies a DSCP value for VRRP packets, in the range of 0 to 63.

Usage guidelines

The DSCP value identifies the packet priority during transmission. A greater DSCP value means a higher packet priority.

Examples

Set the DSCP value to 30 for VRRP packets.

```
<Switch> system-view
[Switch] vrrp dscp 30
```

7.1.7. vrrp state-transition-delay

Use **vrrp state-transition-delay** to set the delay time for the IPv4 VRRP group to transition from **Initialize** to **Master** or **Backup** state.

Use **undo vrrp state-transition-delay** to restore the default.

Syntax

vrrp state-transition-delay *delay-value*

undo vrrp state-transition-delay

Default

The delay time is 0 seconds for the IPv4 VRRP group to transition from **Initialize** to **Master** or **Backup** state.

Views

Interface view

Predefined user roles

network-admin

Parameters

delay-value: Specifies delay time for the IPv4 VRRP group to transition from **Initialize** to **Master** or **Backup** state, in the range of 0 to 60 seconds.

Usage guidelines

Typically, an IPv4 VRRP group immediately transitions from **Initialize** to **Master** or **Backup** state when the interface where the IPv4 VRRP group resides comes up. If the device restarts or the interface state changes frequently, the IPv4 VRRP group state might be unstable, and the VRRP group operation might be affected. After you configure this command, a state transition delay timer is started when the interface comes up. If the interface goes down before the timer expires, the timer is stopped, and the IPv4 VRRP group stays in **Initialize** state. The timer is restarted when the interface

comes up again. When the timer expires, the IPv4 VRRP group transitions from **Initialize** to **Master** or **Backup** state.

Examples

On VLAN-interface 2, set the delay time to 5 seconds for the IPv4 VRRP group to transition from **Initialize** to **Master** or **Backup** state.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp state-transition-delay 5
```

7.1.8. vrrp version

Use **vrrp version** to specify the version of IPv4 VRRP on an interface.

Use **undo vrrp version** to restore the default.

Syntax

vrrp version *version-number*

undo vrrp version

Default

VRRPv3 is used.

Views

Interface view

Predefined user roles

network-admin

Parameters

version-number: Specifies a VRRP version. The version number is 2 or 3, where 2 indicates VRRPv2 (described in RFC 3768), and 3 indicates VRRPv3 (described in RFC 5798).

Usage guidelines

The version of VRRP on all routers in an IPv4 VRRP group must be the same.

Examples

Specify VRRPv2 to run on VLAN-interface 10.

```
<Switch> system-view
[Switch] interface vlan-interface 10
[Switch-Vlan-interface10] vrrp version 2
```

7.1.9. vrrp vrid

Use **vrrp vrid** to create an IPv4 VRRP group and assign a virtual IP address to it, or to assign a virtual IP address to an existing IPv4 VRRP group.

Use **undo vrrp vrid** to remove all configurations of an IPv4 VRRP group, or to remove a virtual IP address from an IPv4 VRRP group.

Syntax

vrrp vrid *virtual-router-id* **virtual-ip** *virtual-address*

undo vrrp vrid *virtual-router-id* [**virtual-ip** [*virtual-address*]]

Default

No IPv4 VRRP groups exist.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv4 VRRP group by its virtual router ID in the range of 1 to 255.

virtual-ip *virtual-address*: Specifies a virtual IP address. You cannot specify the virtual IP address as any of the following IP addresses:

- All-zero address (0.0.0.0).
- Broadcast address (255.255.255.255).
- Loopback address.
- IP address of other than Class A, Class B, and Class C.
- Invalid IP address (for example, 0.0.0.1).

If you do not specify the *virtual-address* argument, the **undo vrrp vrid** command removes all virtual IP addresses from the specified IPv4 VRRP group.

Usage guidelines

You can execute this command multiple times to assign multiple virtual IP addresses to an IPv4 VRRP group. An IPv4 VRRP group can have a maximum of 16 virtual IP addresses.

An IPv4 VRRP group without virtual IP addresses configured can exist on a device provided that other settings (for example, priority and preemption mode) are available. Such a VRRP group stays in inactive state and does not function.

The virtual IP address of an IPv4 VRRP group and the downlink interface IP addresses of the VRRP group members must be in the same subnet. Otherwise, the hosts in the subnet might fail to access external networks.

Examples

Create IPv4 VRRP group 1 and assign virtual IP address 10.10.10.10 to the VRRP group. Then assign virtual IP address 10.10.10.11 to the VRRP group.

```
<Switch> system-view
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] vrrp vrid 1 virtual-ip 10.10.10.10
[Switch-Vlan-interface2] vrrp vrid 1 virtual-ip 10.10.10.11
```

Related commands

display vrrp

7.1.10. vrrp vrid authentication-mode

Use **vrrp vrid authentication-mode** to configure the authentication mode and the authentication key for an IPv4 VRRP group to send and receive VRRP packets.

Use **undo vrrp vrid authentication-mode** to restore the default.

Syntax

vrrp vrid *virtual-router-id* **authentication-mode** { **md5** | **simple** } { **cipher** | **plain** } *string*

undo vrrp vrid *virtual-router-id* **authentication-mode**

Default

Authentication is disabled when a VRRP group sends and receives VRRP packets.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv4 VRRP group by its virtual router ID in the range of 1 to 255.

md5: Specifies the MD5 authentication mode.

simple: Specifies the simple authentication mode.

cipher: Specifies a key in encrypted form.

plain: Specifies a key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. Its plaintext form is a case-sensitive string of 1 to 8 characters. Its encrypted form is a case-sensitive string of 1 to 41 characters.

Usage guidelines

To avoid attacks from unauthorized users, VRRP member routers add authentication keys in VRRP packets to authenticate one another. VRRP provides the following authentication modes:

- **simple**—Simple text authentication.

  The sender fills an authentication key into the VRRP packet, and the receiver compares the received authentication key with its local authentication key. If the two authentication keys are the same, the received VRRP packet is legitimate. Otherwise, the received packet is illegitimate.
- **md5**—MD5 authentication.

  The sender computes a digest for the VRRP packet by using the authentication key and MD5 algorithm, and saves the result to the authentication header. The receiver performs the same operation by using the authentication key and MD5 algorithm, and it compares the result with the content in the authentication header. If the results are the same, the received VRRP packet is legitimate. Otherwise, the received packet is illegitimate.

The MD5 authentication is more secure than the simple text authentication, but it costs more resources.

IMPORTANT:

- You can configure different authentication modes and authentication keys for the VRRP groups on an interface. However, members of the same VRRP group must use the same authentication mode and authentication key.
- For VRRPv3, this command does not take effect because VRRPv3 does not support authentication.

Examples

Set the authentication mode to **simple** and the authentication key to **Sysname** for VRRP group 1 on VLAN-interface 2.

```
<Switch> system-view
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] vrrp vrid 1 authentication-mode simple plain Sysname
```

Related commands

display vrrp

vrrp version

7.1.11. vrrp vrid preempt-mode

Use **vrrp vrid preempt-mode** to enable the preemptive mode for the device in an IPv4 VRRP group and set the preemption delay.

Use **undo vrrp vrid preempt-mode** to disable the preemptive mode for the device in an IPv4 VRRP group.

Use **undo vrrp vrid preempt-mode delay** to restore the default preemption delay.

Syntax

vrrp vrid *virtual-router-id* **preempt-mode** [**delay** *delay-value*]

undo vrrp vrid *virtual-router-id* **preempt-mode** [**delay**]

Default

The device operates in preemptive mode and the preemption delay is 0 centiseconds.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv4 VRRP group by its virtual router ID in the range of 1 to 255.

delay *delay-value*: Specifies the preemption delay in the range of 0 to 180000 in centiseconds.

Usage guidelines

In non-preemptive mode, the master router acts as the master as long as it operates correctly, even if a backup is assigned a higher priority later. The non-preemptive mode helps avoid frequent switchover between the master and backups.

In preemptive mode, a backup sends VRRP advertisements when it detects that it has a higher priority than the master. Then the backup takes over as the master and the previous master becomes a backup. This mechanism ensures that the master is always the device with the highest priority.

You can configure the VRRP preemption delay for the following purposes:

- Avoid frequent state changes among members in a VRRP group.
- Provide the backups with enough time to collect information (such as routing information).

A backup does not immediately become the master after it receives an advertisement with a lower priority than the local priority. Instead, it waits for a period of time before taking over as the master.

Examples

Enable the preemptive mode for the device in VRRP group 1, and set the preemption delay to 5000 centiseconds.

```
<Switch> system-view
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] vrrp vrid 1 preempt-mode delay 5000
```

Related commands

display vrrp

7.1.12. vrrp vrid priority

Use **vrrp vrid priority** to set the priority of the device in an IPv4 VRRP group.

Use **undo vrrp vrid priority** to restore the default.

Syntax

vrrp vrid *virtual-router-id* **priority** *priority-value*

undo vrrp vrid *virtual-router-id* **priority**

Default

The priority of a device in an IPv4 VRRP group is 100.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv4 VRRP group by its virtual router ID in the range of 1 to 255.

priority-value: Specifies a priority value in the range of 1 to 254. A higher value indicates a higher priority.

Usage guidelines

VRRP determines the role (master or backup) of each device in a VRRP group by priority. A device with a higher priority is more likely to become the master.

Priorities 1 to 254 are configurable. Priority 0 is reserved for special uses, and priority 255 is for the IP address owner. The IP address owner in a VRRP group always has a running priority of 255 and acts as the master as long as it operates correctly.

Examples

Set the priority of the switch to 150 in VRRP group 1 on VLAN-interface 2.

```
<Switch> system-view
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] vrrp vrid 1 priority 150
```

Related commands

display vrrp

vrrp vrid track

7.1.13. vrrp vrid timer advertise

Use **vrrp vrid timer advertise** to set the interval at which the master in an IPv4 VRRP group sends VRRP advertisements.

Use **undo vrrp vrid timer advertise** to restore the default.

Syntax

vrrp vrid *virtual-router-id* **timer advertise** *adver-interval*

undo vrrp vrid *virtual-router-id* **timer advertise**

Default

The master in an IPv4 VRRP group sends VRRP advertisements at an interval of 100 centiseconds.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv4 VRRP group by its virtual router ID in the range of 1 to 255.

adver-interval: Specifies an interval for the master in the specified IPv4 VRRP group to send VRRP advertisements. The value range for this argument is 10 to 4095 centiseconds. For VRRPv2, the value of the *adver-interval* argument can only be a multiple of 100. For example, if you configure values in the range of 10 to 100, 101 to 200, and 4001 to 4095, the actual values are 100, 200, and 4100, respectively. For VRRPv3, the configured value for the *adver-interval* argument takes effect.

Usage guidelines

The master in an IPv4 VRRP group periodically sends VRRP advertisements to declare its presence. You can use this command to configure the interval at which the master sends VRRP advertisements.

As a best practice to maintain system stability, set the VRRP advertisement interval to be greater than 100 centiseconds.

In VRRPv2, all routers in an IPv4 VRRP group must have the same interval for sending VRRP advertisements.

In VRRPv3, the routers in an IPv4 VRRP group can have different intervals for sending VRRP advertisements. The master in the VRRP group sends VRRP advertisements at the specified interval and carries the interval attribute in the advertisements. After a backup receives the advertisement, it records the interval in the advertisement. If the backup does not receive any VRRP advertisement when the timer (3 × recorded interval + Skew_Time) expires, it regards the master as failed and takes over.

Large network traffic might disable a backup from receiving VRRP advertisements from the master within the specified timer and trigger an unexpected master switchover. To solve this problem, you can use this command to set a larger interval.

Examples

Configure the master in IPv4 VRRP group 1 to send VRRP advertisements at an interval of 500 centiseconds.

```
<Switch> system-view
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] vrrp vrid 1 timer advertise 500
```

Related commands

display vrrp

7.1.14. vrrp vrid track

Use **vrrp vrid track** to associate a VRRP group in a VRRP group with a track entry.

Use **undo vrrp vrid track** to remove the association between a VRRP group in a VRRP group and a track entry.

Syntax

vrrp vrid *virtual-router-id* **track** *track-entry-number* { **priority reduced** [*priority-reduced*] | **switchover** }

undo vrrp vrid *virtual-router-id* **track** [*track-entry-number*] [**priority reduced** | **switchover**]

Default

A VRRP group in a VRRP group are not associated with any track entries.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv4 VRRP group number in the range of 1 to 255.

track-entry-number: Specifies a track entry by its number in the range of 1 to 1024.

priority reduced [*priority-reduced*]: Reduces the priority of the router in the VRRP group by the specified value when the state of the specified track entry changes to Negative. The value range for the *priority-reduced* argument is 1 to 255, and the default value is 10.

switchover: Enables the router in backup state to take over as the master immediately after the specified track entry changes to the Negative state.

Usage guidelines

When the associated track entry changes to the Negative state, one of the following events occurs depending on your configuration:

- The priority of the router in the VRRP group decreases by a specified value.
- The router immediately takes over as the master if it is a backup.

When the track entry changes from Negative to Positive or NotReady, one of the following events occurs:

- The router automatically restores its priority.
- The failed master router becomes the master again.

Before executing this command, create a VRRP group on the interface and assign a virtual IP address to the VRRP group.

You can create a track entry by using the **track** command before or after you associate it with a VRRP group in a VRRP group. For more information about configuring track entries, see *High Availability Configuration Guide*.

If no track entry is specified, the **undo vrrp vrid track** command removes all associations between track entries and the VRRP group in the VRRP group.

The **vrrp vrid track priority reduced** command and the **vrrp vrid track switchover** command do not take effect on an IP address owner. If you configure the command on an IP address owner, the configuration takes effect after the router changes to be a non-IP address owner.

Examples

Associate VRRP group 1 on VLAN-interface 2 with track entry 1 and decrease the router priority by 50 when the state of track entry 1 changes to Negative.

```
<Switch> system-view
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] vrrp vrid 1 track 1 priority reduced 50
```

Related commands

display vrrp

7.2. IPv6 VRRP commands

7.2.1. display vrrp ipv6

Use **display vrrp ipv6** to display the states of IPv6 VRRP groups.

Syntax

display vrrp ipv6 [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number.

vrid *virtual-router-id*: Specifies an IPv6 VRRP group by its virtual router ID in the range of 1 to 255.

verbose: Displays detailed IPv6 VRRP group information. If you do not specify the **verbose** keyword, the command displays brief IPv6 VRRP group information.

Usage guidelines

If no interface or VRRP group is specified, this command displays the states of all IPv6 VRRP groups.

If only an interface is specified, this command displays the states of all IPv6 VRRP groups on the specified interface.

If both an interface and an IPv6 VRRP group are specified, this command displays the states of the specified IPv6 VRRP group on the specified interface.

Examples

Display brief information about all IPv6 VRRP groups on the device when VRRP operates in standard mode.

```
<Switch> display vrrp ipv6
IPv6 Virtual Router Information:
 Running Mode      : Standard
 ND sending interval : 120 sec
 Total number of virtual routers : 1
 Interface          VRID  State        Running Adver   Auth     Virtual
                                        Pri     Timer   Type       IP
 ------------------------------------------------------------------------
 Vlan2              1     Master       150     100     None     FE80::1
```

Table 7-4 Command output (in standard mode)

Field	Description
Running Mode	VRRP operating mode (standard mode).
ND sending interval	Sending interval for ND packets.
Total number of virtual routers	Total number of VRRP groups.
Interface	Interface where the VRRP group is configured.
VRID	Virtual router ID (VRRP group number).
State	State of the router in the VRRP group: • **Master**—The router is the master in the VRRP group. • **Backup**—The router is the backup in the VRRP group. • **Initialize**—The router is in **Initialize** state. • **Inactive**—The router is in **Inactive** state, for example, when the router is not assigned a virtual IP address by using the **vrrp vrid** command.
Running Pri	Current priority of the router. When a track entry is associated with a VRRP group on the router, the router's priority changes when the track entry's status changes.
Adver Timer	VRRP advertisement sending interval in centiseconds.
Auth Type	Authentication type. Only **none** is available, which means no authentication is required.
Virtual IP	Virtual IP address of the VRRP group.

Display detailed information about all IPv6 VRRP groups on the device when VRRP operates in standard mode.

```
<Switch> display vrrp ipv6 verbose
IPv6 Virtual Router Information:
 Running Mode      : Standard
 ND sending interval : 120 sec
 Total number of virtual routers : 2
   Interface Vlan-interface2
```

```
  VRID             : 1                    Adver Timer   : 100
  Admin Status     : Up                   State         : Master
  Config Pri       : 150                  Running Pri   : 150
  Preempt Mode     : Yes                  Delay Time    : 10
  Auth Type        : None
  Virtual IP       : FE80::1
  Virtual MAC      : 0000-5e00-0201
  Master IP        : FE80::2
  Config Role      : Master
  Name             : abc
VRRP Track Information:
  Track Object   : 1                  State : Positive   Pri Reduced : 50

Interface Vlan-interface2
  VRID             : 2                    Adver Timer   : 100
  Admin Status     : Up                   State         : Backup
  Config Pri       : 80                   Running Pri   : 80
  Preempt Mode     : Yes                  Delay Time    : 0
  Become Master    : 2450ms left
  Auth Type        : None
  Virtual IP       : FE80::11
  Virtual MAC      : 0000-5e00-0202
  Master IP        : FE80::12

Interface Vlan-interface2
  VRID             : 3                    Adver Timer   : 100
  Admin Status     : Up                   State         : Master
  Config Pri       : 100                  Running Pri   : 100
  Preempt Mode     : Yes                  Delay Time    : 0
  Auth Type        : None
  Virtual IP       : FE80::10
  Virtual MAC      : 0000-5e00-0203
  Master IP        : FE80::2
  Config Role      : Subordinate
  Follow Name      : abc
```

Table 7-5 Command output (in standard mode)

Field	Description
Running Mode	VRRP operating mode (standard mode).
ND sending interval	Sending interval for ND packets. This field is displayed only after you configure the **vrrp ipv6 send-nd** command.
Total number of virtual routers	Total number of VRRP groups.
Interface	Interface where the VRRP group is configured.
VRID	Virtual router ID (VRRP group number).
Adver Timer	VRRP advertisement sending interval in centiseconds.

Field	Description
Admin Status	Administrative status: **Up** or **Down**.
State	State of the router in the VRRP group: • **Master**—The router is the master in the VRRP group. • **Backup**—The router is the backup in the VRRP group. • **Initialize**—The router is in **Initialize** state. • **Inactive**—The router is in **Inactive** state, for example, when the router is not assigned a virtual IP address by using the **vrrp vrid** command.
Config Pri	Configured priority of the router, which is configured by using the **vrrp ipv6 vrid priority** command.
Running Pri	Current priority of the router. When a track entry is associated with a VRRP group on the router, the router's priority changes when the track entry's status changes.
Preempt Mode	Preemptive mode: • **Yes**. • **No**.
Delay Time	Preemption delay in centiseconds.
Become Master	Time (in milliseconds) that a backup router has to wait before it becomes the master. This field is displayed only when the router is a backup.
Auth Type	Authentication type. Only **none** is available, which means no authentication is required.
Virtual IP	Virtual IP address of the VRRP group.
Virtual MAC	Virtual MAC address of the VRRP group's virtual IP address, which is displayed when the router is the master.
Master IP	Link-local address of the interface where the master resides.
Config Role	The configured role of the IPv6 VRRP group to which the router belongs. • **Master**. • **Subordinate**.
Name	Master group name assigned to the IPv6 VRRP group.
Follow Name	Name of the master VRRP group that the IPv6 VRRP group follows.
VRRP Track Information	Track entry information. This field is displayed only after you configure the **vrrp ipv6 vrid track** command.
Track Object	Track entry which is associated with the VRRP group.
State	Track entry state: • **Negative**. • **Positive**. • **NotReady**.
Pri Reduced	Value by which the priority decreases when the state of the associated track entry becomes Negative.
Switchover	Switchover mode. When the state of the associated track entry becomes Negative, the backup immediately becomes the

Field	Description
	master.

7.2.2. display vrrp ipv6 statistics

Use **display vrrp ipv6 statistics** to display statistics for IPv6 VRRP groups.

Syntax

display vrrp ipv6 statistics [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number.

vrid *virtual-router-id*: Specifies an IPv6 VRRP group by its virtual router ID in the range of 1 to 255.

Usage guidelines

If no interface or VRRP group is specified, this command displays statistics for all IPv6 VRRP groups.

If only an interface is specified, this command displays statistics for all IPv6 VRRP groups on the specified interface.

If both an interface and an IPv6 VRRP group are specified, this command displays statistics for the specified IPv6 VRRP group on the specified interface.

Examples

Display statistics for all IPv6 VRRP groups when VRRP operates in standard mode.

```
<Switch> display vrrp ipv6 statistics
 Interface              : Vlan-interface2
 VRID                   : 1
 CheckSum Errors        : 0          Version Errors               : 0
 Invalid Pkts Rcvd      : 0          Unexpected Pkts Rcvd         : 0
 Hop Limit Errors       : 0          Advertisement Interval Errors : 0
 Invalid Auth Type      : 0          Auth Failures                : 0
 Packet Length Errors   : 0          Auth Type Mismatch           : 0
 Become Master          : 1          Address List Errors          : 0
 Adver Rcvd             : 0          Priority Zero Pkts Rcvd      : 0
 Adver Sent             : 425        Priority Zero Pkts Sent      : 0
IP Owner Conflicts     : 0

 Global statistics
 CheckSum Errors        : 0
```

```
Version Errors          : 0
VRID Errors             : 0
```

Table 7-6 Command output (in standard mode)

Field	Description
Interface	Interface where the VRRP group is configured.
VRID	VRRP group number.
CheckSum Errors	Number of packets with checksum errors.
Version Errors	Number of packets with version errors.
Invalid Pkts Rcvd	Number of received packets of invalid packet types.
Unexpected Pkts Rcvd	Number of received unexpected packets.
Advertisement Interval Errors	Number of packets with advertisement interval errors.
Hop Limit Errors	Number of packets with hop limit errors.
Auth Failures	Number of packets with authentication failures.
Invalid Auth Type	Number of packets with authentication failures because of invalid authentication types.
Auth Type Mismatch	Number of packets with authentication failures because of mismatching authentication types.
Packet Length Errors	Number of packets with VRRP packet length errors.
Address List Errors	Number of packets with virtual IP address list errors.
Become Master	Number of times that the router has been elected as the master.
Priority Zero Pkts Rcvd	Number of received advertisements with the router priority of 0.
Adver Rcvd	Number of received advertisements.
Priority Zero Pkts Sent	Number of sent advertisements with the router priority of 0.
Adver Sent	Number of sent advertisements.
IP Owner Conflicts	Number of VRRP packets that the local router (IP address owner) has received from conflicting IP address owners.
Global statistics	Global statistics for all IPv6 VRRP groups.
CheckSum Errors	Total number of packets with checksum errors.
Version Errors	Total number of packets with version errors.
VRID Errors	Total number of packets with VRID errors.

Related commands

`reset vrrp ipv6 statistics`

7.2.3. reset vrrp ipv6 statistics

Use **`reset vrrp ipv6 statistics`** to clear statistics for IPv6 VRRP groups.

Syntax

reset vrrp ipv6 statistics [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]]

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number.

vrid *virtual-router-id*: Specifies an IPv6 VRRP group by its virtual router ID in the range of 1 to 255.

Usage guidelines

If no interface or VRRP group is specified, this command clears statistics for all IPv6 VRRP groups.

If only an interface is specified, this command clears statistics for all IPv6 VRRP groups on the specified interface.

If both an interface and an IPv6 VRRP group are specified, this command clears statistics for the specified IPv6 VRRP group on the specified interface.

Examples

Clear statistics for all IPv6 VRRP groups on all interfaces.

```
<Switch> reset vrrp ipv6 statistics
```

Related commands

display vrrp ipv6 statistics

7.2.4. vrrp ipv6 dscp

Use **vrrp ipv6 dscp** to set a DSCP value for IPv6 VRRP packets.

Use **undo vrrp ipv6 dscp** to restore the default.

Syntax

vrrp ipv6 dscp *dscp-value*

undo vrrp ipv6 dscp

Default

The DSCP value for IPv6 VRRP packets is 56.

Views

System view

Predefined user roles

network-admin

Parameters

dscp-value: Specifies a DSCP value for IPv6 VRRP packets, in the range of 0 to 63.

Usage guidelines

The DSCP value identifies the packet priority during transmission. A greater DSCP value means a higher packet priority.

Examples

Set the DSCP value to 30 for IPv6 VRRP packets.

```
<Switch> system-view
[Switch] vrrp ipv6 dscp 30
```

7.2.5. vrrp ipv6 state-transition-delay

Use **vrrp ipv6 state-transition-delay** to set the delay time for the IPv6 VRRP group to transition from **Initialize** to **Master** or **Backup** state.

Use **undo vrrp ipv6 state-transition-delay** to restore the default.

Syntax

vrrp ipv6 state-transition-delay *delay-value*

undo vrrp ipv6 state-transition-delay

Default

The delay time is 0 seconds for the IPv6 VRRP group to transition from **Initialize** to **Master** or **Backup** state.

Views

Interface view

Predefined user roles

network-admin

Parameters

delay-value: Specifies delay time for the IPv6 VRRP group to transition from **Initialize** to **Master** or **Backup** state, in the range of 0 to 60 seconds.

Usage guidelines

Typically, an IPv6 VRRP group immediately transitions from **Initialize** to **Master** or **Backup** state when the interface where the IPv6 VRRP group resides comes up. If the device restarts or the interface state changes frequently, the IPv6 VRRP group state might be unstable, and the VRRP group operation might be affected. After you configure this command, a state transition delay timer is started when the interface comes up. If the interface goes down before the timer expires, the timer is stopped, and the IPv6 VRRP group stays in **Initialize** state. The timer is restarted when the interface comes up again. When the timer expires, the IPv6 VRRP group transitions from **Initialize** to **Master** or **Backup** state.

Examples

Set the delay time to 5 seconds for the IPv6 VRRP group to transition from **Initialize** to **Master** or **Backup** state.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] vrrp ipv6 state-transition-delay 5
```

7.2.6. vrrp ipv6 vrid

Use **vrrp ipv6 vrid** to create an IPv6 VRRP group and assign a virtual IPv6 address to it, or to assign a virtual IPv6 address to an existing IPv6 VRRP group.

Use **undo vrrp ipv6 vrid** to remove all configurations of an IPv6 VRRP group, or to remove a virtual IPv6 address from an IPv6 VRRP group.

Syntax

vrrp ipv6 vrid *virtual-router-id* **virtual-ip** *virtual-address* [**link-local**]

undo vrrp ipv6 vrid *virtual-router-id* [**virtual-ip** [*virtual-address* [**link-local**]]]

Default

No IPv6 VRRP groups exist.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv6 VRRP group by its virtual router ID in the range of 1 to 255.

virtual-ip *virtual-address*: Specifies a virtual IPv6 address. If you do not specify this option, the **undo vrrp ipv6 vrid** command removes all virtual IPv6 addresses from the specified IPv6 VRRP group.

link-local: Specifies a link-local address as the virtual IPv6 address.

Usage guidelines

You can execute this command multiple times to assign multiple virtual IPv6 addresses to an IPv6 VRRP group. An IPv6 VRRP group can have a maximum of 16 virtual IPv6 addresses.

The first virtual IPv6 address that you assign to an IPv6 VRRP group must be a link-local address, and it must be removed last.

An IPv6 VRRP group can have only one link-local address as its virtual IPv6 address.

An IPv6 VRRP group without virtual IPv6 addresses configured can exist on a device provided that other settings (for example, priority and preemption mode) are available. Such a VRRP group stays in inactive state and does not function.

The virtual IPv6 address of an IPv6 VRRP group and the downlink interface IPv6 address of the VRRP group members must be in the same subnet. Otherwise, the hosts in the subnet might fail to access external networks.

Examples

Create IPv6 VRRP group 1 and assign virtual IPv6 address fe80::10 to the VRRP group. Then assign virtual IPv6 address 1::10 to the VRRP group.

```
<Switch> system-view
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
[Switch-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip 1::10
```

Related commands

display vrrp ipv6

7.2.7. vrrp ipv6 vrid preempt-mode

Use **vrrp ipv6 vrid preempt-mode** to enable the preemptive mode for the router in an IPv6 VRRP group and set the preemption delay.

Use **undo vrrp ipv6 vrid preempt-mode** to disable the preemptive mode for the router in an IPv6 VRRP group.

Use **undo vrrp ipv6 vrid preempt-mode delay** to restore the default preemption delay.

Syntax

vrrp ipv6 vrid *virtual-router-id* **preempt-mode** [**delay** *delay-value*]

undo vrrp ipv6 vrid *virtual-router-id* **preempt-mode** [**delay**]

Default

The router operates in preemptive mode and the preemption delay is 0 centiseconds.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv6 VRRP group by its virtual router ID in the range of 1 to 255.

delay *delay-value*: Specifies the preemption delay in the range of 0 to 180000 in centiseconds.

Usage guidelines

In non-preemptive mode, the master router acts as the master as long as it operates correctly, even if a backup is assigned a higher priority later. The non-preemptive mode helps avoid frequent switchover between the master and backups.

In preemptive mode, a backup sends VRRP advertisements when it detects that it has a higher priority than the master. Then the backup takes over as the master and the previous master becomes a backup. This mechanism ensures that the master is always the router with the highest priority.

You can configure the VRRP preemption delay for the following purposes:

- Avoid frequent state changes among members in a VRRP group.
- Provide the backups with enough time to collect information (such as routing information).

A backup does not immediately become the master after it receives an advertisement with a lower priority than the local priority. Instead, it waits for a period of time before taking over.

Examples

Enable the preemptive mode for VRRP group 1, and set the preemption delay to 5000 centiseconds.

```
<Switch> system-view
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] vrrp ipv6 vrid 10 preempt-mode delay 5000
```

Related commands

display vrrp ipv6

7.2.8. vrrp ipv6 vrid priority

Use **vrrp ipv6 vrid priority** to set the priority of the router in an IPv6 VRRP group.

Use **undo vrrp ipv6 vrid priority** to restore the default.

Syntax

vrrp ipv6 vrid *virtual-router-id* **priority** *priority-value*

undo vrrp ipv6 vrid *virtual-router-id* **priority**

Default

The priority of a router in an IPv6 VRRP group is 100.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv6 VRRP group by its virtual router ID in the range of 1 to 255.

priority-value: Specifies a priority value in the range of 1 to 254. A higher value indicates a higher priority.

Usage guidelines

VRRP determines the role (master or backup) of each router in a VRRP group by priority. A router with a higher priority is more likely to become the master.

Priorities 1 to 254 are configurable. Priority 0 is reserved for special uses, and priority 255 is for the IP address owner. The IP address owner in a VRRP group always has a running priority of 255 and acts as the master as long as it operates correctly.

Examples

Set the priority of the switch to 150 in VRRP group 1 on VLAN-interface 2.

```
<Switch> system-view
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] vrrp ipv6 vrid 1 priority 150
```

Related commands

display vrrp ipv6

7.2.9. vrrp ipv6 vrid timer advertise

Use **vrrp ipv6 vrid timer advertise** to set the interval at which the master in an IPv6 VRRP group sends VRRP advertisements.

Use **undo vrrp ipv6 vrid timer advertise** to restore the default.

Syntax

vrrp ipv6 vrid *virtual-router-id* **timer advertise** *adver-interval*

undo vrrp ipv6 vrid *virtual-router-id* **timer advertise**

Default

The master in an IPv6 VRRP group sends VRRP advertisements at an interval of 100 centiseconds.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv6 VRRP group by its virtual router ID in the range of 1 to 255.

adver-interval: Specifies an interval for the master in the specified IPv6 VRRP group to send VRRP advertisements, in the range of 100 to 4095 centiseconds.

Usage guidelines

The master in an IPv6 VRRP group periodically sends VRRP advertisements to declare its presence. You can use this command to set the interval at which the master sends VRRP advertisements.

As a best practice to maintain system stability, set the VRRP advertisement interval to be greater than 100 centiseconds.

The routers in an IPv6 VRRP group can have different intervals for sending VRRP advertisements. The master in the VRRP group sends VRRP advertisements at the specified interval and carries the interval attribute in the advertisements. After a backup receives the advertisement, it records the interval in the advertisement. If the backup does not receive any VRRP advertisement when the timer (3 × VRRP advertisement sending interval + Skew_Time) expires, it regards the master as failed and takes over.

Large network traffic might disable a backup from receiving VRRP advertisements from the master within the specified timer and trigger an unexpected master switchover. To solve this problem, you can use this command to configure a larger interval.

Examples

Configure the master in IPv6 VRRP group 1 to send VRRP advertisements at an interval of 500 centiseconds.

```
<Switch> system-view
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] vrrp ipv6 vrid 1 timer advertise 500
```

Related commands

display vrrp ipv6

7.2.10. vrrp ipv6 vrid track

Use **vrrp ipv6 vrid track** to associate an IPv6 VRRP group in an IPv6 VRRP group with a track entry.

Use **undo vrrp ipv6 vrid track** to remove the association between an IPv6 VRRP group in an IPv6 VRRP group and a track entry.

Syntax

vrrp ipv6 vrid *virtual-router-id* **track** *track-entry-number* { **priority reduced** [*priority-reduced*] | **switchover** }

undo vrrp ipv6 vrid *virtual-router-id* **track** [*track-entry-number*] [**priority reduced** | **switchover**]

Default

An IPv6 VRRP group in an IPv6 VRRP group are not associated with any track entries.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv6 VRRP group number in the range of 1 to 255.

track-entry-number: Specifies a track entry by its number in the range of 1 to 1024.

priority reduced [*priority-reduced*]: Reduces the priority of the router in the VRRP group by the specified value when the state of the specified track entry changes to Negative. The value range for the *priority-reduced* argument is 1 to 255, and the default value is 10.

switchover: Enables the router in backup state to take over as the master immediately after the specified track entry changes to the Negative state.

Usage guidelines

When the associated track entry changes to the Negative state, one of the following events occurs depending on your configuration:

- The priority of the router in the VRRP group decreases by a specified value.
- The router immediately takes over as the master if it is a backup.

When the track entry changes from Negative to Positive or NotReady, one of the following events occurs:

- The router automatically restores its priority.
- The failed master router becomes the master again.

Before executing this command, create an IPv6 VRRP group on the interface and assign a virtual IPv6 address to the IPv6 VRRP group.

You can create a track entry by using the **track** command before or after you associate it with an IPv6 VRRP group in an IPv6 VRRP group. For more information about configuring track entries, see *High Availability Configuration Guide*.

If no track entry is specified, the **undo vrrp ipv6 vrid track** command removes all associations between track entries and the IPv6 VRRP group in the IPv6 VRRP group.

The **vrrp ipv6 vrid track priority reduced** command and the **vrrp ipv6 vrid track switchover** command do not take effect on an IP address owner. If you configure the command on an IP address owner, the configuration takes effect after the router changes to be a non-IP address owner.

Examples

Associate IPv6 VRRP group 1 on VLAN-interface 2 with track entry 1 and decrease the router priority by 50 when the state of track entry 1 changes to Negative.

```
<Switch> system-view
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] vrrp ipv6 vrid 1 track 1 priority reduced 50
```

Related commands

display vrrp ipv6

Contents

A page of this section is **10-x-x**

8. BFD commands 8-1
8.1. BFD commands 8-1
8.1.1. bfd authentication-mode 8-1
8.1.2. bfd demand enable 8-2
8.1.3. bfd detect-multiplier 8-2
8.1.4. bfd echo enable 8-3
8.1.5. bfd echo-source-ip 8-4
8.1.6. bfd min-echo-receive-interval 8-4
8.1.7. bfd min-receive-interval 8-5
8.1.8. bfd min-transmit-interval 8-6
8.1.9. bfd multi-hop authentication-mode 8-7
8.1.10. bfd multi-hop destination-port 8-8
8.1.11. bfd multi-hop detect-multiplier 8-8
8.1.12. bfd multi-hop min-receive-interval 8-9
8.1.13. bfd multi-hop min-transmit-interval 8-10
8.1.14. bfd session init-mode 8-11
8.1.15. display bfd session 8-11
8.1.16. reset bfd session statistics 8-14
8.1.17. snmp-agent trap enable bfd 8-14

8. BFD commands

8.1. BFD commands

8.1.1. bfd authentication-mode

Use **bfd authentication-mode** to configure the BFD authentication mode for single-hop BFD control packets.

Use **undo bfd authentication-mode** to restore the default.

Syntax

bfd authentication-mode { **md5** | **sha1** | **simple** } *key-id* { **cipher** | **plain** } *string*

undo bfd authentication-mode

Default

Single-hop BFD control packets are not authenticated.

Views

Interface view

Predefined user roles

network-admin

Parameters

md5: Specifies the MD5 algorithm.

sha1: Specifies the SHA1 algorithm.

simple: Specifies the simple authentication mode.

key-id: Sets the authentication key ID in the range of 1 to 255.

cipher: Specifies a key in encrypted form.

plain: Specifies a key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. Its plaintext form is a case-sensitive string of 1 to 16 characters. Its encrypted form is a case-sensitive string of 33 to 53 characters.

Usage guidelines

Use this command to enhance BFD session security.

BFD version 0 does not support this command. The configuration does not take effect.

Examples

Configure VLAN-interface 11 to perform simple authentication for single-hop BFD control packets, setting the authentication key ID to **1** and plaintext key to **123456**.

```
<Switch> system-view
[Switch] interface vlan-interface 11
[Switch-Vlan-interface11] bfd authentication-mode simple 1 plain 123456
```

8.1.2. bfd demand enable

Use **bfd demand enable** to enable the Demand BFD session mode.

Use **undo bfd demand enable** to restore the default.

Syntax

bfd demand enable

undo bfd demand enable

Default

The BFD session is in Asynchronous mode.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

In Demand mode, the device periodically sends BFD control packets. If the peer end is operating in Asynchronous mode (default), the peer end stops sending BFD control packets. If the peer end is operating in Demand mode, both ends stop sending BFD control packets. When the connectivity to another system needs to be verified explicitly, a system sends several BFD control packets with the Poll (P) bit set at the negotiated transmit interval. If no response is received within the detection interval, the session is considered down. If the connectivity is found to be up, no more BFD control packets are sent until the next command is issued.

In Asynchronous mode, the device periodically sends BFD control packets. The device considers that the session is down if it does not receive any BFD control packets within a specific interval.

BFD version 0 does not support this command. The configuration does not take effect.

Examples

Enable the Demand BFD session mode on VLAN-interface 11.

```
<Switch> system-view
[Switch] interface vlan-interface 11
[Switch-Vlan-interface11] bfd demand enable
```

8.1.3. bfd detect-multiplier

Use **bfd detect-multiplier** to set the single-hop detection time multiplier for control packet mode and the detection time multiplier for echo packet mode.

Use **undo bfd detect-multiplier** to restore the default.

Syntax

bfd detect-multiplier *value*

undo bfd detect-multiplier

Default

Up to Software Version v7.4.37： The multihop detection time multiplier is 5.

Software Version v7.4.40 or later： The multihop detection time multiplier is 3.

Views

Interface view

Predefined user roles

network-admin

Parameters

value: Specifies a single-hop detection time multiplier in the range of 3 to 50.

Usage guidelines

The detection time multiplier determines the maximum number of concurrent BFD packets (including control packets and echo packets) that can be discarded.

Table 8-1 Detection interval calculation method

Mode	Detection interval
Echo packet mode	Detection time multiplier of the sender × actual packet sending interval of the sender
Control packet mode BFD session in asynchronous mode	Detection time multiplier of the receiver × actual packet sending interval of the receiver
Control packet mode BFD session in demand mode	Detection time multiplier of the sender × actual packet sending interval of the sender

Examples

Set the single-hop detection time multiplier for control packet mode and the detection time multiplier for echo packet mode to 6 on VLAN-interface 11.

```
<Switch> system-view
[Switch] interface vlan-interface 11
[Switch-Vlan-interface11] bfd detect-multiplier 6
```

8.1.4. bfd echo enable

Use **bfd echo enable** to enable the echo packet mode.

Use **undo bfd echo enable** to disable the echo packet mode.

Syntax

bfd echo enable

undo bfd echo enable

Default

The echo packet mode is disabled.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

If you enable the echo packet mode for a BFD session in which control packets are sent and the session comes up, BFD performs the following operations:

- Periodically sends echo packets to detect link connectivity.
- Decreases the control packet receiving rate at the same time.

The command enables both the echo packet receiving and sending capabilities.

BFD version 0 does not support this command. The configuration does not take effect.

Examples

Enable the echo packet mode on VLAN-interface 11.

```
<Switch> system-view
[Switch] interface vlan-interface 11
[Switch-Vlan-interface11] bfd echo enable
```

8.1.5. bfd echo-source-ip

Use **bfd echo-source-ip** to configure the source IP address of BFD echo packets.

Use **undo bfd echo-source-ip** to remove the configured source IP address of BFD echo packets.

Syntax

bfd echo-source-ip *ip-address*

undo bfd echo-source-ip

Default

No source IP address is configured for BFD echo packets.

Views

System view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the source IP address of BFD echo packets.

Usage guidelines

The source IP address cannot be on the same network segment as any local interface's IP address. Otherwise, a large number of ICMP redirect packets might be sent from the peer, resulting in link congestion.

Examples

Configure the source IP address of BFD echo packets as 8.8.8.8.

```
<Switch> system-view
[Switch] bfd echo-source-ip 8.8.8.8
```

8.1.6. bfd min-echo-receive-interval

Use **bfd min-echo-receive-interval** to set the minimum interval for receiving BFD echo packets.

Use **undo bfd min-echo-receive-interval** to restore the default.

Syntax

bfd min-echo-receive-interval *interval*

undo bfd min-echo-receive-interval

Default

The minimum interval for receiving BFD echo packets is 400 milliseconds.

Views

Interface view

Predefined user roles

network-admin

Parameters

interval: Specifies the minimum interval for receiving BFD echo packets, in milliseconds. The value takes 0 or is in the range of 100 to 1000.

Usage guidelines

This command sets the BFD echo packet receiving interval, which is the actual BFD echo packet sending interval.

The local end stops sending echo packets after autonegotiation with the remote end if the following conditions are met:

- The echo packet mode is enabled on the local end.
- The minimum interval for receiving BFD echo packets is set to 0 milliseconds on the remote end.

Examples

Set the minimum interval for receiving BFD echo packets to 500 milliseconds on VLAN-interface 11.

```
<Switch> system-view
[Switch] interface vlan-interface 11
[Switch-Vlan-interface11] bfd min-echo-receive-interval 500
```

8.1.7. bfd min-receive-interval

Use **bfd min-receive-interval** to set the minimum interval for receiving single-hop BFD control packets.

Use **undo bfd min-receive-interval** to restore the default.

Syntax

bfd min-receive-interval *interval*

undo bfd min-receive-interval

Default

The minimum interval for receiving single-hop BFD control packets is 400 milliseconds.

Views

Interface view

Predefined user roles

network-admin

Parameters

Before V7.1.6

interval: Specifies the minimum interval for receiving single-hop BFD control packets, in milliseconds. The value range is 100 to 1000.

After v7.2.16

interval: Specifies the minimum interval for receiving single-hop BFD control packets, in milliseconds. The value range is 3 to 1000.

Usage guidelines

Use this command to prevent the control packet sending rate of the peer end from exceeding the control packet receiving rate of the local end.

The actual control packet sending interval of the peer end takes the greater value between the following values:

- Minimum interval for transmitting BFD control packets on the peer end.
- Minimum interval for receiving BFD control packets on the local end.

Examples

Set the minimum interval for receiving single-hop BFD control packets to 500 milliseconds on VLAN-interface 11.

```
<Switch> system-view
[Switch] interface vlan-interface 11
[Switch-Vlan-interface11] bfd min-receive-interval 500
```

8.1.8. bfd min-transmit-interval

Use **bfd min-transmit-interval** to set the minimum interval for transmitting single-hop BFD control packets.

Use **undo bfd min-transmit-interval** to restore the default.

Syntax

bfd min-transmit-interval *interval*

undo bfd min-transmit-interval

Default

The minimum interval for transmitting single-hop BFD control packets is 400 milliseconds.

Views

Interface view

Predefined user roles

network-admin

Parameters

Before V7.1.6

interval: Specifies the minimum interval for transmitting single-hop BFD control packets, in milliseconds. The value range is 100 to 1000.

After v7.2.16

interval: Specifies the minimum interval for receiving single-hop BFD control packets, in milliseconds. The value range is 3 to 1000.

Usage guidelines

Use this command to prevent the BFD packet sending rate from exceeding the device capability.

The actual BFD control packet transmitting interval on the local end is the greater value between the following values:

- Minimum interval for transmitting BFD control packets on the local end.
- Minimum interval for receiving BFD control packets on the peer end.

Examples

Set the minimum interval for transmitting single-hop BFD control packets to 500 milliseconds on VLAN-interface 11.

```
<Switch> system-view
[Switch] interface vlan-interface 11
[Switch-Vlan-interface11] bfd min-transmit-interval 500
```

8.1.9. bfd multi-hop authentication-mode

Use **bfd multi-hop authentication-mode** to configure the authentication mode for multihop BFD control packets.

Use **undo bfd multi-hop authentication-mode** to restore the default.

Syntax

bfd multi-hop authentication-mode { **md5** | **sha1** | **simple** } *key-id* { **cipher** | **plain** } *string*

undo bfd multi-hop authentication-mode

Default

No authentication is performed.

Views

System view

Predefined user roles

network-admin

Parameters

md5: Specifies the MD5 algorithm.

sha1: Specifies the SHA1 algorithm.

simple: Specifies the simple authentication mode.

key-id: Sets the authentication key ID in the range of 1 to 255.

cipher: Specifies a key in encrypted form.

plain: Specifies a key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. Its plaintext form is a case-sensitive string of 1 to 16 characters. Its encrypted form is a case-sensitive string of 33 to 53 characters.

Usage guidelines

Use this command to enhance BFD session security.

BFD version 0 does not support this command. The configuration does not take effect.

Examples

Configure the simple authentication mode for multihop BFD control packets, setting the authentication key ID to 1 and key to **123456**.

```
<Switch> system-view
[Switch] bfd multi-hop authentication-mode simple 1 plain 123456
```

8.1.10. bfd multi-hop destination-port

Use **bfd multi-hop destination-port** to configure the destination port number for multihop BFD control packets.

Use **undo bfd multi-hop destination-port** to restore the default.

Syntax

bfd multi-hop destination-port *port-number*

undo bfd multi-hop destination-port

Default

The destination port number for multihop BFD control packets is 4784.

Views

System view

Predefined user roles

network-admin

Parameters

port-number: Specifies the destination port number of multihop BFD control packets, 3784 or 4784.

Examples

Specify the destination port number for multihop BFD control packets as 3784.

```
<Switch> system-view
[Switch] bfd multi-hop destination-port 3784
```

8.1.11. bfd multi-hop detect-multiplier

Use **bfd multi-hop detect-multiplier** to set the multihop detection time multiplier for control packet mode.

Use **undo bfd multi-hop detect-multiplier** to restore the default.

Syntax

bfd multi-hop detect-multiplier *value*

undo bfd multi-hop detect-multiplier

Default

Up to Software Version v7.4.37 : The multihop detection time multiplier is 5.

Software Version v7.4.40 or later : The multihop detection time multiplier is 3.

Views

System view

Predefined user roles

network-admin

Parameters

value: Specifies the multihop detection time multiplier in the range of 3 to 50.

Usage guidelines

The detection time multiplier determines the maximum number of concurrent BFD control packets that can be discarded.

Table 8-2 Detection interval calculation method

Mode	Detection interval
Control packet mode BFD session in asynchronous mode	Detection time multiplier of the receiver × actual packet sending interval of the receiver
Control packet mode BFD session in demand mode	Detection time multiplier of the sender × actual packet sending interval of the sender

Examples

Set the multihop detection time multiplier to 6.

```
<Switch> system-view
[Switch] bfd multi-hop detect-multiplier 6
```

8.1.12. bfd multi-hop min-receive-interval

Use **bfd multi-hop min-receive-interval** to set the minimum interval for receiving multihop BFD control packets.

Use **undo bfd multi-hop min-receive-interval** to restore the default.

Syntax

bfd multi-hop min-receive-interval *interval*

undo bfd multi-hop min-receive-interval

Default

The minimum interval for receiving multihop BFD control packets is 400 milliseconds.

Views

System view

Predefined user roles

network-admin

Parameters

Before V7.1.6

interval: Specifies the minimum interval for receiving multihop BFD control packets, in milliseconds. The value range is 100 to 1000.

After v7.2.16

interval: Specifies the minimum interval for receiving single-hop BFD control packets, in milliseconds. The value range is 3 to 1000.

Usage guidelines

Use this command to prevent the packet sending rate of the peer end from exceeding the packet receiving capability (minimum control packet receiving interval) of the local end. If the receiving capability is exceeded, the peer end dynamically adjusts the BFD control packet sending interval to the minimum control packet receiving interval of the local end.

Examples

Set the minimum interval for receiving multihop BFD control packets to 500 milliseconds.

```
<Switch> system-view
[Switch] bfd multi-hop min-receive-interval 500
```

8.1.13. bfd multi-hop min-transmit-interval

Use **bfd multi-hop min-transmit-interval** to set the minimum interval for transmitting multihop BFD control packets.

Use **undo bfd multi-hop min-transmit-interval** to restore the default.

Syntax

bfd multi-hop min-transmit-interval *interval*

undo bfd multi-hop min-transmit-interval

Default

The minimum interval for transmitting multihop BFD control packets is 400 milliseconds.

Views

System view

Predefined user roles

network-admin

Parameters

Before V7.1.6

interval: Specifies the minimum interval for transmitting multihop BFD control packets, in milliseconds. The value range is 100 to 1000.

After v7.2.16

interval: Specifies the minimum interval for receiving single-hop BFD control packets, in milliseconds. The value range is 3 to 1000.

Usage guidelines

Use this command to prevent the BFD packet sending rate from exceeding the device capability.

The actual BFD control packet transmitting interval on the local end is the greater value between the following values:

- Minimum interval for transmitting BFD control packets on the local end.
- Minimum interval for receiving BFD control packets on the peer end.

Examples

Set the minimum interval for transmitting multihop BFD control packets to 500 milliseconds.

```
<Switch> system-view
[Switch] bfd multi-hop min-transmit-interval 500
```

8.1.14. bfd session init-mode

Use **bfd session init-mode** to configure the mode for establishing a BFD session.

Use **undo bfd session init-mode** to restore the default.

Syntax

bfd session init-mode { **active** | **passive** }

undo bfd session init-mode

Default

BFD uses the **active** mode.

Views

System view

Predefined user roles

network-admin

Parameters

active: Specifies the active mode. In active mode, BFD actively transmits BFD control packets to the remote device, regardless of whether it receives a BFD control packet from the remote device.

passive: Specifies the passive mode. In passive mode, BFD does not actively transmit a BFD control packet to the remote end; it transmits a BFD control packet only after receiving a BFD control packet from the remote end.

Usage guidelines

A minimum of one end must operate in active mode for a BFD session to be established.

BFD version 0 does not support this command. The configuration does not take effect.

Examples

Configure the session establishment mode as **passive**.

```
<Switch> system-view
[Switch] bfd session init-mode passive
```

8.1.15. display bfd session

Use **display bfd session** to display BFD session information.

Syntax

display bfd session [**discriminator** *value* | **verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

discriminator *value*: Specifies a local ID in the range of 1 to 4294967295. If this option is not specified, the command displays brief information about all BFD sessions.

verbose: Displays detailed BFD session information. If this keyword is not specified, the command displays brief BFD session information.

Examples

Display all IPv4 BFD session information.

```
<Switch> display bfd session

 Total Session Num: 1     Up Session Num: 1     Init Mode: Active

 IPv4 session working in control packet mode:

 LD/RD          SourceAddr      DestAddr        State    Holdtime    Interface
 513/513        1.1.1.1         1.1.1.2         Up       2297ms      Vlan100
```

Display detailed IPv4 BFD session information.

```
<Switch> display bfd session verbose

 Total Session Num: 1     Up Session Num: 1     Init Mode: Active

 IPv4 session working in control packet mode:

      Local Discr: 513                 Remote Discr: 513
        Source IP: 1.1.1.1           Destination IP: 1.1.1.2
    Session State: Up                     Interface: Vlan-interface100
     Min Tx Inter: 500ms                Act Tx Inter: 500ms
     Min Rx Inter: 500ms                Detect Inter: 2500ms
         Rx Count: 42                       Tx Count: 43
     Connect Type: Direct             Running Up for: 00:00:20
        Hold Time: 2078ms                  Auth mode: None
      Detect Mode: Async                        Slot: 0
         Protocol: OSPF
         Version:1
        Diag Info: No Diagnostic
```

Display all IPv6 BFD session information.

```
<Switch> display bfd session

 Total Session Num: 1     Up Session Num: 1     Init Mode: Active

 IPv6 session working in control packet mode:

      Local Discr: 513                 Remote Discr: 513
        Source IP: FE80::20C:29FF:FED4:7171
   Destination IP: FE80::20C:29FF:FE72:AC4D
    Session State: Up                     Interface: Vlan100
        Hold Time: 2142ms
```

Display detailed IPv6 BFD session information.

```
<Switch> display bfd session verbose
```

```
Total Session Num: 1     Up Session Num: 1     Init Mode: Active

IPv6 session working in control packet mode:

      Local Discr: 513                  Remote Discr: 513
        Source IP: FE80::20C:29FF:FED4:7171
   Destination IP: FE80::20C:29FF:FE72:AC4D
    Session State: Up                      Interface: Vlan-interface100
     Min Tx Inter: 500ms                Act Tx Inter: 500ms
     Min Rx Inter: 500ms                Detect Inter: 2500ms
         Rx Count: 38                       Tx Count: 38
     Connect Type: Direct             Running Up for: 00:00:15
        Hold Time: 2211ms                  Auth mode: None
      Detect Mode: Async                        Slot: 0
         Protocol: OSPFv3
         Version:1
        Diag Info: No Diagnostic
```

Table 8-3 Command output

Field	Description
Total Session Num	Total number of BFD sessions.
Up Session Num	Total number of active BFD sessions.
Init Mode	BFD operating mode: Active or passive.
IPv4 session working in control packet mode	BFD session type and operating mode: • **IPv4 session working in control packet mode**. • **IPv4 session working in echo mode**. • **IPv6 session working in control packet mode**. • **IPv6 session working in echo mode**.
Local Discr/LD	Local ID of the session.
Remote Discr/RD	Remote ID of the session.
Source IP/SourceAddr	Source IP address of the session.
Destination IP/DestAddr	Destination IP address of the session.
Session State/State	Session state: **Down**, **Init**, or **Up**.
Interface	Name of the interface of the session.
Min Tx Inter	Minimum transmit interval.
Min Rx Inter	Minimum receive interval.
Act Tx Inter	Actual transmit interval.
Detect Inter	Actual session detection timer.
Rx Count	Number of packets received.
Tx Count	Number of packets sent.
Hold Time/Holdtime	Length of time before session detection timer expires. For a BFD session in **Down** state, this field displays **0ms**.
Auth mode	Session authentication mode.

Field	Description
Connect Type	Connection type of the interface: Direct or indirect.
Running up for	Time period for which the session has been up.
Detect Mode	Detection mode: • **Async**—Asynchronous mode. • **Demand**—Demand mode. • **Async/Echo**—Asynchronous mode with echo detection enabled. • **Demand/Echo**—Demand mode with echo detection enabled.
Slot	Slot number.
Diag Info	Diagnostic information about the session: • **No Diagnostic**—The BFD session is in up state or receives no BFD packets. • **Control Detection Time Expired**—A control packet mode BFD session goes down because local detection times out. • **Echo Function Failed**—An echo packet mode BFD session goes down, because local detection times out or the source IP address of echo packets is deleted. • **Neighbor Signaled Session Down**—The remote end notifies the local end of BFD session down. • **Administratively Down**—The local system prevents a BFD session from being established.

8.1.16. reset bfd session statistics

Use **reset bfd session statistics** to clear the BFD session statistics.

Syntax

reset bfd session statistics

Views

User view

Predefined user roles

network-admin

Examples

Clear the BFD session statistics.

```
<Switch> reset bfd session statistics
```

8.1.17. snmp-agent trap enable bfd

Use **snmp-agent trap enable bfd** to enable SNMP notifications for BFD.

Use **undo snmp-agent trap enable bfd** to disable SNMP notifications for BFD.

Syntax

snmp-agent trap enable bfd

undo snmp-agent trap enable bfd

Default

All SNMP notifications are enabled for BFD.

Views

System view

Predefined user roles

network-admin

Usage guidelines

To report critical BFD events to an NMS, enable SNMP notifications for BFD. For BFD event notifications to be sent correctly, you must also configure SNMP as described in the network management and monitoring configuration guide for the device.

Examples

Disable SNMP notifications for BFD.

```
<Switch> system-view
[Switch] undo snmp-agent trap enable bfd
```

Contents

A page of this section is **10-x-x**

9. Track commands 9-1
9.1. Track commands 9-1
9.1.1. display track 9-1
9.1.2. track bfd 9-3
9.1.3. track interface 9-5
9.1.4. track interface protocol 9-6
9.1.5. track nqa 9-7

9. Track commands

9.1. Track commands

9.1.1. display track

Use **display track** to display track entry information.

Syntax

display track { *track-entry-number* | **all** [**negative** | **positive**] } [**brief**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

track-entry-number: Specifies the track entry ID in the range of 1 to 1024.

all: Specifies all track entries.

negative: Specifies track entries in Negative state.

positive: Specifies track entries in Positive state.

brief: Displays brief information about track entries.

Examples

Display information about all track entries.

```
<Switch> display track all
Track ID: 1
  State: Positive
  Duration: 0 days 0 hours 0 minutes 7 seconds
  Notification delay: Positive 20, Negative 30 (in seconds)
  Tracked object:
    NQA entry: admin test
    Reaction: 10
    Remote IP/URL: --
    Local IP: --
    Interface: --
Track ID: 2
  State: NotReady
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Notification delay: Positive 20, Negative 30 (in seconds)
  Tracked object:
    BFD session mode: Echo
    Outgoing interface: Vlan-interface2
    VPN instance name: --
```

```
    Remote IP: 192.168.40.1
    Local IP: 192.168.40.2
Track ID: 3
  State: Negative
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Notification delay: Positive 20, Negative 30 (in seconds)
  Tracked object:
    Interface:  Vlan-interface3
    Protocol: IPv4
Track ID: 4
  State: Negative
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Notification delay: Positive 20, Negative 30 (in seconds)
  Tracked object:
    CFD service instance: MEP 2 in Ethernet service instance 1
Track ID: 5
  State: Positive
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Notification delay: Positive 20, Negative 30 (in seconds)
  Tracked object:
    IP route: 0.0.0.0/0 reachability
    VPN instance name: --
    Protocol: BGP
    Nexthop interface : Vlan-Interface4
```

Display information about track entries in Negative state.

```
<Switch> display track all negative brief
ID   Status   Type      Remote IP/URL   Local IP        Interface
1    Negative Interface --              --              Vlan2
10   Negative Interface --              --              Vlan3
```

Table 9-1 Command output

Field	Description
Track ID	ID of a track entry.
State	States of a track entry: • **Positive**—The tracked object operates correctly. • **NotReady**—The tracked object is invalid. • **Negative**—The tracked object is abnormal.
Duration	Time period during which the track entry stays in the state.
Notification delay: Positive 20, Negative 30 (in seconds)	• The Track module notifies the application modules that the status of the track entry changes to Positive after a delay time of 20 seconds. • The Track module notifies the application modules that the status of the track entry changes to Negative after a delay time of 30 seconds.
Tracked object	Tracked object associated with the track entry.
NQA entry	NQA operation associated with the track entry.

Field	Description
Reaction	Reaction entry associated with the track entry.
BFD session mode	BFD session mode. Only echo mode is supported.
Outgoing interface	Outgoing interface of BFD echo packets.
VPN instance name	Name of the VPN instance to which BFD session packets belong. If the packets belong to the public network, two consecutive hyphens (--) are displayed.
Remote IP/URL	Remote IP address or URL. If no remote IP address or URL exists, two consecutive hyphens (--) are displayed.
Local IP	Local IP address. If no local IP address exists, two consecutive hyphens (--) are displayed.
Interface	Interface to be monitored. If no interface is to be monitored, two consecutive hyphens (--) are displayed.
Protocol	Link states or Layer 3 protocol states of the monitored interface: • **None**—Link status of the monitored interface. • **IPv4**—IPv4 protocol status of the monitored Layer 3 interface. • **IPv6**—IPv6 protocol status of the monitored Layer 3 interface.
IP route	Route associated with the track entry.
VPN instance name	Name of the VPN instance to which the route belongs. If the route belongs to the public network, two consecutive hyphens (--) are displayed.
Protocol	Protocol type of the route. If the route does not exist, **N/A** is displayed.
Nexthop interface	Next hop of the route. If the route does not exist, **N/A** is displayed.
LLDP interface	Monitored LLDP interface.
Type	Monitored object type: • BFD. • CFD. • Interface. • LLDP. • NQA. • Route.

Related commands

`track bfd`

`track interface`

`track interface protocol`

`track nqa`

9.1.2. track bfd

Use **`track bfd`** to create a track entry and associate it with a BFD session.

Use **undo track** to remove the track entry.

Syntax

track *track-entry-number* **bfd echo interface** *interface-type interface-number* **remote ip** *remote-ip-address* **local ip** *local-ip-address* [**delay** { **negative** *negative-time* | **positive** *positive-time* } *]

undo track *track-entry-number*

Default

No track entries exist.

Views

System view

Predefined user roles

network-admin

Parameters

track-entry-number: Specifies the track entry ID in the range of 1 to 1024.

interface *interface-type interface-number*: Specifies the outgoing interface by its type and number of the BFD echo packets.

remote ip *remote-ip-address*: Specifies the destination IP address of the BFD echo packets.

local ip *local-ip-address*: Specifies the source IP address of the BFD echo packets.

delay: Specifies the delay before the Track module notifies the application modules of the track entry state change. If you do not specify this keyword, the Track module notifies the application modules immediately when the track entry state changes.

negative *negative-time*: Specifies the delay before the Track module notifies the application modules that the track entry state has changed to Negative. The *negative-time* argument represents the notification delay in the range of 1 to 300 seconds.

positive *positive-time*: Specifies the delay before the Track module notifies the application modules that the track entry state has changed to Positive. The *positive-time* argument represents the notification delay in the range of 1 to 300 seconds.

Usage guidelines

After a track entry is created, you can only use the **track bfd delay** command to modify its notification delay settings. If you execute the **track bfd delay** command multiple times, the most recent configuration takes effect.

To modify other settings for the track entry, execute the **undo track** command to remove the track entry, and then execute the **track bfd** command again.

When you associate Track with BFD, the virtual IP address of a VRRP group cannot be the local or remote address of a BFD session.

Examples

Associate track entry 1 with BFD to monitor the link between local IP address 1.1.1.2 and remote IP address 1.1.1.1 by sending BFD echo packets through VLAN-interface 2.

```
<Switch> system-view
[Switch] track 1 bfd echo interface vlan-interface 2 remote ip 1.1.1.1 local ip 1.1.1.2
```

Related commands

display track

9.1.3. track interface

Use **track interface** to create a track entry and associate it with the link state of an interface.

Use **undo track** to remove the track entry.

Syntax

track *track-entry-number* **interface** *interface-type interface-number* [**delay** { **negative** *negative-time* | **positive** *positive-time* } *]

undo track *track-entry-number*

Default

No track entries exist.

Views

System view

Predefined user roles

network-admin

Parameters

track-entry-number: Specifies the track entry ID in the range of 1 to 1024.

interface-type interface-number: Specifies an interface by its type and number.

delay: Specifies the delay before the Track module notifies the application modules of the track entry state change. If you do not specify this keyword, the Track module notifies the application modules immediately when the track entry state changes.

negative *negative-time*: Specifies the delay before the Track module notifies the application modules that the track entry state has changed to Negative. The *negative-time* argument represents the notification delay in the range of 1 to 300 seconds.

positive *positive-time*: Specifies the delay before the Track module notifies the application modules that the track entry state has changed to Positive. The *positive-time* argument represents the notification delay in the range of 1 to 300 seconds.

Usage guidelines

When you associate Track with interface management to monitor the link status of an interface, the track entry state changes as follows:

- The track entry state is Positive if the link state of the interface is up.
- The track entry state is Negative if the link state of the interface is down.

To display the link state of an interface, use the **display ip interface brief** command.

After a track entry is created, you can only use the **track interface delay** command to modify its notification delay settings. If you execute the **track interface delay** command multiple times, the most recent configuration takes effect.

To modify other settings for the track entry, execute the **undo track** command to remove the track entry, and then execute the **track interface** command again.

Examples

Create track entry 1 and associate it with the link state of interface VLAN-interface 10.

```
<Switch> system-view
[Switch] track 1 interface vlan-interface 10
```

Related commands

display ip interface brief (*Layer 3—IP Services Command Reference*)

display track

9.1.4. track interface protocol

Use **track interface protocol** to create a track entry and associate it with the protocol state of an interface.

Use **undo track** to remove the track entry.

Syntax

track *track-entry-number* **interface** *interface-type interface-number* **protocol** { **ipv4** | **ipv6** } [**delay** { **negative** *negative-time* | **positive** *positive-time* } *]

undo track *track-entry-number*

Default

No track entries exist.

Views

System view

Predefined user roles

network-admin

Parameters

track-entry-number: Specifies the track entry ID in the range of 1 to 1024.

interface-type interface-number: Specifies an interface by its type and number.

ipv4: Monitors the IPv4 protocol state. When the IPv4 protocol state of an interface is up, the state of the track object is Positive. When the IPv4 protocol state of an interface is down, the state of the track object is Negative. To display the IPv4 protocol state of an interface, use the **display ip interface brief** command.

ipv6: Monitors the IPv6 protocol state. When the IPv6 protocol state of an interface is up, the state of the track object is Positive. When the IPv6 protocol state of an interface is down, the state of the track object is Negative. To display the IPv6 protocol state of an interface, use the **display ipv6 interface brief** command.

delay: Specifies the delay before the Track module notifies the application modules of the track entry state change. If you do not specify this keyword, the Track module notifies the application modules immediately when the track entry state changes.

negative *negative-time*: Specifies the delay before the Track module notifies the application modules that the track entry state has changed to Negative. The *negative-time* argument represents the notification delay in the range of 1 to 300 seconds.

positive *positive-time*: Specifies the delay before the Track module notifies the application modules that the track entry state has changed to Positive. The *positive-time* argument represents the notification delay in the range of 1 to 300 seconds.

Usage guidelines

After a track entry is created, you can only use the **track interface protocol delay** command to modify its notification delay settings. If you execute the **track interface protocol delay** command multiple times, the most recent configuration takes effect.

To modify other settings for the track entry, execute the **undo track** command to remove the track entry, and then execute the **track interface protocol** command again.

Examples

Create track entry 1 and associate it with the IPv4 protocol state of interface VLAN-interface 2.

```
<Switch> system-view
[Switch] track 1 interface vlan-interface 2 protocol ipv4
```

Related commands

display ip interface brief (*Layer 3—IP Services Command Reference*)

display ipv6 interface brief (*Layer 3—IP Services Command Reference*)

display track

9.1.5. track nqa

Use **track nqa** to create a track entry and associate it with the reaction entry of an NQA operation.

Use **undo track** to remove the track entry.

Syntax

track *track-entry-number* **nqa entry** *admin-name operation-tag* **reaction** *item-number*

undo track *track-entry-number*

Default

No track entries exist.

Views

System view

Predefined user roles

network-admin

Parameters

track-entry-number: Specifies the track entry ID in the range of 1 to 1024.

entry *admin-name operation-tag*: Specifies the NQA operation to be associated with the track entry. The *admin-name* argument specifies the name of the NQA operation administrator who creates the NQA operation, and is a case-insensitive string of 1 to 32 characters. The *operation-tag* argument specifies the NQA operation tag, and is a case-insensitive string of 1 to 32 characters.

reaction *item-number*: Specifies the reaction entry to be associated with the track entry. The *item-number* argument is the reaction entry ID in the range of 1 to 10.

Usage guidelines

To modify the track entry, execute the **undo track** command to remove the track entry, and then execute the **track nqa** command again.

Examples

Create track entry 1 and associate it with reaction entry 3 of the NQA operation **admin-test**.

```
<Switch> system-view
[Switch] track 1 nqa entry admin test reaction 3
```

Related commands

display track

QX-S5600G Series Ethernet Switches

Command References

11.Network Management and Monitoring

This manual is including the following chapters.

01-Ping, tracert, and system debugging commands

02-NQA commands

03-NTP commands

04-SNMP commands

05-RMON commands

06-NETCONF commands

07-Process monitoring and maintenance commands

08-Port mirroring commands

09-Flow mirroring commands

10-sFlow commands

11-Information center commands

12-NetMeister commands

13- VCF fabric commands

Contents

A page of this section is **11-x-x**

1. Ping, tracert, and system debugging commands ····· 1-1
1.1. Ping, tracert, and system debugging commands ····· 1-1
1.1.1. debugging ····· 1-1
1.1.2. display debugging ····· 1-2
1.1.3. ping ····· 1-2
1.1.4. ping ipv6 ····· 1-5
1.1.5. tracert ····· 1-7
1.1.6. tracert ipv6 ····· 1-9

1. Ping, tracert, and system debugging commands

1.1. Ping, tracert, and system debugging commands

1.1.1. debugging

Use **debugging** to enable debugging for a module.

Use **undo debugging** to disable debugging for a module or for all modules.

Syntax

debugging *module-name* [*option*]

undo debugging { **all** | *module-name* [*option*] }

Default

Debugging is disabled for all modules.

Views

User view

Predefined user roles

network-admin

Parameters

module-name: Specifies a module by its name, such as **arp** or **device**. For a list of supported modules, use the **debugging ?** command.

option: Specifies the debugging option for a module. Available options vary by module. To display the debugging options supported by a module, use the **debugging** *module-name* **?** command.

all: Specifies all modules.

Usage guidelines

Output from debugging commands is memory intensive. To guarantee system performance, enable debugging only for modules that are in an exceptional condition.

The system sends generated debug messages to the device information center, which then sends the messages to appropriate destinations based on the log output configuration. For more information about the information center, see *Network Management and Monitoring Configuration Guide*.

Examples

Enable debugging for the device management module.

```
<Switch> debugging dev
```

Related commands

display debugging

1.1.2. display debugging

Use **display debugging** to display the enabled debugging features for a module or for all modules.

Syntax

display debugging [*module-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

module-name: Specifies a module by its name. For a list of supported modules, use the **display debugging ?** command. If you do not specify a module name, this command displays the enabled debugging features for all modules.

Examples

Display all enabled debugging features.

```
<Switch> display debugging
DEV debugging switch is on
```

Related commands

debugging

1.1.3. ping

Use **ping** to test the reachability of the destination IP address and display ping statistics.

Syntax

ping [**ip**] [**-a** *source-ip* | **-c** *count* | **-f** | **-h** *ttl* | **-i** *interface-type interface-number* | **-m** *interval* | **-n** | **-p** *pad* | **-q** | **-r** | **-s** *packet-size* | **-t** *timeout* | **-tos** *tos* | **-v** | **-vpn-instance** *vpn-instance-name*] * *host*

Views

Any view

Predefined user roles

network-admin

Parameters

ip: Distinguishes between a destination host name and the **ping** command keywords if the name of the destination host is **i**, **ip**, **ipv**, **ipv6**, **l**, **ls**, or **lsp**. For example, you must use the command in the form of **ping ip ip** instead of **ping ip** if the destination host name is **ip**.

-a *source-ip*: Specifies an IP address of the device as the source IP address of ICMP echo requests. If this option is not specified, the source IP address of ICMP echo requests is the primary IP address of the outbound interface.

-c *count*: Specifies the number of ICMP echo requests that are sent to the destination. The value range is 1 to 4294967295, and the default is 5.

-f: Sets the "do-not-fragment" bit in the IP header.

-h *ttl*: Specifies the TTL value of ICMP echo requests. The value range is 1 to 255, and the default is 255.

-i *interface-type interface-number*: Specifies the source interface for ICMP echo requests. If you do not specify this option, the system uses the primary IP address of the matching route's egress interface as the source interface for ICMP echo requests.

-m *interval*: Specifies the interval (in milliseconds) to send ICMP echo requests. The value range is 1 to 65535, and the default is 200.

-n: Disables domain name resolution for the *host* argument. If the *host* argument represents the host name of the destination, and if this keyword is not specified, the device translates *host* into an address.

-p *pad*: Specifies the value of the **pad** field in an ICMP echo request, in hexadecimal format, 1 to 8 bits. The *pad* argument is in the range of 0 to ffffffff. If the specified value is less than 8 bits, 0s are added in front of the value to extend it to 8 bits. For example, if *pad* is configured as 0x2f, then the packets are padded with 0x0000002f to make the total length of the packet meet the requirements of the device. By default, the padded value starts from 0x01 up to 0xff, where another round starts again if necessary, such as 0x010203…feff01….

-q: Displays only the summary statistics. If this keyword is not specified, the system displays all the ping statistics.

-r: Records the addresses of the hops (up to 9) the ICMP echo requests passed. If this keyword is not specified, the addresses of the hops that the ICMP echo requests passed are not recorded.

-s *packet-size*: Specifies the length (in bytes) of ICMP echo requests (excluding the IP packet header and the ICMP packet header). The value range is 20 to 8100, and the default is 56.

-t *timeout*: Specifies the timeout time (in milliseconds) of an ICMP echo reply. The value range is 0 to 65535, and the default is 2000. If the source does not receive an ICMP echo reply within the timeout, it considers the ICMP echo reply timed out.

-tos *tos*: Specifies the ToS value of ICMP echo requests. The value range is 0 to 255, and the default is 0.

-v: Displays non-ICMP echo reply packets. If this keyword is not specified, the system does not display non-ICMP echo reply packets.

-vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance to which the destination belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. If the destination is on the public network, do not specify this option.

host: Specifies the IP address or host name of the destination. The host name is a case-insensitive string of 1 to 253 characters. It can contain letters, digits, and special characters such as hyphen (-), underscore (_), and dot (.).

Usage guidelines

To ping a device identified by its host name, configure the DNS settings on the device first. If the DNS settings are not configured, the ping operation fails.

To abort the ping operation during the execution of the command, press **Ctrl+C**.

Examples

Test whether the device with an IP address of 1.1.2.2 is reachable.

```
<Switch> ping 1.1.2.2
Ping 1.1.2.2 (1.1.2.2): 56 data bytes, press CTRL_C to break
56 bytes from 1.1.2.2: icmp_seq=0 ttl=254 time=2.137 ms
```

```
56 bytes from 1.1.2.2: icmp_seq=1 ttl=254 time=2.051 ms
56 bytes from 1.1.2.2: icmp_seq=2 ttl=254 time=1.996 ms
56 bytes from 1.1.2.2: icmp_seq=3 ttl=254 time=1.963 ms
56 bytes from 1.1.2.2: icmp_seq=4 ttl=254 time=1.991 ms

--- Ping statistics for 1.1.2.2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.963/2.028/2.137/0.062 ms
```

Test whether the device with an IP address of 1.1.2.2 is reachable. Only results are displayed.

```
<Switch> ping -q 1.1.2.2
Ping 1.1.2.2 (1.1.2.2): 56 data bytes, press CTRL_C to break

--- Ping statistics for 1.1.2.2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.962/2.196/2.665/0.244 ms
```

Test whether the device with an IP address of 1.1.2.2 is reachable. The IP addresses of the hops that the ICMP packets passed in the path are displayed.

```
<Switch> ping -r 1.1.2.2
Ping 1.1.2.2 (1.1.2.2): 56 data bytes, press CTRL_C to break
56 bytes from 1.1.2.2: icmp_seq=0 ttl=254 time=4.685 ms
RR:      1.1.2.1
         1.1.2.2
         1.1.1.2
         1.1.1.1
56 bytes from 1.1.2.2: icmp_seq=1 ttl=254 time=4.834 ms  (same route)
56 bytes from 1.1.2.2: icmp_seq=2 ttl=254 time=4.770 ms  (same route)
56 bytes from 1.1.2.2: icmp_seq=3 ttl=254 time=4.812 ms  (same route)
56 bytes from 1.1.2.2: icmp_seq=4 ttl=254 time=4.704 ms  (same route)

--- Ping statistics for 1.1.2.2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 4.685/4.761/4.834/0.058 ms
```

The output shows the following information:

- The destination is reachable.
- The route is 1.1.1.1 <-> {1.1.1.2; 1.1.2.1} <-> 1.1.2.2.

Table 1-1 Command output

Field	Description
Ping 1.1.2.2 (1.1.2.2): 56 data bytes, press CTRL_C to break	Test whether the device with IP address 1.1.2.2 is reachable. There are 56 bytes in each ICMP echo request. Press **Ctrl+C** to abort the ping operation.
56 bytes from 1.1.2.2: icmp_seq=0 ttl=254 time=4.685 ms	Received ICMP echo replies from the device whose IP address is 1.1.2.2. If no echo reply is received within the timeout period, no information is displayed. • **bytes**—Number of bytes in the ICMP echo reply. • **icmp_seq**—Packet sequence, used to determine whether a segment is lost, disordered or repeated. • **ttl**—TTL value in the ICMP echo reply.

Field	Description
	• **time**—Response time.
RR:	Routers through which the ICMP echo request passed. They are displayed in inversed order, which means the router with a smaller distance to the destination is displayed first.
--- Ping statistics for 1.1.2.2 ---	Statistics on data received and sent in the ping operation.
--- Ping statistics for 1.1.2.2 in VPN instance vpn1 ---	Ping statistics for a device in a VPN instance.
5 packet(s) transmitted	Number of ICMP echo requests sent.
5 packet(s) received	Number of ICMP echo replies received.
0.0% packet loss	Percentage of unacknowledged packets to the total packets sent.
round-trip min/avg/max/std-dev = 4.685/4.761/4.834/0.058 ms	Minimum/average/maximum/standard deviation response time, in milliseconds.

1.1.4. ping ipv6

Use **ping ipv6** to test the reachability of the destination IPv6 address and display IPv6 ping statistics.

Syntax

ping ipv6 [**-a** *source-ipv6* | **-c** *count* | **-i** *interface-type interface-number* | **-m** *interval* | **-q** | **-s** *packet-size* | **-t** *timeout* | **-v** | **-vpn-instance** *vpn-instance-name*] * *host*

Views

Any view

Predefined user roles

network-admin

Parameters

-a *source-ipv6*: Specifies an IPv6 address of the device as the source IP address of ICMP echo requests. If this option is not specified, the source IPv6 address of ICMP echo requests is the IPv6 address of the outbound interface. See RFC 3484 for information about the address selection rule.

-c *count*: Specifies the number of ICMPv6 echo requests that are sent to the destination. The value range is 1 to 4294967295, and the default is 5.

-i *interface-type interface-number*: Specifies the source interface for ICMPv6 echo requests. This option must be specified when the destination address is a multicast address or a link local address. If you do not specify this option, the system uses the primary IP address of the matching route's egress interface as the source interface for ICMPv6 echo requests.

-m *interval*: Specifies the interval (in milliseconds) to send an ICMPv6 echo reply. The value range is 1 to 65535, and the default is 1000.

-q: Displays only the summary statistics. If you do not specify this keyword, the system displays all the ping statistics.

-s *packet-size*: Specifies the length (in bytes) of ICMPv6 echo requests (excluding the IPv6 packet header and the ICMPv6 packet header). The value range is 20 to 8100, and the default is 56.

-t *timeout*: Specifies the timeout time (in milliseconds) of an ICMPv6 echo reply. The value range is 0 to 65535, and the default is 2000.

-v: Displays detailed information (including the **dst** field and the **idx** field) about ICMPv6 echo replies. If this keyword is not specified, the system only displays brief information (not including the **dst** field and the **idx** field) about ICMPv6 echo replies.

-vpn-instance *vpn-instance-name*: Specifies a VPN instance to which the destination belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. If the destination is on the public network, do not specify this option.

host: Specifies the IPv6 address or host name of the destination. The host name is a case-insensitive string of 1 to 253 characters. It can contain letters, digits, and special characters such as hyphen (-), underscore (_), and dot (.).

Usage guidelines

To ping a device identified by its host name, configure the DNS settings on the device first. If the DNS settings are not configured, the ping ipv6 operation fails.

To abort the ping ipv6 operation during the execution of the command, press **Ctrl+C**.

Examples

Test whether the IPv6 address (2001::2) is reachable.

```
<Switch> ping ipv6 2001::2
Ping6(56 data bytes) 2001::1 --> 2001::2, press CTRL_C to break
56 bytes from 2001::2, icmp_seq=0 hlim=64 time=62.000 ms
56 bytes from 2001::2, icmp_seq=1 hlim=64 time=23.000 ms
56 bytes from 2001::2, icmp_seq=2 hlim=64 time=20.000 ms
56 bytes from 2001::2, icmp_seq=3 hlim=64 time=4.000 ms
56 bytes from 2001::2, icmp_seq=4 hlim=64 time=16.000 ms

--- Ping6 statistics for 2001::2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 4.000/25.000/62.000/20.000 ms
```

Test whether the IPv6 address (2001::2) is reachable. Only the statistics are displayed.

```
<Switch> ping ipv6 -q 2001::2
Ping6(56 data bytes) 2001::1 --> 2001::2, press CTRL_C to break

--- Ping6 statistics for 2001::2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 4.000/25.000/62.000/20.000 ms
```

Test whether the IPv6 address (2001::2) is reachable. Detailed ping information is displayed.

```
<Switch> ping ipv6 -v 2001::2
Ping6(56 data bytes) 2001::1 --> 2001::2, press CTRL_C to break
56 bytes from 2001::2, icmp_seq=0 hlim=64 dst=2001::1 idx=3 time=62.000 ms
56 bytes from 2001::2, icmp_seq=1 hlim=64 dst=2001::1 idx=3 time=23.000 ms
56 bytes from 2001::2, icmp_seq=2 hlim=64 dst=2001::1 idx=3 time=20.000 ms
56 bytes from 2001::2, icmp_seq=3 hlim=64 dst=2001::1 idx=3 time=4.000 ms
56 bytes from 2001::2, icmp_seq=4 hlim=64 dst=2001::1 idx=3 time=16.000 ms

--- Ping6 statistics for 2001::2 ---
```

```
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 4.000/25.000/62.000/20.000 ms
```

Table 1-2 Command output

Field	Description
Ping6(56 data bytes) 2001::1 --> 2001::2, press CTRL_C to break	An ICMPv6 echo reply with a data length of 56 bytes is sent from 2001::1 to 2001::2. Press **Ctrl+C** to abort the ping IPv6 operation.
56 bytes from 2001::2, icmp_seq=1 hlim=64 dst=2001::1 idx=3 time=62.000 ms	Received ICMPv6 echo replies from the device whose IPv6 address is 2001::2. • The number of data bytes is 56. • The packet sequence is 1. • The hop limit value is 64. • The destination address is 2001::1. Specify the **-v** keyword to display this field. • The index for the packet inbound interface is 3. Specify the **-v** keyword to display this field. • The response time is 62 milliseconds.
--- Ping6 statistics for 2001::2 ------	Statistics on data received and sent in an IPv6 ping operation.
5 packet(s) transmitted	Number of ICMPv6 echo requests sent.
5 packet(s) received	Number of ICMPv6 echo replies received.
0.0% packet loss	Percentage of unacknowledged packets to the total packets sent.
round-trip min/avg/max/ std-dev =4.000/25.000/62.000/20.000 ms	Minimum/average/maximum/standard deviation response time, in milliseconds.

1.1.5. tracert

Use **tracert** to trace the path that the packets traverse from source to destination.

Syntax

tracert [**-a** *source-ip* | **-f** *first-ttl* | **-m** *max-ttl* | **-p** *port* | **-q** *packet-number* || **-t** *tos* | **-vpn-instance** *vpn-instance-name* [**-resolve-as** { **global** | **none** | **vpn** }] | **-w** *timeout*] * *host*

Views

Any view

Predefined user roles

network-admin

Parameters

-a *source-ip*: Specifies an IP address of the device as the source IP address of probe packets. If this option is not specified, the source IP address of probe packets is the primary IP address of the outbound interface.

-f *first-ttl*: Specifies the TTL of the first packet sent to the destination. The value range is 1 to 255, and the default is 1. It must be no greater than the value of the *max-ttl* argument.

-m *max-ttl*: Specifies the maximum number of hops allowed for a probe packet. The value range is 1 to 255, and the default is 30. It must be no smaller than the value of the *first-ttl* argument.

-p *port*: Specifies an invalid UDP port of the destination. The value range is 1 to 65535, and the default is 33434.

-q *packet-number*: Specifies the number of probe packets to send per hop. The value range is 1 to 65535, and the default is 3.

-t *tos*: Specifies the ToS value of probe packets. The value range is 0 to 255, and the default is 0.

-vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance to which the destination belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. If the destination is on the public network, do not specify this option.

-resolve-as: Specifies a routing table for autonomous system (AS) resolution. Tracert searches the specified routing table for the AS that each hop along the path belongs to. If you do not specify this keyword, the global routing table is used. If the AS information is found, this command displays the AS number next to the address of the hop in the probe result.

- **global**: Specifies the global routing table.
- **none**: Disables AS resolution.

vpn: Specifies the VPN routing table.

-w *timeout*: Specifies the timeout time in milliseconds of the reply packet for a probe packet. The value range is 1 to 65535, and the default is 5000.

host: Specifies the IP address or host name of the destination. The host name is a case-insensitive string of 1 to 253 characters. It can contain letters, digits, and special characters such as hyphen (-), underscore (_), and dot (.).

Usage guidelines

After identifying network failure with the **ping** command, use the **tracert** command to locate failed nodes.

If the destination address is on a private network, address information of intermediate hops might be stored in either the global routing table.

The output from the **tracert** command includes IP addresses of all the Layer 3 devices that the packets traverse from source to destination. Asterisks (* * *) are displayed if the device cannot reply with an ICMP error message. The reason might be the destination is unreachable or sending ICMP timeout/destination unreachable packets is disabled.

To abort the tracert operation during the execution of the command, press **Ctrl+C**.

Examples

Display the path that the packets traverse from source to destination (1.1.2.2).

```
<Switch> tracert 1.1.2.2
traceroute to 1.1.2.2 (1.1.2.2), 30 hops at most, 40 bytes each packet, press CTRL_C to
break
 1  1.1.1.2 (1.1.1.2) 673 ms 425 ms 30 ms
 2  1.1.2.2 (1.1.2.2) [AS 100] 580 ms 470 ms 80 ms
```

Table 1-3 Command output

Field	Description
traceroute to 1.1.2.2 (1.1.2.2)	Display the route that the IP packets traverse from the current device to the device whose IP address is 1.1.2.2.

Field	Description
hops at most	Maximum number of hops of the probe packets, which can be set by the **-m** keyword.
bytes each packet	Number of bytes of a probe packet.
press CTRL_C to break	During the execution of the command, press **Ctrl+C** to abort the tracert operation.
2 1.1.2.2 (1.1.2.2) [AS 100] 580 ms 470 ms 80 ms	Probe result of the probe packets that contain a TTL value of 2, including the following information about the second hop: • Domain name of the hop. If no domain name is configured, the IP address is displayed as the domain name. • IP address of the hop. The IP address is displayed in parentheses. • Number of the AS that the hop belongs to. The AS number appears only when it is found for the hop in the specified routing table. • The round-trip time of the probe packets. The number of packets that can be sent in each probe can be set by using the **-q** keyword.

1.1.6. tracert ipv6

Use **tracert ipv6** to display the path that the IPv6 packets traverse from source to destination.

Syntax

tracert ipv6 [**-f** *first-hop* | **-m** *max-hops* | **-p** *port* | **-q** *packet-number* | **-t** *traffic-class* | **-vpn-instance** *vpn-instance-name* | **-w** *timeout*] * *host*

Views

Any view

Predefined user roles

network-admin

Parameters

-f *first-hop*: Specifies the TTL value of the first packet. The value range is 1 to 255, and the default is 1. The value must be no greater than the value of the *max-hops* argument.

-m *max-hops*: Specifies the maximum number of hops allowed for a packet. The value range is 1 to 255, and the default is 30. The value must be no smaller than the value of the *first-hop* argument.

-p *port*: Specifies an invalid UDP port of the destination. The value range is 1 to 65535, and the default is 33434.

-q *packet-number*: Specifies the number of probe packets sent each time. The value range is 1 to 65535, and the default is 3.

-t *traffic-class*: Specifies the traffic class value in an IPv6 probe packet. The value range is 0 to 255, and the default is 0.

-vpn-instance *vpn-instance-name*: Specifies a VPN instance to which the destination belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. If the destination is on the public network, do not specify this option.

-w *timeout*: Specifies the timeout time (in milliseconds) of the reply packet of a probe packet. The value range is 1 to 65535, and the default is 5000.

host: Specifies the IPv6 address or host name of the destination. The host name is a case-insensitive string of 1 to 253 characters. It can contain letters, digits, and special characters such as hyphen (-), underscore (_), and dot (.).

Usage guidelines

After identifying network failure with the **ping ipv6** command, you can use the **tracert ipv6** command to locate failed nodes.

If the destination address is on a private network, address information of intermediate hops might be stored in either the global routing table or the VPN routing table.

The output from the **tracert ipv6** command includes IPv6 addresses of all the Layer 3 devices that the packets traverse from source to destination. Asterisks (* * *) are displayed if the device cannot reply with an ICMP error message. The reason might be the destination is unreachable or sending ICMP timeout/destination unreachable packets is disabled.

To abort the tracert operation during the execution of the command, press **Ctrl+C**.

Examples

Display the path that the packets traverse from source to destination (2001:3::2).

```
<Switch> tracert ipv6 2001:3::2
traceroute to 2001:3::2(2001:3::2), 30 hops at most, 60 byte packets, press CTRL_C to break
 1  2001:1::2  0.661 ms  0.618 ms  0.579 ms
 2  2001:2::2 [AS 100]  0.861 ms  0.718 ms  0.679 ms
 3  2001:3::2 [AS 200]  0.822 ms  0.731 ms  0.708 ms
```

Table 1-4 Command output

Field	Description
traceroute to 2001:3::2	Display the route that the IPv6 packets traverse from the current device to the device whose IP address is 2001:3:2.
hops at most	Maximum number of hops of the probe packets, which can be set by the **-m** keyword.
byte packets	Number of bytes of a probe packet.
2 2001:2::2 [AS 100] 0.861 ms 0.718 ms 0.679 ms	Probe result of the probe packets that contain a hoplimit value of 2, including the following information about the second hop: • IPv6 address of the hop. • Number of the AS the hop belongs to. The AS number appears only when it is found for the hop in the specified routing table. • The round-trip time of the probe packets. The number of packets that can be sent in each probe can be set by using the **-q** keyword.

Contents

A page of this section is **11-x-x**

2. NQA commands ····· 2-1
2.1. NQA client commands ····· 2-1
2.1.1. advantage-factor ····· 2-1
2.1.2. codec-type ····· 2-1
2.1.3. data-fill ····· 2-2
2.1.4. data-size ····· 2-3
2.1.5. description ····· 2-4
2.1.6. destination ip ····· 2-4
2.1.7. destination port ····· 2-5
2.1.8. display nqa history ····· 2-6
2.1.9. display nqa result ····· 2-7
2.1.10. display nqa statistics ····· 2-11
2.1.11. filename ····· 2-18
2.1.12. frequency ····· 2-18
2.1.13. history-record enable ····· 2-19
2.1.14. history-record keep-time ····· 2-20
2.1.15. history-record number ····· 2-20
2.1.16. next-hop ip ····· 2-21
2.1.17. nqa ····· 2-22
2.1.18. nqa agent enable ····· 2-22
2.1.19. nqa schedule ····· 2-23
2.1.20. operation (FTP operation view) ····· 2-24
2.1.21. operation (HTTP operation view) ····· 2-25
2.1.22. password ····· 2-26
2.1.23. probe count ····· 2-26
2.1.24. probe packet-interval ····· 2-28
2.1.25. probe packet-number ····· 2-28
2.1.26. probe packet-timeout ····· 2-29
2.1.27. probe timeout ····· 2-29
2.1.28. reaction checked-element probe-fail (for trap) ····· 2-30
2.1.29. reaction checked-element probe-fail (for trigger) ····· 2-31
2.1.30. reaction trap ····· 2-32
2.1.31. resolve-target ····· 2-33
2.1.32. route-option bypass-route ····· 2-34
2.1.33. source interface (ICMP echo operation view) ····· 2-34
2.1.34. source ip ····· 2-35
2.1.35. source port ····· 2-36
2.1.36. statistics hold-time ····· 2-36
2.1.37. statistics interval ····· 2-37
2.1.38. statistics max-group ····· 2-38
2.1.39. tos ····· 2-39
2.1.40. ttl ····· 2-39
2.1.41. type ····· 2-40
2.1.42. url ····· 2-41
2.1.43. username ····· 2-41
2.1.44. version ····· 2-42
2.1.45. vpn-instance ····· 2-43
2.2. NQA server commands ····· 2-43
2.2.1. display nqa server ····· 2-44
2.2.2. nqa server enable ····· 2-44
2.2.3. nqa server tcp-connect ····· 2-45
2.2.4. nqa server udp-echo ····· 2-46

2. NQA commands

2.1. NQA client commands

2.1.1. advantage-factor

Use **advantage-factor** to set the advantage factor to be used for calculating Mean Opinion Scores (MOS) and Calculated Planning Impairment Factor (ICPIF) values.

Use **undo advantage-factor** to restore the default.

Syntax

advantage-factor *factor*

undo advantage-factor

Default

The advantage factor is 0.

Views

Voice operation view

Predefined user roles

network-admin

Parameters

factor: Specifies the advantage factor in the range of 0 to 20.

Usage guidelines

The evaluation of voice quality depends on users' tolerance for voice quality. For users with higher tolerance for voice quality, use the **advantage-factor** command to set an advantage factor. When the system calculates the ICPIF value, it subtracts the advantage factor to modify ICPIF and MOS values for voice quality evaluation.

Examples

Set the advantage factor to 10 for the voice operation.

```
<Switch> system-view
[Switch] nqa entry admin test
[Switch-nqa-admin-test] type voice
[Switch-nqa-admin-test-voice] advantage-factor 10
```

2.1.2. codec-type

Use **codec-type** to configure the codec type for the voice operation.

Use **undo codec-type** to restore the default.

Syntax

codec-type { **g711a** | **g711u** | **g729a** }

undo codec-type

Default

The codec type for the voice operation is G.711 A-law.

Views

Voice operation view

Predefined user roles

network-admin

Parameters

g711a: Specifies G.711 A-law codec type.

g711u: Specifies G.711 μ-law codec type

g729a: Specifies G.729 A-law codec type.

Examples

Set the codec type to **g729a** for the voice operation.

```
<Switch> system-view
[Switch] nqa entry admin test
[Switch-nqa-admin-test] type voice
[Switch-nqa-admin-test-voice] codec-type g729a
```

2.1.3. data-fill

Use **data-fill** to configure the payload fill string for probe packets.

Use **undo data-fill** to restore the default.

Syntax

data-fill *string*

undo data-fill

Default

The default payload fill string is the hexadecimal string 00010203040506070809.

Views

ICMP/UDP echo operation view

UDP jitter/voice operation view

Predefined user roles

network-admin

Parameters

string: Specifies a case-sensitive string of 1 to 200 characters.

Usage guidelines

If the payload length is smaller than the string length, only the first part of the string is filled. For example, if you configure the string as **abcd** and set the payload size to 3 bytes, **abc** is filled.

If the payload length is greater than the string length, the system fills the payload with the string cyclically until the payload is full. For example, if you configure the string as **abcd** and the payload size as 6 bytes, **abcdab** is filled.

How the string is filled depends on the operation type.

- For the ICMP echo operation, the string fills the whole payload of an ICMP echo request.
- For the UDP echo operation, the first five bytes of the payload of a UDP packet are for special purpose. The string fills the remaining part of payload.
- For the UDP jitter operation, the first 68 bytes of the payload of a UDP packet are for special purpose. The string fills the remaining part of the payload.
- For the voice operation, the first 16 bytes of the payload of a UDP packet are for special purpose. The string fills the remaining part of the payload.

Examples

Specify **abcd** as the payload fill string for ICMP echo requests.

```
<Switch> system-view
[Switch] nqa entry admin test
[Switch-nqa-admin-test] type icmp-echo
[Switch-nqa-admin-test-icmp-echo] data-fill abcd
```

2.1.4. data-size

Use **data-size** to set the payload size for each probe packet.

Use **undo data-size** to restore the default.

Syntax

data-size *size*

undo data-size

Default

The default payload size of a probe packet for different operations is described in Table 2-1 .

Table 2-1 Default payload size of a probe packet

Operation type	Codec type	Default size (bytes)
ICMP echo	N/A	100
UDP echo	N/A	100
UDP jitter	N/A	100
Voice	G.711 A-law	172
Voice	G.711 μ-law	172
Voice	G.729 A-law	32

Views

ICMP/UDP echo operation view

UDP jitter/voice operation view

Predefined user roles

network-admin

Parameters

size: Specifies the payload size. Available value ranges include:

- 20 to 65507 bytes for the ICMP echo, or UDP echo operation.
- 68 to 65507 bytes for the UDP jitter operation.

- 16 to 65507 bytes for the voice operation.

Usage guidelines

In ICMP echo operations, the command sets the payload size for each ICMP echo request.

In UDP echo, UDP jitter, and voice operations, the command sets the payload size for each UDP packet.

Examples

Set the payload size to 80 bytes for each ICMP echo request.

```
<Switch> system-view
[Switch] nqa entry admin test
[Switch-nqa-admin-test] type icmp-echo
[Switch-nqa-admin-test-icmp-echo] data-size 80
```

2.1.5. description

Use **description** to configure a description for an NQA operation, such as the operation type or purpose.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

No description is configured for an NQA operation.

Views

Any NQA operation view

Predefined user roles

network-admin

Parameters

text: Specifies a description, a case-sensitive string of 1 to 200 characters.

Examples

Configure the description as **icmp-probe** for the ICMP echo operation.

```
<Switch> system-view
[Switch] nqa entry admin test
[Switch-nqa-admin-test] type icmp-echo
[Switch-nqa-admin-test-icmp-echo] description icmp-probe
```

2.1.6. destination ip

Use **destination ip** to configure the destination IPv4 address for the operation.

Use **undo destination ip** to restore the default.

Syntax

destination ip *ip-address*

undo destination ip

Default

No destination IPv4 address is configured for an operation.

Views

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

UDP jitter/voice operation view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the destination IPv4 address for the operation.

Examples

Specify 10.1.1.1 as the destination IPv4 address for the ICMP echo operation.

```
<Switch> system-view
[Switch] nqa entry admin test
[Switch-nqa-admin-test] type icmp-echo
[Switch-nqa-admin-test-icmp-echo] destination ip 10.1.1.1
```

2.1.7. destination port

Use **destination port** to configure the destination port number for the operation.

Use **undo destination port** to restore the default.

Syntax

destination port *port-number*

undo destination port

Default

No destination port number is configured for other types of operations.

Views

TCP/UDP echo operation view

UDP jitter/voice operation view

Predefined user roles

network-admin

Parameters

port-number: Specifies the destination port number for the operation, in the range of 1 to 65535.

Examples

Set the destination port number to 9000 for the UDP echo operation.

```
<Switch> system-view
[Switch] nqa entry admin test
[Switch-nqa-admin-test] type udp-echo
[Switch-nqa-admin-test-udp-echo] destination port 9000
```

2.1.8. display nqa history

Use **display nqa history** to display the history records of NQA operations.

Syntax

display nqa history [*admin-name operation-tag*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

admin-name operation-tag: Specifies an NQA operation by its administrator name and operation tag. The *admin-name* argument represents the name of the administrator who creates the NQA operation. The *operation-tag* argument represents the operation tag. Each of the arguments is a case-insensitive string of 1 to 32 characters that cannot contain hyphens (-). If you do not specify an NQA operation, the command displays the history records of all NQA operations.

Usage guidelines

The **display nqa history** command does not display the results or statistics of the following operations:

- UDP jitter.
- Voice.

To view the results or statistics of the UDP jitter, and voice operations, use the **display nqa result** or **display nqa statistics** command.

Examples

Display the history records of the NQA operation with administrator name **administrator** and operation tag **test**.

```
<Switch> display nqa history administrator test
NQA entry (admin administrator, tag test) history records:
  Index      Response     Status           Time
  10         329          Succeeded        2011-04-29 20:54:26.5
  9          344          Succeeded        2011-04-29 20:54:26.2
  8          328          Succeeded        2011-04-29 20:54:25.8
  7          328          Succeeded        2011-04-29 20:54:25.5
  6          328          Succeeded        2011-04-29 20:54:25.1
  5          328          Succeeded        2011-04-29 20:54:24.8
  4          328          Succeeded        2011-04-29 20:54:24.5
  3          328          Succeeded        2011-04-29 20:54:24.1
  2          328          Succeeded        2011-04-29 20:54:23.8
  1          328          Succeeded        2011-04-29 20:54:23.4
```

Table 2-2 Command output

Field	Description
Index	History record ID.

Field	Description
TTL	TTL value in the probe packet.
Response	Round-trip time if the operation succeeds, timeout time upon timeout, or 0 if the operation cannot be completed, in milliseconds.
Hop IP	IP address of the node that sent the reply packet.
Status	Status of the operation result: • Succeeded. • Unknown error. • Internal error. • Timeout.
Time	Time when the operation was completed.

2.1.9. display nqa result

Use **display nqa result** to display the most recent result of an NQA operation.

Syntax

display nqa result [*admin-name operation-tag*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

admin-name operation-tag: Specifies an NQA operation by its administrator name and operation tag. The *admin-name* argument represents the name of the administrator who creates the NQA operation. The *operation-tag* argument represents the operation tag. Each of the arguments is a case-insensitive string of 1 to 32 characters that cannot contain hyphens (-). If you do not specify an NQA operation, the command displays the most recent results of all NQA operations.

Examples

Display the most recent result of the TCP operation with administrator name **admin** and operation tag **test**.

```
<Switch> display nqa result admin test
NQA entry (admin admin, tag test) test results:
    Send operation times: 1              Receive response times: 1
    Min/Max/Average round trip time: 35/35/35
    Square-Sum of round trip time: 1225
    Last succeeded probe time: 2011-05-29 10:50:33.2
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to disconnect: 0
    Failures due to no connection: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
```

Display the most recent result of the UDP jitter operation with administrator name **admin** and operation tag **test**.

```
<Switch> display nqa result admin test
NQA entry (admin admin, tag test) test results:
    Send operation times: 10             Receive response times: 10
    Min/Max/Average round trip time: 15/46/26
    Square-Sum of round trip time: 8103
    Last packet received time: 2011-05-29 10:56:38.7
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
    Packets out of sequence: 0
    Packets arrived late: 0
  UDP-jitter results:
   RTT number: 10
    Min positive SD: 8                   Min positive DS: 8
    Max positive SD: 18                  Max positive DS: 8
    Positive SD number: 5                Positive DS number: 2
    Positive SD sum: 75                  Positive DS sum: 32
    Positive SD average: 15              Positive DS average: 16
    Positive SD square-sum: 1189         Positive DS square-sum: 640
    Min negative SD: 8                   Min negative DS: 1
    Max negative SD: 24                  Max negative DS: 30
    Negative SD number: 4                Negative DS number: 7
    Negative SD sum: 56                  Negative DS sum: 99
    Negative SD average: 14              Negative DS average: 14
    Negative SD square-sum: 946          Negative DS square-sum: 1495
  One way results:
    Max SD delay: 22                     Max DS delay: 23
    Min SD delay: 7                      Min DS delay: 7
    Number of SD delay: 10               Number of DS delay: 10
    Sum of SD delay: 125                 Sum of DS delay: 132
    Square-Sum of SD delay: 1805         Square-Sum of DS delay: 1988
    SD lost packets: 0                   DS lost packets: 0
    Lost packets for unknown reason: 0
```

Display the most recent result of the voice operation with administrator name **admin** and operation tag **test**.

```
<Switch> display nqa result admin test
NQA entry (admin admin, tag test) test results:
    Send operation times: 1000           Receive response times: 0
    Min/Max/Average round trip time: 0/0/0
    Square-Sum of round trip time: 0
    Last packet received time: 0-00-00 00:00:00.0
  Extended results:
    Packet loss ratio: 100%
    Failures due to timeout: 1000
```

```
  Failures due to internal error: 0
  Failures due to other errors: 0
  Packets out of sequence: 0
  Packets arrived late: 0
Voice results:
 RTT number: 0
  Min positive SD: 0                    Min positive DS: 0
  Max positive SD: 0                    Max positive DS: 0
  Positive SD number: 0                 Positive DS number: 0
  Positive SD sum: 0                    Positive DS sum: 0
  Positive SD average: 0                Positive DS average: 0
  Positive SD square-sum: 0             Positive DS square-sum: 0
  Min negative SD: 0                    Min negative DS: 0
  Max negative SD: 0                    Max negative DS: 0
  Negative SD number: 0                 Negative DS number: 0
  Negative SD sum: 0                    Negative DS sum: 0
  Negative SD average: 0                Negative DS average: 0
  Negative SD square-sum: 0             Negative DS square-sum: 0
One way results:
  Max SD delay: 0                       Max DS delay: 0
  Min SD delay: 0                       Min DS delay: 0
  Number of SD delay: 0                 Number of DS delay: 0
  Sum of SD delay: 0                    Sum of DS delay: 0
  Square-Sum of SD delay: 0             Square-Sum of DS delay: 0
  SD lost packets: 0                    DS lost packets: 0
  Lost packets for unknown reason: 1000
Voice scores:
  MOS value: 0.99                       ICPIF value: 87
```

Table 2-3 Command output

Field	Description
Data collecting in progress	The operation is in progress.
Send operation times	Number of operations.
Receive response times	Number of response packets received.
Min/Max/Average round trip time	Minimum/maximum/average round-trip time in milliseconds.
Square-Sum of round trip time	Square sum of round-trip time.
Last succeeded probe time	Time when the last successful probe was completed. If no probes are successful in an operation, the field displays **0**. This field is not available for UDP jitter, and voice operations.
Last packet received time	Time when the last response packet was received. If no response packets in a probe were received, the field displays **0**. This field is available only for UDP jitter and voice operations.

Field	Description
Packet loss ratio	Average packet loss ratio.
Failures due to timeout	Number of timeout occurrences in an operation.
Failures due to disconnect	Number of disconnections by the peer.
Failures due to no connection	Number of failures to connect with the peer.
Failures due to internal error	Number of failures due to internal errors.
Failures due to other errors	Failures due to other errors.
Packets out of sequence	Number of failures due to out-of-sequence packets.
Packets arrived late	Number of response packets received after a probe times out.
UDP-jitter results	UDP jitter operation results. This field is available only for the UDP jitter operation.
Voice results	Voice operation results. This field is available only for the voice operation.
RTT number	Number of response packets received.
Min positive SD	Minimum positive jitter from source to destination.
Min positive DS	Minimum positive jitter from destination to source.
Max positive SD	Maximum positive jitter from source to destination.
Max positive DS	Maximum positive jitter from destination to source.
Positive SD number	Number of positive jitters from source to destination.
Positive DS number	Number of positive jitters from destination to source.
Positive SD sum	Sum of positive jitters from source to destination.
Positive DS sum	Sum of positive jitters from destination to source.
Positive SD average	Average positive jitters from source to destination.
Positive DS average	Average positive jitters from destination to source.
Positive SD square-sum	Square sum of positive jitters from source to destination.
Positive DS square-sum	Square sum of positive jitters from destination to source.
Min negative SD	Minimum absolute value among negative jitters from source to destination.
Min negative DS	Minimum absolute value among negative jitters from destination to source.
Max negative SD	Maximum absolute value among negative jitters from source to destination.
Max negative DS	Maximum absolute value among negative jitters from destination to source.
Negative SD number	Number of negative jitters from source to destination.
Negative DS number	Number of negative jitters from destination to source.
Negative SD sum	Sum of absolute values of negative jitters from source to destination.
Negative DS sum	Sum of absolute values of negative jitters from

Field	Description
	destination to source.
Negative SD average	Average absolute value of negative jitters from source to destination.
Negative DS average	Average absolute value of negative jitters from destination to source.
Negative SD square-sum	Square sum of negative jitters from source to destination.
Negative DS square-sum	Square sum of negative jitters from destination to source.
One way results	Unidirectional delay. This field is available only for the UDP jitter, and voice operations.
Max SD delay	Maximum delay from source to destination.
Max DS delay	Maximum delay from destination to source.
Min SD delay	Minimum delay from source to destination.
Min DS delay	Minimum delay from destination to source.
Number of SD delay	Number of delays from source to destination.
Number of DS delay	Number of delays from destination to source.
Sum of SD delay	Sum of delays from source to destination.
Sum of DS delay	Sum of delays from destination to source.
Square-Sum of SD delay	Square sum of delays from source to destination.
Square-Sum of DS delay	Square sum of delays from destination to source.
SD lost packets	Number of lost packets from the source to the destination.
DS lost packets	Number of lost packets from the destination to the source.
Lost packets for unknown reason	Number of lost packets for unknown reasons.
Voice scores	Voice parameters. This field is available only for the voice operation.
MOS value	MOS value calculated for the voice operation.
ICPIF value	ICPIF value calculated for the voice operation.
TTL	TTL value in the received reply packet.
Hop IP	IP address of the node that sent the reply packet.
Time	Time when the NQA client received the reply packet.

2.1.10. display nqa statistics

Use **display nqa statistics** to display NQA operation statistics.

Syntax

display nqa statistics [*admin-name operation-tag*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

admin-name operation-tag: Specifies an NQA operation by its administrator name and operation tag. The *admin-name* argument represents the name of the administrator who creates the NQA operation. The *operation-tag* argument represents the operation tag. Each of the arguments is a case-insensitive string of 1 to 32 characters that cannot contain hyphens (-). If you do not specify an NQA operation, the command displays statistics for all NQA operations.

Usage guidelines

The statistics are generated after the NQA operation completes. If you execute the **display nqa statistics** command before the operation completes, the statistics are displayed as all 0s.

If a reaction entry is configured, the command displays the monitoring results of the reaction entry in the period specified by the **statistics interval** command. The result fields display hyphens (-) in one of the following conditions:

- The threshold type is average value.
- The monitored performance metric is ICPIF or MOS for the voice operation.

Examples

Display the statistics for the TCP operation with administrator name **admin** and operation tag **test**.

```
<Switch> display nqa statistics admin test
NQA entry (admin admin, tag test) test statistics:
  NO. : 1
    Start time: 2007-01-01 09:30:20.0
    Life time: 2 seconds
    Send operation times: 1              Receive response times: 1
    Min/Max/Average round trip time: 13/13/13
    Square-Sum of round trip time: 169
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to disconnect: 0
    Failures due to no connection: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
```

Display the statistics for the UDP jitter operation with administrator name **admin** and operation tag **test**.

```
<Switch> display nqa statistics admin test
NQA entry (admin admin, tag test) test statistics:
  NO. : 1
    Start time: 2007-01-01 09:33:22.3
    Life time: 23 seconds
    Send operation times: 100            Receive response times: 100
    Min/Max/Average round trip time: 1/11/5
```

```
    Square-Sum of round trip time: 24360
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
    Packets out of sequence: 0
    Packets arrived late: 0
  UDP-jitter results:
   RTT number: 550
    Min positive SD: 1                    Min positive DS: 1
    Max positive SD: 7                    Max positive DS: 1
    Positive SD number: 220               Positive DS number: 97
    Positive SD sum: 283                  Positive DS sum: 287
    Positive SD average: 1                Positive DS average: 2
    Positive SD square-sum: 709           Positive DS square-sum: 1937
    Min negative SD: 2                    Min negative DS: 1
    Max negative SD: 10                   Max negative DS: 1
    Negative SD number: 81                Negative DS number: 94
    Negative SD sum: 556                  Negative DS sum: 191
    Negative SD average: 6                Negative DS average: 2
    Negative SD square-sum: 4292          Negative DS square-sum: 967
  One way results:
    Max SD delay: 5                       Max DS delay: 5
    Min SD delay: 1                       Min DS delay: 1
    Number of SD delay: 550               Number of DS delay: 550
    Sum of SD delay: 1475                 Sum of DS delay: 1201
    Square-Sum of SD delay: 5407          Square-Sum of DS delay: 3959
    SD lost packets: 0                    DS lost packets: 0
    Lost packets for unknown reason: 0
  Reaction statistics:
    Index  Checked Element  Threshold Type  Checked Num  Over-threshold Num
    1      jitter-DS        accumulate      90           25
    2      jitter-SD        average         -            -
    3      OWD-DS           -               100          24
    4      OWD-SD           -               100          13
    5      packet-loss      accumulate      0            0
    6      RTT              accumulate      100          52
```

Display the statistics for the voice operation with administrator name **admin** and operation tag **test**.

```
<Switch> display nqa statistics admin test
NQA entry (admin admin, tag test) test statistics:
  NO. : 1
    Start time: 2007-01-01 09:33:45.3
    Life time: 120 seconds
    Send operation times: 10              Receive response times: 10
    Min/Max/Average round trip time: 1/12/7
    Square-Sum of round trip time: 620
```

```
Extended results:
  Packet loss ratio: 0%
  Failures due to timeout: 0
  Failures due to internal error: 0
  Failures due to other errors: 0
  Packets out of sequence: 0
  Packets arrived late: 0
Voice results:
 RTT number: 10
  Min positive SD: 3                    Min positive DS: 1
  Max positive SD: 10                   Max positive DS: 1
  Positive SD number: 3                 Positive DS number: 2
  Positive SD sum: 18                   Positive DS sum: 2
  Positive SD average: 6                Positive DS average: 1
  Positive SD square-sum: 134           Positive DS square-sum: 2
  Min negative SD: 3                    Min negative DS: 1
  Max negative SD: 9                    Max negative DS: 1
  Negative SD number: 4                 Negative DS number: 2
  Negative SD sum: 25                   Negative DS sum: 2
  Negative SD average: 6                Negative DS average: 1
  Negative SD square-sum: 187           Negative DS square-sum: 2
One way results:
  Max SD delay: 0                       Max DS delay: 0
  Min SD delay: 0                       Min DS delay: 0
  Number of SD delay: 0                 Number of DS delay: 0
  Sum of SD delay: 0                    Sum of DS delay: 0
  Square-Sum of SD delay: 0             Square-Sum of DS delay: 0
  SD lost packets: 0                    DS lost packets: 0
  Lost packets for unknown reason: 0
Voice scores:
  Max MOS value: 4.40                   Min MOS value: 4.40
  Max ICPIF value: 0                    Min ICPIF value: 0
Reaction statistics:
  Index  Checked Element  Threshold Type  Checked Num  Over-threshold Num
  1      ICPIF            -               -            -
  2      MOS              -               -            -
```

Table 2-4 Command output

Field	Description
No.	Statistics group ID.
Start time	Time when the operation started.
Life time	Duration of the operation in seconds.
Send operation times	Number of probe packets sent.
Receive response times	Number of response packets received.
Min/Max/Average round trip time	Minimum/maximum/average round-trip time in milliseconds.

Field	Description
Square-Sum of round trip time	Square sum of round-trip time.
Packet loss ratio	Average packet loss ratio.
Failures due to timeout	Number of timeout occurrences in an operation.
Failures due to disconnect	Number of disconnections by the peer.
Failures due to no connection	Number of failures to connect with the peer.
Failures due to internal error	Number of failures due to internal errors.
Failures due to other errors	Failures due to other errors.
Packets out of sequence	Number of failures due to out-of-sequence packets.
Packets arrived late	Number of response packets received after a probe times out.
UDP-jitter results	UDP jitter operation results. This field is available only for the UDP jitter operation.
Voice results	Voice operation results. This field is available only for the voice operation.
RTT number	Number of response packets received.
Min positive SD	Minimum positive jitter from source to destination.
Min positive DS	Minimum positive jitter from destination to source.
Max positive SD	Maximum positive jitter from source to destination.
Max positive DS	Maximum positive jitter from destination to source.
Positive SD number	Number of positive jitters from source to destination.
Positive DS number	Number of positive jitters from destination to source.
Positive SD sum	Sum of positive jitters from source to destination.
Positive DS sum	Sum of positive jitters from destination to source.
Positive SD average	Average positive jitters from source to destination.
Positive DS average	Average positive jitters from destination to source.
Positive SD square-sum	Square sum of positive jitters from source to destination.
Positive DS square-sum	Square sum of positive jitters from destination to source.
Min negative SD	Minimum absolute value among negative jitters from source to destination.
Min negative DS	Minimum absolute value among negative jitters from destination to source.
Max negative SD	Maximum absolute value among negative jitters from source to destination.
Max negative DS	Maximum absolute value among negative jitters from destination to source.
Negative SD number	Number of negative jitters from source to destination.
Negative DS number	Number of negative jitters from destination to source.

Field	Description
Negative SD sum	Sum of absolute values of negative jitters from source to destination.
Negative DS sum	Sum of absolute values of negative jitters from destination to source.
Negative SD average	Average absolute value of negative jitters from source to destination.
Negative DS average	Average absolute value of negative jitters from destination to source.
Negative SD square-sum	Square sum of negative jitters from source to destination.
Negative DS square-sum	Square sum of negative jitters from destination to source.
One way results	Unidirectional delay result. This field is available only for the UDP jitter, and voice operations.
Max SD delay	Maximum delay from source to destination.
Max DS delay	Maximum delay from destination to source.
Min SD delay	Minimum delay from source to destination.
Min DS delay	Minimum delay from destination to source.
Number of SD delay	Number of delays from source to destination.
Number of DS delay	Number of delays from destination to source.
Sum of SD delay	Sum of delays from source to destination.
Sum of DS delay	Sum of delays from destination to source.
Square-Sum of SD delay	Square sum of delays from source to destination.
Square-Sum of DS delay	Square sum of delays from destination to source.
SD lost packets	Number of lost packets from the source to the destination.
DS lost packets	Number of lost packets from the destination to the source.
Lost packets for unknown reason	Number of lost packets for unknown reasons.
Voice scores	Voice parameters. This field is available only for the voice operation.
Max MOS value	Maximum MOS value.
Min MOS value	Minimum MOS value.
Max ICPIF value	Maximum ICPIF value.
Min ICPIF value	Minimum ICPIF value.
Reaction statistics	Statistics about the reaction entry in the counting interval.
Index	ID of a reaction entry.
Checked Element	Monitored element.
Threshold Type	Threshold type.

Field	Description
Checked Num	Number of targets that have been monitored for data collection.
Over-threshold Num	Number of threshold violations.

Table 2-5 Monitored performance metrics for DHCP/DLSw/DNS/FTP/HTTP/ICMP echo/SNMP/TCP/UDP echo operations

Monitored performance metric	Threshold type	Collect data in	Checked Num	Over-threshold Num
probe-duration	accumulate	Probes in the counting interval.	Number of completed probes.	Number of probes of which the duration exceeds the threshold.
	average	N/A	N/A	N/A
	consecutive	Probes in the counting interval.	Number of completed probes.	Number of probes of which the duration exceeds the threshold.
probe-fail	accumulate	Probes in the counting interval.	Number of completed probes.	Number of probe failures.
	consecutive	Probes in the counting interval.	Number of completed probes.	Number of probe failures.

Table 2-6 Monitored performance metrics for UDP jitter/voice operations

Monitored performance metric	Threshold type	Collect data in	Checked Num	Over-threshold Num
RTT	accumulate	Packets sent in the counting interval.	Number of sent packets.	Number of packets of which the round-trip time exceeds the threshold.
	average	N/A	N/A	N/A
jitter-DS/jitter-SD	accumulate	Packets sent in the counting interval.	Number of sent packets.	Number of packets of which the one-way jitter exceeds the threshold.
	average	N/A	N/A	N/A
OWD-DS/OWD-SD	N/A	Packets sent in the counting interval.	Number of sent packets.	Number of packets of which the one-way delay exceeds the threshold.
packet-loss	accumulate	Packets sent in the counting interval.	Number of sent packets.	Number of packet loss.
ICPIF/MOS	N/A	N/A	N/A	N/A

Monitored performance metric	Threshold type	Collect data in	Checked Num	Over-threshold Num
(available only for the voice operation)				

Related commands

statistics interval

2.1.11. filename

Use **filename** to specify a file to be transferred between the FTP server and the FTP client.

Use **undo filename** to restore the default.

Syntax

filename *filename*

undo filename

Default

No file is specified.

Views

FTP operation view

Predefined user roles

network-admin

Parameters

filename: Specifies the name of a file, a case-sensitive string of 1 to 200 characters that cannot contain slashes (/).

Examples

Specify **config.txt** as the file to be transferred between the FTP server and the FTP client for the FTP operation.

```
<Switch> system-view
[Switch] nqa entry admin test
[Switch-nqa-admin-test] type ftp
[Switch-nqa-admin-test-ftp] filename config.txt
```

2.1.12. frequency

Use **frequency** to specify the interval at which the NQA operation repeats.

Use **undo frequency** to restore the default.

Syntax

frequency *interval*

undo frequency

Default

The interval between two consecutive voice operations is 60000 milliseconds. The interval between two consecutive operations of other types is 0 milliseconds.

Views

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

UDP jitter/voice operation view

Predefined user roles

network-admin

Parameters

interval: Specifies the interval between two consecutive operations, in the range of 0 to 604800000 milliseconds. An interval of 0 milliseconds configures NQA to perform the operation only once, and not to generate any statistics.

Usage guidelines

If an operation is not completed when the interval is reached, the next operation does not start.

Examples

Configure the ICMP echo operation to repeat every 1000 milliseconds.

```
<Switch> system-view
[Switch] nqa entry admin test
[Switch-nqa-admin-test] type icmp-echo
[Switch-nqa-admin-test-icmp-echo] frequency 1000
```

2.1.13. history-record enable

Use **history-record enable** to enable the saving of history records for the NQA operation.

Use **undo history-record enable** to disable the saving of history records.

Syntax

history-record enable

undo history-record enable

Default

The saving of history records is disabled.

Views

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

Predefined user roles

network-admin

Usage guidelines

To display the history records of the NQA operation, use the **display nqa history** command.

The **undo** form of the command also removes existing history records of an NQA operation.

Examples

Enable the saving of history records for the NQA operation.

```
<Switch> system-view
[Switch] nqa entry admin test
[Switch-nqa-admin-test] type icmp-echo
[Switch-nqa-admin-test-icmp-echo] history-record enable
```

Related commands

display nqa history

2.1.14. history-record keep-time

Use **history-record keep-time** to set the lifetime of history records for an NQA operation.

Use **undo history-record keep-time** to restore the default.

Syntax

history-record keep-time *keep-time*

undo history-record keep-time

Default

The history records of an NQA operation are kept for 120 minutes.

Views

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

Predefined user roles

network-admin

Parameters

keep-time: Specifies how long the history records can be saved. The value range is 1 to 1440 minutes.

Usage guidelines

When an NQA operation completes, the timer starts. All records are removed when the lifetime is reached.

Examples

Set the lifetime of the history records to 100 minutes for the ICMP echo operation.

```
<Switch> system-view
[Switch] nqa entry admin test
[Switch-nqa-admin-test] type icmp-echo
[Switch-nqa-admin-test-icmp-echo] history-record keep-time 100
```

2.1.15. history-record number

Use **history-record number** to set the maximum number of history records that can be saved for an NQA operation.

Use **undo history-record number** to restore the default.

Syntax

history-record number *number*

undo history-record number

Default

A maximum of 50 history records can be saved for an NQA operation.

Views

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

Predefined user roles

network-admin

Parameters

number: Specifies the maximum number of history records that can be saved for an NQA operation. The value range is 0 to 50.

Usage guidelines

If the number of history records for an NQA operation exceeds the maximum number, earliest history records are removed.

Examples

Set the maximum number of history records to 10 for the ICMP echo operation.

```
<Switch> system-view
[Switch] nqa entry admin test
[Switch-nqa-admin-test] type icmp-echo
[Switch-nqa-admin-test-icmp-echo] history-record number 10
```

2.1.16. next-hop ip

Use **next-hop ip** to specify the next hop IPv4 address for probe packets.

Use **undo next-hop ip** to restore the default.

Syntax

next-hop ip *ip-address*

undo next-hop ip

Default

No next hop IPv4 address is specified for probe packets.

Views

ICMP echo operation view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the IPv4 address of the next hop.

Usage guidelines

If the next hop IPv4 address is not configured, the device searches the routing table to determine the next hop IPv4 address for the probe packets.

Examples

Specify 10.1.1.1 as the next hop IPv4 address for the ICMP echo operation.

```
<Switch> system-view
[Switch] nqa entry admin test
[Switch-nqa-admin-test] type icmp-echo
[Switch-nqa-admin-test-icmp-echo] next-hop ip 10.1.1.1
```

2.1.17. nqa

Use **nqa** to create an NQA operation and enter its view, or enter the view of an existing NQA operation.

Use **undo nqa** to remove the operation.

Syntax

nqa entry *admin-name operation-tag*

undo nqa { **all** | **entry** *admin-name operation-tag* }

Default

No NQA operations exist.

Views

System view

Predefined user roles

network-admin

Parameters

admin-name operation-tag: Specifies an NQA operation by its administrator name and operation tag. The *admin-name* argument represents the name of the administrator who creates the NQA operation. The *operation-tag* argument represents the operation tag. Each of the arguments is a case-insensitive string of 1 to 32 characters that cannot contain hyphens (-).

all: Removes all NQA operations.

Examples

Create an NQA operation with administrator name **admin** and operation tag **test**, and enter NQA operation view.

```
<Switch> system-view
[Switch] nqa entry admin test
[Switch-nqa-admin-test]
```

2.1.18. nqa agent enable

Use **nqa agent enable** to enable the NQA client.

Use **undo nqa agent enable** to disable the NQA client and stop all operations being performed.

Syntax

nqa agent enable

undo nqa agent enable

Default

The NQA client is enabled.

Views

System view

Predefined user roles

network-admin

Examples

Enable the NQA client.

```
<Switch> system-view
[Switch] nqa agent enable
```

Related commands

nqa server enable

2.1.19. nqa schedule

Use **nqa schedule** to configure scheduling parameters for an NQA operation.

Use **undo nqa schedule** to stop the operation.

Syntax

nqa schedule *admin-name operation-tag* **start-time** { *hh*:*mm*:*ss* [*yyyy/mm/dd* | *mm/dd/yyyy*] | **now** } **lifetime** { *lifetime* | **forever** } [**recurring**]

undo nqa schedule *admin-name operation-tag*

Default

No schedule is configured for an NQA operation.

Views

System view

Predefined user roles

network-admin

Parameters

admin-name operation-tag: Specifies an NQA operation by its administrator name and operation tag. The *admin-name* argument represents the name of the administrator who creates the NQA operation. The *operation-tag* argument represents the operation tag. Each of the arguments is a case-insensitive string of 1 to 32 characters that cannot contain hyphens (-).

start-time: Specifies the start time and date of the NQA operation.

hh:*mm*:*ss*: Specifies the start time of an NQA operation.

yyyy/mm/dd: Specifies the start date of an NQA operation. The default value is the current system time, and the value for the *yyyy* argument is in the range of 2000 to 2035.

mm/dd/yyyy: Specifies the start date of an NQA operation. The default value is the current system time, and the value for the *yyyy* argument is in the range of 2000 to 2035.

now: Starts the operation immediately.

lifetime: Specifies the duration of an operation.

lifetime: Specifies the duration of an operation in seconds. The value range is 1 to 2147483647.

forever: Performs the operation until you stop it by using the **undo nqa schedule** command.

recurring: Runs the operation automatically at the start time and for the specified duration. If you do not specify this keyword, the NQA operation is performed only once at the specified date and time.

Usage guidelines

The NQA operation works between the specified start time and the end time (the start time plus operation duration). If the specified start time is ahead of the system time, the operation starts immediately. If both the specified start time and end time are ahead of the system time, the operation does not start. To display the current system time, use the **display clock** command.

You cannot enter the view of a scheduled NQA operation. If you want to enter such view, use the **undo nqa schedule** command to stop the NQA operation first.

Specify a lifetime long enough for an operation to complete.

Examples

Schedule the operation with administrator name **admin** and operation tag **test** to start on 08:08:08 2008/08/08 and last 1000 seconds.

```
<Switch> system-view
[Switch] nqa schedule admin test start-time 08:08:08 2008/08/08 lifetime 1000 recurring
```

Related commands

destination ip

display clock (*Fundamentals Command Reference*)

nqa entry

type

2.1.20. operation (FTP operation view)

Use **operation** to specify the operation type for the FTP operation.

Use **undo operation** to restore the default.

Syntax

operation { **get** | **put** }

undo operation

Default

The FTP operation type is **get**.

Views

FTP operation view

Predefined user roles

network-admin

Parameters

get: Gets a file from the FTP server.

put: Transfers a file to the FTP server.

Usage guidelines

When you perform the **put** operation with the **filename** command configured, make sure the file exists on the NQA client.

If you get a file from the FTP server, make sure the file specified in the URL exists on the FTP server. The NQA client does not save the file obtained from the FTP server.

Use a small file for the FTP operation. A big file might result in transfer failure because of timeout, or might affect other services for occupying much network bandwidth.

Examples

Set the operation type to **put** for the FTP operation.

```
<Switch> system-view
[Switch] nqa entry admin test
[Switch-nqa-admin-test] type ftp
[Switch-nqa-admin-test-ftp] operation put
```

Related commands

password

username

2.1.21. operation (HTTP operation view)

Use **operation** to specify the operation type for the HTTP operation.

Use **undo operation** to restore the default.

Syntax

operation { **get** | **post** }

undo operation

Default

The HTTP operation type is **get**.

Views

HTTP operation view

Predefined user roles

network-admin

Parameters

get: Gets data from the HTTP server.

post: Transfers data to the HTTP server.

Usage guidelines

The HTTP operations use HTTP requests as probe packets.

For the **get** or **post** operation, the content in the request is obtained from the URL specified by the **url** command.

Examples

Set the operation type to **get** for the HTTP operation.

```
<Switch> system-view
```

```
[Switch] nqa entry admin test
[Switch-nqa-admin-test] type http
[Switch-nqa-admin-test-http] operation get
```

Related commands

password

username

2.1.22. password

Use **password** to specify a password.

Use **undo password** to restore the default.

Syntax

password { **cipher** | **simple** } *string*

undo password

Default

No password is specified.

Views

FTP/HTTP operation view

Predefined user roles

network-admin

Parameters

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password. For FTP, HTTP, and HTTPS operations, the plaintext form of the password is a case-sensitive string of 1 to 32 characters. The encrypted form of the password is a case-sensitive string of 1 to 73 characters.

Examples

Set the FTP login password to **ftpuser**.

```
<Switch> system-view
[Switch] nqa entry admin test
[Switch-nqa-admin-test] type ftp
[Switch-nqa-admin-test-ftp] password simple ftpuser
```

Related commands

operation

username

2.1.23. probe count

Use **probe count** to specify the probe times.

Use **undo probe count** to restore the default.

Syntax

probe count *times*

undo probe count

Default

The NQA client performs one probe to the destination per operation.

Views

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

UDP jitter operation view

Predefined user roles

network-admin

Parameters

times: Specifies the probe times. This argument specifies the times of probes to the destination per operation. The value range for this argument is 1 to 15.

Usage guidelines

The following describes how NQA performs different types of operations:

- A TCP or DLSw operation sets up a connection.
- A UDP jitter operation sends a number of probe packets. The number of probe packets is set by using the **probe packet-number** command.
- An FTP operation uploads or downloads a file.
- An HTTP operation gets a Web page.
- A DHCP operation gets an IP address through DHCP.
- A DNS operation translates a domain name to an IP address.
- An ICMP echo sends an ICMP echo request.
- A UDP echo operation sends a UDP packet.
- An SNMP operation sends one SNMPv1 packet, one SNMPv2c packet, and one SNMPv3 packet.
- A frame loss, latency, or throughput operation sends probe frames to the destination device to test the frame loss ratio, latency, or throughput of the network.

If an operation is to perform multiple probes, the NQA client starts a new probe in one of the following conditions:

- The NQA client receives responses to packets sent in the last probe.
- The probe timeout time expires.

This command is not available for the voice operations. Each of these operations performs only one probe.

Examples

Configure the ICMP echo operation to perform 10 probes.

```
<Switch> system-view
[Switch] nqa entry admin test
[Switch-nqa-admin-test] type icmp-echo
[Switch-nqa-admin-test-icmp-echo] probe count 10
```

2.1.24. probe packet-interval

Use **probe packet-interval** to configure the packet sending interval in the probe.

Use **undo probe packet-interval** to restore the default.

Syntax

probe packet-interval *interval*

undo probe packet-interval

Default

The packet sending interval is 20 milliseconds.

Views

UDP jitter/voice operation view

Predefined user roles

network-admin

Parameters

interval: Specifies the sending interval in the range of 10 to 60000 milliseconds.

Examples

Configure the UDP jitter operation to send packets every 100 milliseconds.

```
<Switch> system-view
[Switch] nqa entry admin test
[Switch-nqa-admin-test] type udp-jitter
[Switch-nqa-admin-test-udp-jitter] probe packet-interval 100
```

2.1.25. probe packet-number

Use **probe packet-number** to set the number of packets to be sent in a UDP jitter, or voice probe.

Use **undo probe packet-number** to restore the default.

Syntax

probe packet-number *packet-number*

undo probe packet-number

Default

A UDP jitter probe sends 10 packets and a voice probe sends 1000 packets.

Views

UDP jitter/voice operation view

Predefined user roles

network-admin

Parameters

packet-number: Specifies the number of packets to be sent per probe. Available value ranges include:

- 10 to 1000 for the UDP jitter operations.

- 10 to 60000 for the voice operation.

Examples

Configure the UDP jitter probe to send 100 packets.

```
<Switch> system-view
[Switch] nqa entry admin test
[Switch-nqa-admin-test] type udp-jitter
[Switch-nqa-admin-test-udp-jitter] probe packet-number 100
```

2.1.26. probe packet-timeout

Use **probe packet-timeout** to set the timeout time for waiting for a response in the UDP jitter, or voice operation.

Use **undo probe packet-timeout** to restore the default.

Syntax

probe packet-timeout *timeout*

undo probe packet-timeout

Default

The response timeout time in the UDP jitter operation is 3000 milliseconds.

The response timeout time in the voice operation is 5000 milliseconds.

Views

UDP jitter/voice operation view

Predefined user roles

network-admin

Parameters

timeout: Specifies the timeout time in milliseconds. The value range is 10 to 3600000.

Examples

Set the response timeout time to 100 milliseconds in the UDP jitter operation.

```
<Switch> system-view
[Switch] nqa entry admin test
[Switch-nqa-admin-test] type udp-jitter
[Switch-nqa-admin-test-udp-jitter] probe packet-timeout 100
```

2.1.27. probe timeout

Use **probe timeout** to set the probe timeout time.

Use **undo probe timeout** to restore the default.

Syntax

probe timeout *timeout*

undo probe timeout

Default

The timeout time of a probe is 3000 milliseconds.

Views

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

Predefined user roles

network-admin

Parameters

timeout: Specifies the probe timeout time in milliseconds. The value range for this argument varies as follows:

- For FTP and HTTP operations, the value range is 10 to 86400000.
- For DHCP, DNS, DLSw, ICMP echo, SNMP, TCP, and UDP echo operations, the value range is 10 to 3600000.

Usage guidelines

If a probe does not complete within the period, the probe is timed out.

Examples

Set the probe timeout time to 10000 milliseconds for the DHCP operation.

```
<Switch> system-view
[Switch] nqa entry admin test
[Switch-nqa-admin-test] type dhcp
[Switch-nqa-admin-test-dhcp] probe timeout 10000
```

2.1.28. reaction checked-element probe-fail (for trap)

Use **reaction checked-element probe-fail** to configure a reaction entry for monitoring the probe failures of the operation.

Use **undo reaction** to delete a reaction entry.

Syntax

reaction *item-number* **checked-element probe-fail threshold-type** { **accumulate** *accumulate-occurrences* | **consecutive** *consecutive-occurrences* } [**action-type** { **none** | **trap-only** }]

undo reaction *item-number*

Default

No reaction entries for monitoring probe failures exist.

Views

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

Predefined user roles

network-admin

Parameters

item-number: Assigns an ID to the reaction entry, in the range of 1 to 10.

threshold-type: Specifies a threshold type.

accumulate *accumulate-occurrences*: Checks the total number of probe failures. The value range is 1 to 15.

consecutive *consecutive-occurrences*: Checks the maximum number of consecutive probe failures. The value range is 1 to 16.

action-type: Specifies what action to be triggered. The default action is **none**.

none: Specifies the action of displaying results on the terminal display.

trap-only: Specifies the action of displaying results on the terminal display and meanwhile sending SNMP trap messages to the NMS. This keyword is not available for the DNS operation.

Usage guidelines

You cannot edit a reaction entry after it is created. To change the attributes in a reaction entry, use the **undo reaction** command to delete the entry, and then configure a new one.

Examples

Create reaction entry 1 for monitoring the probe failures in ICMP echo operation. Before the NQA operation starts, the initial state of the reaction entry is invalid. If the total number of probe failures reaches or exceeds 10, the state of the entry is set to over-threshold. If it is below the threshold, the state of the entry is set to below-threshold. Once the state of the reaction entry changes, a trap message is generated and sent to the NMS.

```
<Switch> system-view
[Switch] nqa entry admin test
[Switch-nqa-admin-test] type icmp-echo
[Switch-nqa-admin-test-icmp-echo] reaction 1 checked-element probe-fail threshold-type
accumulate 10 action-type trap-only
```

Create reaction entry 2 for monitoring the probe failures in ICMP echo operation. Before the NQA operation starts, the initial state of the reaction entry is invalid. If the number of consecutive probe failures reaches or exceeds 10, the state of the entry is set to over-threshold. If it is below the threshold, the state of the entry is set to below-threshold. Once the state of the reaction entry changes, a trap message is generated and sent to the NMS.

```
<Switch> system-view
[Switch] nqa entry admin test
[Switch-nqa-admin-test] type icmp-echo
[Switch-nqa-admin-test-icmp-echo] reaction 2 checked-element probe-fail threshold-type
consecutive 10 action-type trap-only
```

2.1.29. reaction checked-element probe-fail (for trigger)

Use **reaction checked-element probe-fail** to configure a reaction entry for monitoring probe failures.

Use **undo reaction** to delete a reaction entry.

Syntax

reaction *item-number* **checked-element probe-fail threshold-type consecutive** *consecutive-occurrences* **action-type trigger-only**

undo reaction *item-number*

Default

No reaction entries for monitoring probe failures exist.

Views

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

Predefined user roles

network-admin

Parameters

item-number: Assigns an ID to the reaction entry, in the range of 1 to 10.

threshold-type: Specifies a threshold type.

consecutive *consecutive-occurrences*: Checks the maximum number of consecutive probe failures, in the range of 1 to 16.

action-type: Specifies what action to be triggered.

trigger-only: Triggers other modules to react to certain conditions.

Usage guidelines

You cannot edit a reaction entry after it is created. To change the attributes in a reaction entry, use the **undo reaction** command to delete the entry, and then configure a new one.

Examples

Create reaction entry 1. If the number of consecutive probe failures reaches 3, collaboration is triggered.

```
<Switch> system-view
[Switch] nqa entry admin test
[Switch-nqa-admin-test] type tcp
[Switch-nqa-admin-test-tcp] reaction 1 checked-element probe-fail threshold-type
consecutive 3 action-type trigger-only
```

Related commands

track (*High Availability Command Reference*)

2.1.30. reaction trap

Use **reaction trap** to configure the sending of traps to the NMS under specific conditions.

Use **undo reaction trap** to restore the default.

Syntax

reaction trap { **probe-failure** *consecutive-probe-failures* | **test-complete** | **test-failure** [*accumulate-probe-failures*] }

undo reaction trap { **probe-failure** | **test-complete** | **test-failure** }

Default

No traps are sent to the NMS.

Views

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

UDP jitter/voice operation view

Predefined user roles

network-admin

Parameters

probe-failure *consecutive-probe-failures*: Sends a trap to the NMS if the number of consecutive probe failures in an operation is greater than or equal to *consecutive-probe-failures.* The value range for the *consecutive-probe-failures* argument is 1 to 15. The system counts the number of consecutive probe failures for each operation, so multiple traps might be sent.

test-complete: Sends a trap to indicate that the operation is completed.

test-failure: Sends a trap when an operation fails. the system counts the total number of probe failures in an operation. If the number reaches or exceeds the value for the *accumulate-probe-failures* argument, a trap is sent for the operation failure.

accumulate-probe-failures: Specifies the total number of probe failures in an operation. The value range is 1 to 15.

Usage guidelines

The UDP jitter, and voice operations support only the **test-complete** keyword.

Examples

Configure the system to send a trap if five or more consecutive probe failures occur in an ICMP echo operation.

```
<Switch> system-view
[Switch] nqa entry admin test
[Switch-nqa-admin-test] type icmp-echo
[Switch-nqa-admin-test-icmp-echo] reaction trap probe-failure 5
```

2.1.31. resolve-target

Use **resolve-target** to specify the domain name to be resolved in the DNS operation.

Use **undo resolve-target** to restore the default.

Syntax

resolve-target *domain-name*

undo resolve-target

Default

The domain name to be resolved in the DNS operation is not specified.

Views

DNS operation view

Predefined user roles

network-admin

Parameters

domain-name: Specifies the domain name to be resolved. It is a dot-separated case-sensitive string of 1 to 255 characters including letters, digits, hyphens (-), and underscores (_) (for example, aabbcc.com). Each part consists of 1 to 63 characters, and consecutive dots (.) are not allowed.

Examples

Specify **domain1** as the domain name to be resolved.

```
<Switch> system-view
[Switch] nqa entry admin test
[Switch-nqa-admin-test] type dns
[Switch-nqa-admin-test-dns] resolve-target domain1
```

2.1.32. route-option bypass-route

Use **route-option bypass-route** to enable the routing table bypass feature to test the connectivity to the direct destination.

Use **undo route-option bypass-route** to disable the routing table bypass feature.

Syntax

route-option bypass-route

undo route-option bypass-route

Default

The routing table bypass feature is disabled.

Views

ICMP echo/TCP/UDP echo operation view

DLSw/DNS/FTP/HTTP/SNMP operation view

UDP jitter/voice operation view

Predefined user roles

network-admin

Usage guidelines

When the routing table bypass feature is enabled, the following events occur:

- The routing table is not searched. Packets are sent to the destination on a directly connected network.
- The TTL value in the probe packet is set to 1. The TTL set in the **ttl** command does not take effect.

Examples

Enable the routing table bypass feature.

```
<Switch> system-view
[Switch] nqa entry admin test
[Switch-nqa-admin-test] type icmp-echo
[Switch-nqa-admin-test-icmp-echo] route-option bypass-route
```

2.1.33. source interface (ICMP echo operation view)

Use **source interface** to specify the IP address of an interface as the source IP address of probe packets.

Use **undo source interface** to restore the default.

Syntax

source interface *interface-type interface-number*

undo source interface

Default

The probe packets take the primary IP address of the outgoing interface as their source IP address.

Views

ICMP echo operation view

Predefined user roles

network-admin

Parameters

interface-type interface-number: Specifies an interface by its type and number.

Usage guidelines

The specified interface must be up. If the interface is down, no probe requests can be sent out.

If you execute this command and the **source ip** command for an ICMP echo operation multiple times, the most recent configuration takes effect.

Examples

Specify the IP address of the interface VLAN-interface 1 as the source IP address of ICMP echo request packets.

```
<Switch> system-view
[Switch] nqa entry admin test
[Switch-nqa-admin-test] type icmp-echo
[Switch-nqa-admin-test-icmp-echo] source interface vlan-interface 1
```

Related commands

source ip

2.1.34. source ip

Use **source ip** to configure the source IPv4 address for probe packets.

Use **undo source ip** to restore the default.

Syntax

source ip *ip-address*

undo source ip

Default

The probe packets takes the primary IP address of their output interface as the source IP address.

Views

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/FTP/HTTP/SNMP operation view

UDP jitter/voice operation view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the source IPv4 address for probe packets.

Usage guidelines

The specified source IPv4 address must be the IPv4 address of a local interface, and the local interface must be up. Otherwise, no probe packets can be sent out.

If you execute the **source interface** and **source ip** commands multiple times for an ICMP echo operation, the most recent configuration takes effect.

Examples

Specify 10.1.1.1 as the source IPv4 address for ICMP echo requests.

```
<Switch> system-view
[Switch] nqa entry admin test
[Switch-nqa-admin-test] type icmp-echo
[Switch-nqa-admin-test-icmp-echo] source ip 10.1.1.1
```

Related commands

source interface

2.1.35. source port

Use **source port** to configure the source port number for probe packets.

Use **undo source port** to restore the default.

Syntax

source port *port-number*

undo source port

Default

The source port number is not specified.

Views

UDP echo operation view

SNMP operation view

UDP jitter/voice operation view

Predefined user roles

network-admin

Parameters

port-number: Specifies the source port number in the range of 1 to 65535.

Examples

Set the source port number to 8000 for probe packets in the UDP echo operation.

```
<Switch> system-view
[Switch] nqa entry admin test
[Switch-nqa-admin-test] type udp-echo
[Switch-nqa-admin-test-udp-echo] source port 8000
```

2.1.36. statistics hold-time

Use **statistics hold-time** to set the hold time of statistics groups for an NQA operation.

Use **undo statistics hold-time** to restore the default.

Syntax

statistics hold-time *hold-time*

undo statistics hold-time

Default

The hold time of statistics groups for an NQA operation is 120 minutes.

Views

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

UDP jitter/voice operation view

Predefined user roles

network-admin

Parameters

hold-time: Specifies the hold time in minutes, in the range of 1 to 1440.

Usage guidelines

A statistics group is deleted when its hold time expires.

Examples

Set the hold time to 3 minutes for statistics groups of the ICMP echo operation.

```
<Switch> system-view
[Switch] nqa entry admin test
[Switch-nqa-admin-test] type icmp-echo
[Switch-nqa-admin-test-icmp-echo] statistics hold-time 3
```

2.1.37. statistics interval

Use **statistics interval** to set the statistics collection interval for an NQA operation.

Use **undo statistics interval** to restore the default.

Syntax

statistics interval *interval*

undo statistics interval

Default

The statistics collection interval is 60 minutes.

Views

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

UDP jitter/voice operation view

Predefined user roles

network-admin

Parameters

interval: Specifies the interval in minutes, in the range of 1 to 35791394.

Usage guidelines

NQA forms statistics within the same collection interval as a statistics group. To display information about the statistics groups, use the **display nqa statistics** command.

Examples

Configure NQA to collect the ICMP echo operation statistics every 2 minutes.

```
<Switch> system-view
[Switch] nqa entry admin test
[Switch-nqa-admin-test] type icmp-echo
[Switch-nqa-admin-test-icmp-echo] statistics interval 2
```

2.1.38. statistics max-group

Use **statistics max-group** to set the maximum number of statistics groups that can be saved.

Use **undo statistics max-group** to restore the default.

Syntax

statistics max-group *number*

undo statistics max-group

Default

A maximum of two statistics groups can be saved.

Views

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

UDP jitter/voice operation view

Predefined user roles

network-admin

Parameters

number: Specifies the maximum number of statistics groups, in the range of 0 to 100. To disable statistics collection, set the value to 0.

Usage guidelines

When the maximum number of statistics groups is reached and a new statistics group is to be saved, the earliest statistics group is deleted.

Examples

Configure NQA to save a maximum of five statistics groups for the ICMP echo operation.

```
<Switch> system-view
[Switch] nqa entry admin test
[Switch-nqa-admin-test] type icmp-echo
[Switch-nqa-admin-test-icmp-echo] statistics max-group 5
```

2.1.39. tos

Use **tos** to set the ToS value in the IP header for probe packets.

Use **undo tos** to restore the default.

Syntax

tos *value*

undo tos

Default

The ToS value in the IP header of probe packets is 0.

Views

Any operation view

Predefined user roles

network-admin

Parameters

value: Specifies the ToS value in the range of 0 to 255.

Examples

In ICMP echo operation view, set the ToS value to 1 in the IP header for probe packets.

```
<Switch> system-view
[Switch] nqa entry admin test
[Switch-nqa-admin-test] type icmp-echo
[Switch-nqa-admin-test-icmp-echo] tos 1
```

2.1.40. ttl

Use **ttl** to set the maximum number of hops that the probe packets can traverse.

Use **undo ttl** to restore the default.

Syntax

ttl *value*

undo ttl

Default

The maximum number of hops is 20 for probe packets.

Views

ICMP echo/TCP/UDP echo operation view

DLSw/DNS/FTP/HTTP/SNMP operation view

UDP jitter/voice operation view

Predefined user roles

network-admin

Parameters

value: Specifies the maximum number of hops that the probe packets can traverse, in the range of 1 to 255.

Usage guidelines

The **route-option bypass-route** command sets the TTL to 1 for probe packets. If you configure both the **route-option bypass-route** and **ttl** commands for an operation, the **ttl** command does not take effect.

Examples

Set the maximum number of hops to 16 for probe packets in the ICMP echo operation.

```
<Switch> system-view
[Switch] nqa entry admin test
[Switch-nqa-admin-test] type icmp-echo
[Switch-nqa-admin-test-icmp-echo] ttl 16
```

2.1.41. type

Use **type** to specify an NQA operation type and enter its view.

Syntax

type { **dhcp** | **dlsw** | **dns** | **ftp** | **http** | **icmp-echo** | **snmp** | **tcp** | **udp-echo** | **udp-jitter** | **voice** }

Default

No operation type is specified.

Views

NQA operation view

Predefined user roles

network-admin

Parameters

dhcp: Specifies the DHCP operation type.

dlsw: Specifies the DLSw operation type.

dns: Specifies the DNS operation type.

ftp: Specifies the FTP operation type.

http: Specifies the HTTP operation type.

icmp-echo: Specifies the ICMP echo operation type.

snmp: Specifies the SNMP operation type.

tcp: Specifies the TCP operation type.

udp-echo: Specifies the UDP echo operation type.

udp-jitter: Specifies the UDP jitter operation type.

voice: Specifies the voice operation type.

Examples

Specify FTP as the NQA operation type and enter FTP operation view.

```
<Switch> system-view
[Switch] nqa entry admin test
[Switch-nqa-admin-test] type ftp
[Switch-nqa-admin-test-ftp]
```

2.1.42. url

Use **url** to specify the URL of the destination.

Use **undo url** to restore the default.

Syntax

url *url*

undo url

Default

The destination URL is not specified.

Views

FTP/HTTP operation view

Predefined user roles

network-admin

Parameters

url: Specifies the URL of the destination server, a case-sensitive string of 1 to 255 characters. The following table describes the URL format and parameters for different operations.

Operation	URL format	Parameter description
HTTP operation	http://*host*/*resource* http://*host*:*port*/*resource*	The *host* parameter represents the host name of the destination server. The host name is a dot-separated case-sensitive string including letters, digits, hyphens (-), and underscores (_). Host names are composed of series of labels, aabbcc.com for example. Each label consists of 1 to 63 characters. Consecutive dots (.) and question marks are not allowed. For description about the filename parameter, see *Fundamentals Configuration Guide*.
FTP operation	ftp://*host/filename* ftp://*host*:*port*/*filename*	

Examples

Configure the URL that the HTTP operation visits as **http://www.company.com/index.htm**.

```
<Switch> system-view
[Switch] nqa entry admin test
[Switch-nqa-admin-test] type http
[Switch-nqa-admin-test-http] url http://www.company.com/index.html
```

2.1.43. username

Use **username** to specify a username.

Use **undo username** to restore the default.

Syntax

username *username*

undo username

Default

No username is configured.

Views

FTP/HTTP operation view

Predefined user roles

network-admin

Parameters

username: Specifies the username. This argument is case sensitive. It is a string of 1 to 32 characters for an FTP, HTTP, or HTTPS username, and a string of 1 to 253 characters for a RADIUS authentication username.

Examples

Set the FTP login username to **administrator**.

```
<Switch> system-view
[Switch] nqa entry admin test
[Switch-nqa-admin-test] type ftp
[Switch-nqa-admin-test-ftp] username administrator
```

Related commands

operation

password

2.1.44. version

Use **version** to specify the version used in the HTTP operation.

Use **undo version** to restore the default.

Syntax

version { **v1.0** | **v1.1** }

undo version

Default

Version 1.0 is used in the HTTP operation.

Views

HTTP operation view

Predefined user roles

network-admin

Parameters

v1.0: Uses version 1.0.

v1.1: Uses version 1.1.

Examples

Configure the HTTP operation to use the HTTP version 1.1.

```
<Switch> system-view
[Switch] nqa entry admin test
[Switch-nqa-admin-test] type http
[Switch-nqa-admin-test-http] version v1.1
```

2.1.45. vpn-instance

Use **vpn-instance** to apply the operation to a VPN instance.

Use **undo vpn-instance** to restore the default.

Syntax

vpn-instance *vpn-instance-name*

undo vpn-instance

Default

The operation applies to the public network.

Views

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

UDP jitter/voice operation view

Predefined user roles

network-admin

Parameters

vpn-instance-name: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

After you specify the VPN, the NQA operation tests the connectivity in the specified VPN instance.

Examples

Apply the ICMP echo operation to **vpn1**.

```
<Switch> system-view
[Switch] nqa entry admin test
[Switch-nqa-admin-test] type icmp-echo
[Switch-nqa-admin-test-icmp-echo] vpn-instance vpn1
```

2.2. NQA server commands

IMPORTANT:
Configure the NQA server only for UDP jitter, TCP, UDP echo, and voice operations.

2.2.1. display nqa server

Use **display nqa server status** to display NQA server status.

Syntax

display nqa server

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display NQA server status.

```
<Switch> display nqa server
NQA server status: Enabled
TCP connect:
   IP address          Port      Tos    VPN instance
   2.2.2.2             2000      200    -
UDP echo:
   IP address          Port      Tos    VPN instance
   3.3.3.3             3000      255    -
```

Table 2-7 Command output

Field	Description
NQA server status	Whether the NQA server is enabled.
TCP connect	Information about the TCP listening service on the NQA server.
UDP echo	Information about the UDP listening service on the NQA server.
IP address	IP address specified for the TCP/UDP listening service on the NQA server.
Port	Port number specified for the TCP/UDP listening service on the NQA server.
Tos	ToS value in reply packets sent by the NQA server.
VPN instance	Name of the VPN instance to which the IP address that the NQA server listens on belongs. This field displays a hyphen (-) if the NQA server listens on a public IP address.

Related commands

nqa server enable

nqa server tcp-connect

nqa server udp-echo

2.2.2. nqa server enable

Use **nqa server enable** to enable the NQA server.

Use **undo nqa server enable** to disable the NQA server.

Syntax

nqa server enable

undo nqa server enable

Default

The NQA server is disabled.

Views

System view

Predefined user roles

network-admin

Examples

Enable the NQA server.

```
<Switch> system-view
[Switch] nqa server enable
```

Related commands

display nqa server

nqa server tcp-connect

nqa server udp-echo

2.2.3. nqa server tcp-connect

Use **nqa server tcp-connect** to configure a TCP listening service to enable the NQA server to listen to a port on an IP address.

Use **undo nqa server tcp-connect** to remove a TCP listening service.

Syntax

nqa server tcp-connect *ip-address port-number* [**vpn-instance** *vpn-instance-name*] [**tos** *tos*]

undo nqa server tcp-connect *ip-address port-number*

Default

No TCP listening services exist.

Views

System view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the IP address for the TCP listening service.

port-number: Specifies the port number for the TCP listening service, in the range of 1 to 65535.

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the NQA server listens on a public IP address.

tos *tos*: Specifies the ToS value in the IP header for reply packets. The value range is 0 to 255, and the default value is 0.

Usage guidelines

Use this command on the NQA server only for the TCP operation.

When you configure the IP address and port number for a TCP listening service on the NQA server, follow these restrictions and guidelines:

- The IP address, port number, and VPN instance must be unique on the NQA server and match the configuration on the NQA client.
- The IP address must be the address of an interface on the NQA server.
- To ensure successful NQA operations and avoid affecting existing services, do not configure the TCP listening service on well-known ports from 1 to 1023.

Examples

Configure a TCP listening service to enable the NQA server to listen to port 9000 on the IP address 169.254.10.2.

```
<Switch> system-view
[Switch] nqa server tcp-connect 169.254.10.2 9000
```

Related commands

display nqa server

nqa server enable

2.2.4. nqa server udp-echo

Use **nqa server udp-echo** to configure a UDP listening service to enable the NQA server to listen to a port on an IP address.

Use **undo nqa server udp-echo** to remove the UDP listening service created.

Syntax

nqa server udp-echo *ip-address port-number* [**vpn-instance** *vpn-instance-name*] [**tos** *tos*]

undo nqa server udp-echo *ip-address port-number*

Default

No UDP listening services exist.

Views

System view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the IP address for the UDP listening service.

port-number: Specifies the port number for the UDP listening service, in the range of 1 to 65535.

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the NQA server listens on a public IP address.

tos *tos*: Specifies the ToS value in the IP header for reply packets. The value range for this argument is 0 to 255, and the default value is 0.

Usage guidelines

Use this command on the NQA server only for the UDP jitter, UDP echo, and voice operations.

When you configure the IP address and port number for a UDP listening service on the NQA server, follow these restrictions and guidelines:

- The IP address, port number, and VPN instance must be unique on the NQA server and match the configuration on the NQA client.
- The IP address must be the address of an interface on the NQA server.
- To ensure successful NQA operations and avoid affecting existing services, do not configure the UDP listening service on well-known ports from 1 to 1023.

Examples

Configure a UDP listening service to enable the NQA server to listen to port 9000 on the IP address 169.254.10.2.

```
<Switch> system-view
[Switch] nqa server udp-echo 169.254.10.2 9000
```

Related commands

display nqa server

nqa server enable

Contents

A page of this section is **11-x-x**

3. NTP commands 3-1
3.1. NTP commands 3-1
3.1.1. display ntp-service sessions 3-1
3.1.2. display ntp-service status 3-5
3.1.3. display ntp-service trace 3-7
3.1.4. ntp-service acl 3-8
3.1.5. ntp-service authentication enable 3-10
3.1.6. ntp-service authentication-keyid 3-10
3.1.7. ntp-service broadcast-client 3-11
3.1.8. ntp-service broadcast-server 3-12
3.1.9. ntp-service dscp 3-13
3.1.10. ntp-service enable 3-13
3.1.11. ntp-service inbound enable 3-14
3.1.12. ntp-service max-dynamic-sessions 3-14
3.1.13. ntp-service multicast-client 3-15
3.1.14. ntp-service multicast-server 3-16
3.1.15. ntp-service refclock-master 3-17
3.1.16. ntp-service reliable authentication-keyid 3-18
3.1.17. ntp-service source 3-19
3.1.18. ntp-service unicast-peer 3-20
3.1.19. ntp-service unicast-server 3-22

3. NTP commands

3.1. NTP commands

NTP is supported on the following Layer 3 interfaces:

- Layer 3 Ethernet interfaces.
- VLAN interfaces.
- Tunnel interfaces.

3.1.1. display ntp-service sessions

Use **display ntp-service sessions** to display information about all IPv4 NTP associations.

Syntax

display ntp-service sessions [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

verbose: Displays detailed information about all IPv4 NTP associations. If you do not specify this keyword, the command displays only brief information about the NTP associations.

Usage guidelines

When a device is operating in NTP broadcast or multicast server mode, the **display ntp-service sessions** command does not display the IPv4 NTP association information corresponding to the broadcast or multicast server. However, the associations are counted in the total number of associations.

Examples

Display brief information about all IPv4 NTP associations.

```
<Switch> display ntp-service sessions
       source          reference       stra reach poll  now offset  delay disper
**********************************************************************************
[12345]LOCAL(0)        LOCL              0     1    64    - 0.0000 0.0000 7937.9
    [5]0.0.0.0         INIT             16     0    64    - 0.0000 0.0000 0.0000
Notes: 1 source(master), 2 source(peer), 3 selected, 4 candidate, 5 configured.
 Total sessions: 1
```

Table 3-1 Command output

Field	Description
source	• When the reference clock is the local clock, the field displays **LOCAL** (*number*). It indicates that the IP address of the local clock is 127.127.1.*number*, where *number* represents the NTP process

Field	Description
	number in the range of 0 to 3. • When the reference clock is the clock of another device, the field displays the IP address of the NTP server. If this field displays **0.0.0.0**, the IP address of the NTP server has not been resolved successfully.

reference	Reference clock ID of the NTP server:
	• If the reference clock is the local clock, the value of this field is related to the value of the **stra** field:
	  ○ When the value of the **stra** field is 0 or 1, this field displays **LOCL**.
	  ○ When the **stra** field has another value, this field displays the IP address of the local clock.
	• If the reference clock is the clock of another device on the network, this field displays the IP address of the device. If the device supports IPv6, this field displays the MD5 digest of the first 32 bits of the IPv6 address of the device. If this field displays **INIT**, the local device has not established a connection with the NTP server.

stra	Stratum level of the clock source, which determines the clock accuracy. The value is in the range of 1 to 16. The clock accuracy decreases from stratum 1 to stratum 16. A stratum 1 clock has the highest precision, and a stratum 16 clock is not synchronized and cannot be used as a reference clock.
reach	Reachability count of the clock source. 0 indicates that the clock source is unreachable.
poll	Polling interval in seconds. It is the maximum interval between successive NTP messages.
now	Length of time from when the last NTP message was received or when the local clock was last updated to the current time. Time is in seconds by default. • If the time length is greater than 2048 seconds, it is displayed in minutes (m). • If the time length is greater than 300 minutes, it is displayed in hours (h). • If the time length is greater than 96 hours, it is displayed in days (d). • If the time length is greater than 999 days, it is displayed in years (y). If the time when the most recent NTP message was received or when the local clock was updated most recently is behind the current time, this field displays a hyphen (-).
offset	Offset of the system clock relative to the reference clock, in milliseconds.
delay	Roundtrip delay from the local device to the NTP server, in milliseconds.
disper	Maximum error of the system clock relative to the reference source, in milliseconds.
[12345]	• **1**—Clock source selected by the system (the current reference source). • **2**—The stratum level of the clock source is less than or equal to 15. • **3**—The clock source has survived the clock selection algorithm. • **4**—The clock source is a candidate clock source. • **5**—The clock source was created by a configuration command.

Field	Description
Total sessions	Total number of associations.

Display detailed information about all IPv4 NTP associations.

```
<Switch> display ntp-service sessions verbose
 Clock source: 192.168.1.40
 Session ID: 35888
 Clock stratum: 2
 Clock status:  configured, master, sane, valid
 Reference clock ID: 127.127.1.0
 VPN instance: Not specified
 Local mode: client, local poll interval: 6
 Peer mode: server, peer poll interval: 6
 Offset: 0.2862ms, roundtrip delay: 3.2653ms, dispersion: 4.5166ms
 Root roundtrip delay: 0.0000ms, root dispersion: 10.910ms
 Reachabilities:31, sync distance: 0.0194
 Precision: 2^18, version: 3, source interface: Not specified
 Reftime: d17cbba5.1473de1e  Tue, May 17 2011  9:17:25.079
 Orgtime: 00000000.00000000  Thu, Feb  7 2036  6:28:16.000
 Rcvtime: d17cbbc0.b1959a30  Tue, May 17 2011  9:17:52.693
 Xmttime: d17cbbc0.b1959a30  Tue, May 17 2011  9:17:52.693
 Roundtrip delay samples: 0.007 0.010 0.006 0.011 0.010 0.005 0.007 0.003
 Offset samples: 5629.55 3913.76 5247.27 6526.92 31.99 148.72 38.27 0.29
 Filter order: 7     5     2     6     0     4     1     3

 Total sessions: 1
```

Table 3-2 Command output

Field	Description
Clock source	IP address of the NTP server. If this field displays **0.0.0.0**, the IP address of the NTP server has not been resolved successfully.
Clock stratum	Stratum level of the NTP server, which determines the clock accuracy. The value is in the range of 1 to 16. A lower stratum level represents greater clock accuracy. A stratum 16 clock is not synchronized and cannot be used as a reference clock.
Clock status	Status of the clock source corresponding to this association: • **configured**—The association was created by a configuration command. • **dynamic**—The association is established dynamically. • **master**—The clock source is the primary reference source of the current system. • **selected**—The clock source has survived the clock selection algorithm. • **candidate**—The clock source is the candidate reference source. • **sane**—The clock source has passed authentication and will be used as a reference clock. • **insane**—The clock source has not passed authentication, or it has passed authentication but will not be used as a reference

Field	Description

	clock.
	• **valid**—The clock source is valid, which means the clock source meets the following requirements:
	  ○ It has been authenticated and synchronized.
	  ○ Its stratum level is valid.
	  ○ Its root delay and root dispersion values are within their ranges.
	• **invalid**—The clock source is invalid.
	• **unsynced**—The clock source has not been synchronized or the value of the stratum level is invalid.

Reference clock ID	Reference clock ID of the NTP server:
	• If the reference clock is the local clock, the value of this field is related to the value of the **Clock** stratum field:
	  ○ When the value of the **Clock** stratum field is 0 or 1, this field displays **LOCL**.
	  ○ When the **Clock** stratum field has another value, this field displays the IP address of the local clock.
	• If the reference clock is the clock of another device on the network, this field displays the IP address of the device. If the device supports IPv6, this field displays the MD5 digest of the first 32 bits of the IPv6 address of the device. If this field displays **INIT**, the local device has not established a connection with the NTP server.

VPN instance	VPN instance to which the NTP server belongs. If the NTP server is in a public network, the field displays **Not specified**.
Local mode	Operation mode of the local device: • **unspec**—The mode is unspecified. • **active**—Active mode. • **passive**—Passive mode. • **client**—Client mode. • **server**—Server mode. • **broadcast**—Broadcast or multicast server mode. • **bclient**—Broadcast or multicast client mode.
local poll interval	Polling interval of the local device, in seconds. The value displayed is a power of 2. For example, if the displayed value is 6, the poll interval of the local device is 2^6, or 64 seconds.
Peer mode	Operation mode of the peer device: • **unspec**—The mode is unspecified. • **active**—Active mode. • **passive**—Passive mode. • **client**—Client mode. • **server**—Server mode. • **broadcast**—Broadcast or multicast server mode. • **bclient**—Broadcast or multicast client mode.
peer poll interval	Polling interval of the peer device, in seconds. The value displayed is a power of 2. For example, if the displayed value is 6, the poll interval of the local device is 2^6, or 64 seconds.
Offset	Offset of the system clock relative to the reference clock, in milliseconds.
roundtrip delay	Roundtrip delay from the local device to the NTP server, in

Field	Description
	milliseconds.
dispersion	Maximum error of the system clock relative to the reference clock.
Root roundtrip delay	Roundtrip delay from the local device to the primary reference source, in milliseconds.
root dispersion	Maximum error of the system clock relative to the primary reference clock, in milliseconds.
Reachabilities	Reachability count of the clock source. 0 indicates that the clock source is unreachable.
sync distance	Synchronization distance relative to the upper-level clock, in seconds, and calculated from dispersion and roundtrip delay values.
Precision	Accuracy of the system clock.
version	NTP version in the range of 1 to 4.
source interface	Source interface. If the source interface is not specified, this field is **Not specified**.
Reftime	Reference timestamp in the NTP message.
Orgtime	Originate timestamp in the NTP message.
Rcvtime	Receive timestamp in the NTP message.
Xmttime	Transmit timestamp in the NTP message.
Filter order	Sample information order.
Reference clock status	Status of the local clock. The field is displayed only when you use the **ntp-service refclock-master** command to set the local clock as a reference clock. When the reach field of the local clock is 255, the field is displayed as **working normally**. Otherwise, the field is displayed as **working abnormally**.
Total sessions	Total number of associations.

3.1.2. display ntp-service status

Use **display ntp-service status** to display NTP service status.

Syntax

display ntp-service status

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display NTP service status after time synchronization.

```
<Switch> display ntp-service status
 Clock status: synchronized
```

```
 Clock stratum: 2
 System peer: LOCAL(0)
 Local mode: client
 Reference clock ID: 127.127.1.0
 Leap indicator: 00
 Clock jitter: 0.000977 s
 Stability: 0.000 pps
 Clock precision: 2^-19
 Root delay: 0.00000 ms
 Root dispersion: 3.96367 ms
 Reference time: d0c5fc32.92c70b1e  Wed, Dec 29 2010 18:28:02.573
 System poll interval: 256 s
```

Display the NTP service status when time is not synchronized.

```
<Switch> display ntp-service status
 Clock status: unsynchronized
 Clock stratum: 16
 Reference clock ID: none
 Clock jitter: 0.000000 s
 Stability: 0.000 pps
 Clock precision: 2^-19
 Clock precision:
 Root delay: 0.00000 ms
 Root dispersion: 0.00002 ms
 Reference time: d0c5fc32.92c70b1e  Wed, Dec 29 2010 18:28:02.573
 System poll interval: 8 s
```

Table 3-3 Command output

Field	Description
Clock status	Status of the system clock: • **synchronized**—The system clock has been synchronized. • **unsynchronized**—The system clock has not been synchronized.
Clock stratum	Stratum level of the system clock.
System peer	IP address of the selected NTP server.
Local mode	Operation mode of the local device: • **unspec**—The mode is unspecified. • **active**—Active mode. • **passive**—Passive mode. • **client**—Client mode. • **server**—Server mode. • **broadcast**—Broadcast or multicast server mode. • **bclient**—Broadcast or multicast client mode.
Reference clock ID	For an IPv4 NTP server: The field represents the IP address of the remote server when the local device is synchronized to a remote NTP server. The field represents the local clock when the local device uses the local clock as a reference source. • When the local clock has a stratum level of 1, this field displays

Field	Description
	LOCL. • When the local clock has any other stratum, this field displays the IP address of the local clock. For an IPv6 NTP server: The field represents the MD5 digest of the first 32 bits of the IPv6 address of the remote server when the local device is synchronized to a remote IPv6 NTP server. The field represents the local clock when the local device uses the local clock as a reference source. • When the local clock has a stratum level of 1, this field displays **LOCL**. • When the local clock has any other stratum, this field displays the MD5 digest of the first 32 bits of the IPv6 address of the local clock.
Leap indicator	Alarming status: • **00**—Normal. • **01**—Leap second, indicates that the last minute in a day has 61 seconds. • **10**—Leap second, indicates that the last minute in a day has 59 seconds. • **11**—Time is not synchronized.
Clock jitter	Difference between the system clock and reference clock, in seconds.
Stability	Clock frequency stability. A lower value represents better stability.
Clock precision	Accuracy of the system clock.
Root delay	Roundtrip delay from the local device to the primary reference source, in milliseconds.
Root dispersion	Maximum error of the system clock relative to the primary reference source, in milliseconds.
Reference time	Reference timestamp.
System poll interval	System polling interval in seconds.

3.1.3. display ntp-service trace

Use **display ntp-service trace** to display brief information about each NTP server from the local device back to the primary reference source.

Syntax

display ntp-service trace

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

To trace back to the primary reference source from the source interface, make sure the source interface and the NTP servers from the local device to the primacy reference source are reachable to each other.

Examples

Display brief information about each NTP server from the local device back to the primary reference source.

```
<Switch> display ntp-service trace
Server     127.0.0.1
Stratum    3, jitter  0.000, synch distance 0.0000.
Server     3000::32
Stratum    2 , jitter 790.00, synch distance 0.0000.
RefID      127.127.1.0
```

The output shows that server 127.0.0.1 is synchronized to server 3000::32, and server 3000::32 is synchronized to the local clock.

Table 3-4 Command output

Field	Description
Server	IP address of the NTP server.
Stratum	Stratum level of the NTP server.
jitter	Root mean square (RMS) value of the clock offset relative to the upper-level clock, in seconds.
synch distance	Synchronization distance relative to the upper-level NTP server, in seconds, calculated from dispersion and roundtrip delay values.
RefID	Identifier of the primary reference source. When the stratum level of the primary reference clock is 0, it is displayed as **LOCL**. Otherwise, it is displayed as the IP address of the primary reference clock.

Related commands

ntp-service source

ntp-service unicast-server

ntp-service unicast-peer

3.1.4. ntp-service acl

Use **ntp-service acl** to configure the right for peer devices to access the IPv4 NTP services on the local device.

Use **undo ntp-service** to remove the configured IPv4 NTP service access right.

Syntax

ntp-service { **peer** | **query** | **server** | **synchronization** } **acl** *ipv4-acl-number*

undo ntp-service { **peer** | **query** | **server** | **synchronization** } [**acl** *ipv4-acl-number*]

Default

The right for the peer devices to access the IPv4 NTP services on the local device is **peer**.

Views

System view

Predefined user roles

network-admin

Parameters

peer: Allows time requests and NTP control queries (such as alarms, authentication status, and time server information) from a peer device and allows the local device to synchronize itself to a peer device.

query: Allows only NTP control queries from a peer device to the local device.

server: Allows time requests and NTP control queries from a peer device, but does not allow the local device to synchronize itself to a peer device.

synchronization: Allows only time requests from a peer device.

acl *ipv4-acl-number*: Specifies an IPv4 ACL by its number. The peer devices that match the IPv4 ACL have the access right specified in the command. The *ipv4-acl-number* argument represents an IPv4 basic ACL number in the range of 2000 to 2999 or an IPv4 advanced ACL number in the range of 3000 to 3999.

Usage guidelines

When the device receives an IPv4 NTP request, it matches the request against the access rights in order from the least restrictive to the most restrictive: **peer**, **server**, **synchronization**, and **query**.

- If no IPv4 NTP access control is configured, the **peer** access right applies.
- If the IP address of the peer device matches a **permit** statement in an IPv4 ACL, the access right is granted to the peer device. If a **deny** statement or no IPv4 ACL is matched, no access right is granted.
- If no IPv4 ACL is specified for an access right or the IPv4 ACL specified for the access right is not created, the access right is not granted.
- If none of the IPv4 ACLs specified for the access rights is created, the **peer** access right applies.
- If none of the IPv4 ACLs specified for the access rights contains rules, no access right is granted.

The **ntp-service acl** command provides minimal security for a system running NTP. A more secure method is NTP authentication.

Examples

Configure the peer devices on subnet 10.10.0.0/16 to have full access to the local device.

```
<Switch> system-view
[Switch] acl basic 2001
[Switch-acl-ipv4-basic-2001] rule permit source 10.10.0.0 0.0.255.255
[Switch-acl-ipv4-basic-2001] quit
[Switch] ntp-service peer acl 2001
```

Related commands

ntp-service authentication enable

ntp-service authentication-keyid

ntp-service reliable authentication-keyid

3.1.5. ntp-service authentication enable

Use **ntp-service authentication enable** to enable NTP authentication.

Use **undo ntp-service authentication enable** to disable NTP authentication.

Syntax

ntp-service authentication enable

undo ntp-service authentication enable

Default

NTP authentication is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Enable NTP authentication in networks that require time synchronization security to make sure NTP clients are synchronized only to authenticated NTP servers.

To authenticate an NTP server, set an authentication key and specify it as a trusted key.

Examples

Enable NTP authentication.

```
<Switch> system-view
[Switch] ntp-service authentication enable
```

Related commands

ntp-service authentication-keyid

ntp-service reliable authentication-keyid

3.1.6. ntp-service authentication-keyid

Use **ntp-service authentication-keyid** to set an NTP authentication key.

Use **undo ntp-service authentication-keyid** to remove an NTP authentication key.

Syntax

ntp-service authentication-keyid *keyid* **authentication-mode md5** { **cipher** | **simple** } *string*

undo ntp-service authentication-keyid *keyid*

Default

No NTP authentication key exists.

Views

System view

Predefined user roles

network-admin

Parameters

keyid: Specifies an authentication key ID in the range of 1 to 4294967295.

authentication-mode: Specifies an authentication algorithm.

- **md5**: Specifies the MD5 algorithm.

cipher: Specifies an authentication key in encrypted form.

simple: Specifies an authentication key in plaintext form. For security purposes, the authentication key specified in plaintext form will be stored in encrypted form.

string: Specifies a case-sensitive authentication key. Its plaintext form is a string of 1 to 32 characters. Its encrypted form is a string of 1 to 73 characters.

Usage guidelines

In a network where there is a high security demand, the NTP authentication feature must be enabled for a system running NTP. This feature enhances the network security by using client-server key authentication, which prohibits a client from synchronizing to a device that has failed the authentication.

To ensure a successful NTP authentication, configure the same key ID, authentication algorithm, and key on the time server and client.

After you specify an NTP authentication key, use the **ntp-service reliable authentication-keyid** command to configure the key as a trusted key. The key automatically changes to untrusted after you delete the key. In this case, you do not need to execute the **undo ntp-service reliable authentication-keyid** command.

You can set a maximum of 128 authentication keys by executing the command.

Examples

Set a plaintext MD5 authentication key, with the key ID of **10** and key value of **BetterKey**.

```
<Switch> system-view
[Switch] ntp-service authentication enable
[Switch] ntp-service authentication-keyid 10 authentication-mode md5 simple BetterKey
```

Related commands

ntp-service authentication enable

ntp-service reliable authentication-keyid

3.1.7. ntp-service broadcast-client

Use **ntp-service broadcast-client** to configure the device to operate in NTP broadcast client mode and use the current interface to receive NTP broadcast packets.

Use **undo ntp-service broadcast-client** to remove the configuration.

Syntax

ntp-service broadcast-client

undo ntp-service broadcast-client

Default

The device does not operate in any NTP association mode.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

After you configure the command, the device listens to NTP messages sent by the NTP broadcast server and is synchronized based on the received NTP messages.

If you have configured the device to operate in broadcast client mode on an interface with the command, do not add the interface to any aggregate group. To add the interface to an aggregate group, remove the configuration of the command.

Examples

Configure the device to operate in broadcast client mode and receive NTP broadcast messages on VLAN-interface 1.

```
<Switch> system-view
[Switch] interface vlan-interface 1
[Switch-Vlan-interface1] ntp-service broadcast-client
```

Related commands

ntp-service broadcast-server

3.1.8. ntp-service broadcast-server

Use **ntp-service broadcast-server** to configure the device to operate in NTP broadcast server mode and use the current interface to send NTP broadcast packets.

Use **undo ntp-service broadcast-server** to remove the configuration.

Syntax

ntp-service broadcast-server [**authentication-keyid** *keyid* | **version** *number*] *

undo ntp-service broadcast-server

Default

The device does not operate in any NTP association mode.

Views

Interface view

Predefined user roles

network-admin

Parameters

authentication-keyid *keyid*: Specifies the key ID to be used for sending broadcast messages to broadcast clients. The value range for the *keyid* argument is 1 to 4294967295. If you do not specify this option, the local device cannot synchronize broadcast clients enabled with NTP authentication.

version *number*: Specifies the NTP version. The value range for the *number* argument is 1 to 4, and the default is 4.

Usage guidelines

After you configure the command, the device periodically sends NTP messages to the broadcast address 255.255.255.255.

If you have configured the device to operate in broadcast server mode on an interface with the command, do not add the interface to any aggregate group. To add the interface to an aggregate group, remove the configuration of the command.

Examples

Configure the device to operate in broadcast server mode and send NTP broadcast messages on VLAN-interface 1, using key 4 for encryption. Set the NTP version to 4.

```
<Switch> system-view
[Switch] interface vlan-interface 1
[Switch-Vlan-interface1] ntp-service broadcast-server authentication-keyid 4 version 4
```

Related commands

ntp-service broadcast-client

3.1.9. ntp-service dscp

Use **ntp-service dscp** to set a DSCP value for IPv4 NTP packets.

Use **undo ntp-service dscp** to restore the default.

Syntax

ntp-service dscp *dscp-value*

undo ntp-service dscp

Default

The DSCP value for IPv4 NTP packets is 48.

Views

System view

Predefined user roles

network-admin

Parameters

dscp-value: Sets a DSCP value in the range of 0 to 63 for IPv4 NTP packets.

Usage guidelines

The DSCP value is included in the ToS field of an IPv4 packet to identify the packet priority.

Examples

Set the DSCP value for IPv4 NTP packets to **30**.

```
<Switch> system-view
[Switch] ntp-service dscp 30
```

3.1.10. ntp-service enable

Use **ntp-service enable** to enable the NTP service.

Use **undo ntp-service enable** to disable the NTP service.

Syntax

ntp-service enable

undo ntp-service enable

Default

The NTP service is disabled.

Views

System view

Predefined user roles

network-admin

Examples

Enable the NTP service.

```
<Switch> system-view
[Switch] ntp-service enable
```

3.1.11. ntp-service inbound enable

Use **ntp-service inbound enable** to enable an interface to receive NTP messages.

Use **undo ntp-service inbound enable** to disable an interface from receiving NTP messages.

Syntax

ntp-service inbound enable

undo ntp-service inbound enable

Default

An interface receives NTP messages.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

Execute the **undo ntp-service inbound enable** command on an interface in the following cases:

- You do not want the interface to synchronize the peer device in the corresponding subnet.
- You do not want the device to be synchronized by the peer device in the subnet corresponding to the interface.

Examples

Disable VLAN-interface 1 from receiving NTP messages.

```
<Switch> system-view
[Switch] interface vlan-interface 1
[Switch-Vlan-interface1] undo ntp-service inbound enable
```

3.1.12. ntp-service max-dynamic-sessions

Use **ntp-service max-dynamic-sessions** to set the maximum number of dynamic NTP sessions.

Use **undo ntp-service max-dynamic-sessions** to restore the default.

Syntax

ntp-service max-dynamic-sessions *number*

undo ntp-service max-dynamic-sessions

Default

The maximum number of dynamic NTP sessions is 100.

Views

System view

Predefined user roles

network-admin

Parameters

number: Sets the maximum number of dynamic NTP associations, in the range of 0 to 100.

Usage guidelines

A device can have a maximum of 128 concurrent associations, including static associations and dynamic associations. A static association refers to an association that a user has manually created by using an NTP command. A dynamic association is a temporary association created by the system during operation.

This command limits the number of dynamic NTP associations and prevents dynamic NTP associations from occupying too many system resources.

Examples

Set the maximum number of dynamic NTP associations to 50.

```
<Switch> system-view
[Switch] ntp-service max-dynamic-sessions 50
```

Related commands

display ntp-service sessions

3.1.13. ntp-service multicast-client

Use **ntp-service multicast-client** to configure the device to operate in NTP multicast client mode and use the current interface to receive NTP multicast packets.

Use **undo ntp-service multicast-client** to remove the configuration.

Syntax

ntp-service multicast-client [*ip-address*]

undo ntp-service multicast-client [*ip-address*]

Default

The device does not operate in any NTP association mode.

Views

Interface view

Predefined user roles

network-admin

Parameters

ip-address: Specifies a multicast IP address. The default is 224.0.1.1. A multicast server and client must be configured with the same multicast IP address.

Usage guidelines

After you configure the command, the device listens to NTP messages using the specified multicast address as the destination address.

If you have configured the device to operate in multicast client mode on an interface with the command, do not add the interface to any aggregate group. To add the interface to an aggregate group, remove the configuration of the command.

The value range for the *ip-address* argument is 224.0.1.1 to 224.0.1.255 for VLAN interfaces and for Layer 3 Ethernet interfaces on the master device in an IRF fabric.

Examples

Configure the device to operate in multicast client mode and receive NTP multicast messages on VLAN-interface 1, and set the multicast address to 224.0.1.1.

```
<Switch> system-view
[Switch] interface vlan-interface 1
[Switch-Vlan-interface1] ntp-service multicast-client 224.0.1.1
```

Related commands

ntp-service multicast-server

3.1.14. ntp-service multicast-server

Use **ntp-service multicast-server** to configure the device to operate in NTP multicast server mode and use the current interface to send NTP multicast packets.

Use **undo ntp-service multicast-server** to remove the configuration.

Syntax

ntp-service multicast-server [*ip-address*] [**authentication-keyid** *keyid* | **ttl** *ttl-number* | **version** *number*] *

undo ntp-service multicast-server [*ip-address*]

Default

The device does not operate in any NTP association mode.

Views

Interface view

Predefined user roles

network-admin

Parameters

ip-address: Specifies a multicast IP address. The default is 224.0.1.1. A multicast server and client must be configured with the same multicast IP address.

authentication-keyid *keyid*: Specifies the key ID to be used for sending multicast messages to multicast clients. The value range for the *keyid* argument is 1 to 4294967295. If you do not specify this option, the local device cannot synchronize multicast clients enabled with NTP authentication.

ttl *ttl-number*: Specifies the TTL of NTP multicast messages. The value range for the *ttl-number* argument is 1 to 255. The default value is 16.

version *number*: Specifies the NTP version. The value range for the *number* argument is 1 to 4. The default value is 4.

Usage guidelines

After you configure the command, the device periodically sends NTP messages to the specified multicast address.

If you have configured the device to operate in multicast server mode on an interface with the command, do not add the interface to any aggregate group. To add the interface to an aggregate group, remove the configuration of the command.

The value range for the *ip-address* argument is 224.0.1.1 to 224.0.1.255 for VLAN interfaces and for Layer 3 Ethernet interfaces on the master device in an IRF fabric.

Examples

Configure the device to operate in multicast server mode and send NTP multicast messages on VLAN-interface 1 to the multicast address 224.0.1.1, using key 4 for encryption. Set the NTP version to 4.

```
<Switch> system-view
[Switch] interface vlan-interface 1
[Switch-Vlan-interface1] ntp-service multicast-server 224.0.1.1 version 4
authentication-keyid 4
```

Related commands

ntp-service multicast-client

3.1.15. ntp-service refclock-master

Use **ntp-service refclock-master** to configure the local clock as the reference source.

Use **undo ntp-service refclock-master** to remove the configuration.

Syntax

ntp-service refclock-master [*ip-address*] [*stratum*]

undo ntp-service refclock-master [*ip-address*]

Default

The device does not use its local clock as the reference clock.

Views

System view

Predefined user roles

network-admin

Parameters

ip-address: IP address of the local clock, 127.127.1.*u*, where *u* is the NTP process ID in the range of 0 to 3. The default value is 127.127.1.0.

stratum: Stratum level of the local clock, in the range of 1 to 15. The default value is 8. A lower stratum level represents higher clock accuracy.

Usage guidelines

Typically an NTP server that gets its time from an authoritative time source, such as an atomic clock has stratum 1 and operates as the primary time server to provide time synchronization for other devices in the network. The accuracy of each server is the stratum, with the topmost level (primary servers) assigned as one and each level downwards (secondary servers) in the hierarchy assigned as one greater than the preceding level.

If the devices in a network cannot synchronize to an authoritative time source, you can perform the following tasks:

- Select a device that has a relatively accurate clock from the network.
- Use the local clock of the device as the reference clock to synchronize other devices in the network.

Use the command with caution to avoid time errors. As a best practice, set the local clock time to a correct value before you execute the command.

Examples

Specify the local clock as the reference source, with the stratum level 2.

```
<Switch> system-view
[Switch] ntp-service refclock-master 2
```

3.1.16. ntp-service reliable authentication-keyid

Use **ntp-service reliable authentication-keyid** to specify an authentication key as a trusted key.

Use **undo ntp-service reliable authentication-keyid** to remove the configuration.

Syntax

ntp-service reliable authentication-keyid *keyid*

undo ntp-service reliable authentication-keyid *keyid*

Default

No trusted key is specified.

Views

System view

Predefined user roles

network-admin

Parameters

keyid: Specifies an authentication key by its ID in the range of 1 to 4294967295.

Usage guidelines

When NTP authentication is enabled, a client can be synchronized only to a server that can provide a trusted authentication key.

Before you use the command, make sure NTP authentication is enabled and an authentication key is configured. The key automatically changes to untrusted after you delete the key. In this case, you do not need to execute the **undo ntp-service reliable authentication-keyid** command.

You can set a maximum of 128 keys by executing the command.

Examples

Enable NTP authentication, specify the MD5 algorithm, with the key ID of 37 and key value of **BetterKey**.

```
<Switch> system-view
[Switch] ntp-service authentication enable
[Switch] ntp-service authentication-keyid 37 authentication-mode md5 simple BetterKey
```

Specify this key as a trusted key.

```
[Switch] ntp-service reliable authentication-keyid 37
```

Related commands

ntp-service authentication enable

ntp-service authentication-keyid

3.1.17. ntp-service source

Use **ntp-service source** to specify a source interface for NTP messages.

Use **undo ntp-service source** to restore the default.

Syntax

ntp-service source *interface-type interface-number*

undo ntp-service source

Default

No source interface is specified for NTP messages. The device performs the following operations:

- Searches the routing table for the outbound interface of NTP messages.
- Uses the primary IP address of the outbound interface as the source IP address for NTP messages.

Views

System view

Predefined user roles

network-admin

Parameters

interface-type interface-number: Specifies an interface by its type and number.

Usage guidelines

If you specify a source interface for NTP messages, the device uses the primary IP address of the specified interface as the source IP address to send NTP messages. Consequently, the destination address of the NTP response messages is the primary IP address of the source interface.

When the device responds to an NTP request, the source IP address of the NTP response is always the IP address of the interface that has received the NTP request.

If you do not want the IP address of an interface on the local device to become the destination address for response messages, use the command to specify another interface as the source interface for NTP messages.

The source interface for NTP messages can also be specified in the following ways:

- In NTP client/server mode, if you have specified the source interface for NTP messages in the **ntp-service unicast-server** command, the specified interface acts as the source interface for NTP messages.
- In NTP symmetric active/passive mode, if you have specified the source interface for NTP messages in the **ntp-service unicast-peer** command, the specified interface acts as the source interface for NTP messages.
- In NTP multicast mode, if you have configured the **ntp-service multicast-server** command on an interface, the interface acts as the source interface for NTP multicast messages.
- In NTP broadcast mode, if you have configured the **ntp-service broadcast-server** command on an interface, the interface acts as the source interface for NTP broadcast messages.

If the specified source interface is down, the device does not send NTP messages.

Examples

Specify the source interface for NTP messages as VLAN-interface 1.

```
<Switch> system-view
[Switch] ntp-service source vlan-interface 1
```

3.1.18. ntp-service unicast-peer

Use **ntp-service unicast-peer** to specify a symmetric-passive peer for the device.

Use **undo ntp-service unicast-peer** to remove the symmetric-passive peer specified for the device.

Syntax

ntp-service unicast-peer { *peer-name* | *ip-address* } [**vpn-instance** *vpn-instance-name*] [**authentication-keyid** *keyid* | **maxpoll** *maxpoll-interval* | **minpoll** *minpoll-interval* | **priority** | **source** *interface-type interface-number* | **version** *number*] *

undo ntp-service unicast-peer { *peer-name* | *ip-address* } [**vpn-instance** *vpn-instance-name*]

Default

No symmetric-passive peer is specified.

Views

System view

Predefined user roles

network-admin

Parameters

peer-name: Specifies a symmetric-passive peer by its host name, a case-insensitive string of 1 to 253 characters.

ip-address: Specifies a symmetric-passive peer by its IP address. It must be a unicast address, rather than a broadcast address, a multicast address, or the IP address of the local clock.

vpn-instance *vpn-instance-name*: Specifies the VPN instance to which the symmetric-passive peer belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If the symmetric-passive peer is on the public network, do not specify this option.

authentication-keyid *keyid*: Specifies the key ID to be used for sending NTP messages to the peer. The value range for the *keyid* argument is 1 to 4294967295. If you do not specify this option, the local device and the peer do not authenticate each other.

maxpoll *maxpoll-interval*: Specifies the maximum polling interval. The value range for the *maxpoll-interval* argument is 4 to 17, to which base 2 is raised to get the interval in seconds. The maximum polling interval is in the range of 2^4 to 2^{17} (16 to 131072) seconds. The default value for the *maxpoll-interval* argument is 6 and the default maximum polling interval is 2^6 (64) seconds.

minpoll *minpoll-interval*: Specifies the minimum polling interval. The value range for the *minpoll-interval* argument is 4 to 17, to which base 2 is raised to get the interval in seconds. The minimum polling interval is in the range of 2^4 to 2^{17} (16 to 131072) seconds. The default value for the *minpoll-interval* argument is 6 and the default minimum polling interval is 2^6 (64) seconds.

priority: Specifies the peer specified by *ip-address* or *peer-name* as the first choice under the same condition.

source *interface-type interface-number*: Specifies the source interface for NTP messages. In an NTP message the local device sends to its peer, the source IP address is the primary IP address of this interface. The *interface-type interface-number* argument represents the interface type and number. If you do not specify this option, the device searches the routing table for the outgoing interface and uses the primary IP address of the outgoing interface as the source IP address of the NTP messages.

version *number*: Specifies the NTP version. The value range for the *number* argument is 1 to 4. The default value is 4.

Usage guidelines

When you specify a passive peer for the device, the device and its passive peer can be synchronized to each other. If their clocks are in synchronized state, the clock with a high stratum level is synchronized to the clock with a lower stratum level.

To synchronize the PE to a PE or CE in a VPN instance, provide **vpn-instance** *vpn-instance-name* in your command.

If you include **vpn-instance** *vpn-instance-name* in the **undo ntp-service unicast-peer** command, the command removes the symmetric-passive peer in the specified VPN instance. If you do not include **vpn-instance** *vpn-instance-name* in the command, the command removes the symmetric-passive peer on the public network.

After you specify a symmetric-passive peer for a device, the device polls and synchronizes its time with the peer device at the minimum polling interval. If the time discrepancy between the two maintains in the acceptable range, the system gradually increases the polling interval until the maximum polling interval is reached. If the time discrepancy exceeds the acceptable range repeatedly, the polling interval decreases gradually.

The polling interval configuration takes effect from the next polling.

Examples

Specify the device with the IP address of 10.1.1.1 as the symmetric-passive peer of the device, and configure the device to run NTP version 4. Specify the source interface of NTP messages as VLAN-interface 1.

```
<Switch> system-view
[Switch] ntp-service unicast-peer 10.1.1.1 version 4 source-interface vlan-interface 1
```

Related commands

ntp-service authentication enable

ntp-service authentication-keyid

ntp-service reliable authentication-keyid

3.1.19. ntp-service unicast-server

Use **ntp-service unicast-server** to specify an NTP server for the device.

Use **undo ntp-service unicast-server** to remove an NTP server specified for the device.

Syntax

ntp-service unicast-server { *server-name* | *ip-address* } [**vpn-instance** *vpn-instance-name*] [**authentication-keyid** *keyid* | **maxpoll** *maxpoll-interval* | **minpoll** *minpoll-interval* | **priority** | **source** *interface-type interface-number* | **version** *number*] *

undo ntp-service unicast-server { *server-name* | *ip-address* } [**vpn-instance** *vpn-instance-name*]

Default

No NTP server is specified.

Views

System view

Predefined user roles

network-admin

Parameters

server-name: Specifies an NTP server by its host name, a case-insensitive string of 1 to 253 characters.

ip-address: Specifies an NTP server by its IP address. It must be a unicast address, rather than a broadcast address, a multicast address, or the IP address of the local clock.

vpn-instance *vpn-instance-name*: Specifies the VPN instance to which the NTP server belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If the NTP server is on the public network, do not specify this option.

authentication-keyid *keyid*: Specifies the key ID to be used for sending NTP messages to the NTP server. The value range for the *keyid* argument is 1 to 4294967295. If you do not specify this option, the local device and NTP server do not authenticate each other.

maxpoll *maxpoll-interval*: Specifies the maximum polling interval. The value range for the *maxpoll-interval* argument is 4 to 17, to which base 2 is raised to get the interval in seconds. The maximum polling interval is in the range of 2^4 to 2^{17} (16 to 131072) seconds. The default value for the *maxpoll-interval* argument is 6 and the default maximum polling interval is 2^6 (64) seconds.

minpoll *minpoll-interval*: Specifies the minimum polling interval. The value range for the *minpoll-interval* argument is 4 to 17, to which base 2 is raised to get the interval in seconds. The minimum polling interval is in the range of 2^4 to 2^{17} (16 to 131072) seconds. The default value for the *minpoll-interval* argument is 6 and the default minimum polling interval is 2^6 (64) seconds.

priority: Specifies this NTP server as the first choice under the same condition.

source *interface-type interface-number*: Specifies the source interface for NTP messages. For an NTP message the local device sends to the NTP server, the source IP address is the primary IP address of this interface. The *interface-type interface-number* argument represents the interface type and number. If you do not specify this option, the device searches the

routing table for the outgoing interface and uses the primary IP address of the outgoing interface as the source IP address of the NTP messages.

version *number*: Specifies the NTP version. The value range for the *number* argument is 1 to 4. The default value is 4.

Usage guidelines

When you specify an NTP server for the device, the device is synchronized to the NTP server, but the NTP server is not synchronized to the device.

To synchronize the PE to a PE or CE in a VPN instance, provide **vpn-instance** *vpn-instance-name* in your command.

If you include the **vpn-instance** *vpn-instance-name* option in the **undo ntp-service unicast-server** command, the command removes the NTP server in the specified VPN instance. If you do not include the **vpn-instance** *vpn-instance-name* option in the command, the command removes the NTP server on the public network.

After you specify an NTP server for a device, the device polls and synchronizes its time with the server at the minimum polling interval. If the time discrepancy between the two maintains in the acceptable range, the system gradually increases the polling interval until the maximum polling interval is reached. If the time discrepancy exceeds the acceptable range repeatedly, the polling interval decreases gradually.

The polling interval configuration takes effect from the next polling.

Examples

Specify NTP server 10.1.1.1 for the device, and configure the device to run NTP version 4.

```
<Switch> system-view
[Switch] ntp-service unicast-server 10.1.1.1 version 4
```

Related commands

ntp-service authentication enable

ntp-service authentication-keyid

ntp-service reliable authentication-keyid

Contents

A page of this section is **11-x-x**

4. SNMP commands ····· 4-1
4.1. SNMP commands ····· 4-1
4.1.1. display snmp-agent community ····· 4-1
4.1.2. display snmp-agent group ····· 4-3
4.1.3. display snmp-agent local-engineid ····· 4-4
4.1.4. display snmp-agent mib-view ····· 4-4
4.1.5. display snmp-agent statistics ····· 4-6
4.1.6. display snmp-agent sys-info ····· 4-8
4.1.7. display snmp-agent trap queue ····· 4-8
4.1.8. display snmp-agent trap-list ····· 4-9
4.1.9. display snmp-agent usm-user ····· 4-10
4.1.10. enable snmp trap updown ····· 4-12
4.1.11. snmp-agent ····· 4-12
4.1.12. snmp-agent { inform | trap } source ····· 4-13
4.1.13. snmp-agent calculate-password ····· 4-14
4.1.14. snmp-agent community ····· 4-15
4.1.15. snmp-agent group ····· 4-17
4.1.16. snmp-agent local-engineid ····· 4-20
4.1.17. snmp-agent log ····· 4-21
4.1.18. snmp-agent mib-view ····· 4-21
4.1.19. snmp-agent packet max-size ····· 4-23
4.1.20. snmp-agent packet response dscp ····· 4-23
4.1.21. snmp-agent sys-info contact ····· 4-24
4.1.22. snmp-agent sys-info location ····· 4-24
4.1.23. snmp-agent sys-info version ····· 4-25
4.1.24. snmp-agent target-host ····· 4-26
4.1.25. snmp-agent trap enable ····· 4-27
4.1.26. snmp-agent trap if-mib link extended ····· 4-29
4.1.27. snmp-agent trap life ····· 4-29
4.1.28. snmp-agent trap log ····· 4-30
4.1.29. snmp-agent trap periodical-interval ····· 4-30
4.1.30. snmp-agent trap queue-size ····· 4-31
4.1.31. snmp-agent usm-user { v1 | v2c } ····· 4-32
4.1.32. snmp-agent usm-user v3 ····· 4-34

4. SNMP commands

4.1. SNMP commands

The SNMP agent sends notifications (traps and informs) to inform the NMS of significant events, such as link state changes and user logins or logouts. Unless otherwise stated, the **trap** keyword in the command line includes both traps and informs.

4.1.1. display snmp-agent community

Use **display snmp-agent community** to display information about SNMPv1 or SNMPv2c communities.

Syntax

display snmp-agent community [**read** | **write**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

read: Specifies SNMP read-only communities.

write: Specifies SNMP read and write communities.

Usage guidelines

If you do not specify the **read** or **write** keyword, this command displays information about all SNMPv1 and SNMPv2c communities.

This command displays SNMPv1 and SNMPv2c communities created in the following ways:

- Created by using the **snmp-agent community** command.
- Automatically created by the system for SNMPv1 and SNMPv2c users that have been assigned to an existing SNMP group.

Examples

Display information about all SNMPv1 and SNMPv2c communities.

```
<Switch> display snmp-agent community
   Community name: aa
       Group name: aa
       ACL:2001
       Storage-type: nonVolatile
       Context name: con1

   Community name: bb
       Role name: bb
       Storage-type: nonVolatile
```

```
   Community name: userv1
       Group name: testv1
       Storage-type: nonvolatile
Community name: cc
       Group name: cc
       ACL name: testacl
       Storage-type: nonVolatile
```

Table 4-1 Command output

Field	Description
Community name	Community name created by using the **snmp-agent community** command or username created by using the **snmp-agent usm-user** { **v1** | **v2c** } command.
Group name	SNMP group name. • If the community is created by using the **snmp-agent community** command in VACM mode, the group name is the same as the community name. • If the community is created by using the **snmp-agent usm-user** { **v1** | **v2c** } command, the name of the group that has the user is displayed.
Role name	User role name for the community.
ACL	Number of the ACL. This field appears only when an ACL is specified for the SNMPv1 or SNMPv2c community. It is exclusive with the **ACL name** field.
ACL name	Name of the ACL. This field appears only when an ACL is specified for the SNMPv1 or SNMPv2c community. It is exclusive with the **ACL** field.
Storage-type	Storage type: • **volatile**—Settings are lost when the system reboots. • **nonVolatile**—Settings remain after the system reboots. • **permanent**—Settings remain after the system reboots and can be modified but not deleted. • **readOnly**—Settings remain after the system reboots and cannot be modified or deleted. • **other**—Any other storage type.
Context name	SNMP context: • If a mapping between the SNMP community and an SNMP context is configured, the SNMP context is displayed. • If no mapping between the SNMP community and an SNMP context exists, this field is empty.

Related commands

snmp-agent community

snmp-agent usm-user { **v1** | **v2c** }

4.1.2. display snmp-agent group

Use **display snmp-agent group** to display information about SNMP groups.

Syntax

display snmp-agent group [*group-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

group-name: Specifies a SNMPv1, SNMPv2c, or SNMPv3 group name. It is a case-sensitive string of 1 to 32 characters. If you do not specify a group, this command displays information about all SNMP groups.

Examples

Display information about all SNMP groups.

```
<Switch> display snmp-agent group
   Group name: groupv3
       Security model: v3 noAuthnoPriv
       Readview: ViewDefault
       Writeview: <no specified>
       Notifyview: <no specified>
       Storage-type: nonvolatile
        ACL name: testacl
```

Table 4-2 Command output

Field	Description
Group name	SNMP group name.
Security model	Security model of the SNMP group: • **authPriv**—Authentication with privacy. • **authNoPriv**—Authentication without privacy. • **noAuthNoPriv**—No authentication, no privacy. Security model of a SNMPv1 or SNMPv2c group can only be noAuthNoPriv.
Readview	Read-only MIB view accessible to the SNMP group.
Writeview	Write MIB view accessible to the SNMP group.
Notifyview	Notify MIB view for the SNMP group. The SNMP users in the group can send notifications only for the nodes in the notify MIB view.
Storage-type	Storage type, including **volatile**, **nonvolatile**, **permanent**, **readOnly**, and **other**. For more information, see Table 4-1 .
ACL	Number of the ACL. This field appears only when an ACL is specified for the SNMP group. It is exclusive with the **ACL name** field.

Field	Description
ACL name	Name of the ACL. This field appears only when an ACL is specified for the SNMP group. It is exclusive with the **ACL** field.

Related commands

snmp-agent group

4.1.3. display snmp-agent local-engineid

Use **display snmp-agent local-engineid** to display the local SNMP engine ID.

Syntax

display snmp-agent local-engineid

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

Every SNMP entity has one SNMP engine to provide services for sending and receiving messages, authenticating and encrypting messages, and controlling access to managed objects.

An SNMP engine ID uniquely identifies an SNMP entity in an SNMP domain.

Examples

Display the local SNMP engine ID.

```
<Switch> display snmp-agent local-engineid
   SNMP local engine ID: 800063A2800084E52BED7900000001
```

Related commands

snmp-agent local-engineid

4.1.4. display snmp-agent mib-view

Use **display snmp-agent mib-view** to display MIB views.

Syntax

display snmp-agent mib-view [**exclude** | **include** | **viewname** *view-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

exclude: Displays the subtrees excluded from any MIB view.

include: Displays the subtrees included in any MIB view.

viewname *view-name*: Displays information about the specified MIB view. The *view-name* argument is a case-sensitive string of 1 to 32 characters.

Usage guidelines

If you do not specify any parameters, this command displays all MIB views.

Examples

Display all MIB views.

```
<Switch> display snmp-agent mib-view
   View name: ViewDefault
       MIB Subtree: iso
       Subtree mask:
       Storage-type: nonVolatile
       View Type: included
       View status: active

   View name: ViewDefault
       MIB Subtree: snmpUsmMIB
       Subtree mask:
       Storage-type: nonVolatile
       View Type: excluded
       View status: active

   View name: ViewDefault
       MIB Subtree: snmpVacmMIB
       Subtree mask:
       Storage-type: nonVolatile
       View Type: excluded
       View status: active

   View name: ViewDefault
       MIB Subtree: snmpModules.18
       Subtree mask:
       Storage-type: nonVolatile
       View Type: excluded
       View status: active
```

ViewDefault is the default MIB view. The output shows that except for the MIB objects in the **snmpUsmMIB**, **snmpVacmMIB**, and **snmpModules.18** subtrees, all the MIB objects in the **iso** subtree are accessible.

Table 4-3 Command output

Field	Description
View name	MIB view name.
MIB Subtree	MIB subtree covered by the MIB view.
Subtree mask	MIB subtree mask.
Storage-type	Type of the medium (see Table 4-1) where the subtree view is stored.

Field	Description
View Type	Access privilege for the MIB subtree in the MIB view: • **Included**—All objects in the MIB subtree are accessible in the MIB view. • **Excluded**—None of the objects in the MIB subtree is accessible in the MIB view.
View status	Status of the MIB view: • **active**—MIB view is effective. • **inactive**—MIB view is ineffective. The objects in the MIB view are not accessible, but they can send notifications.

Related commands

snmp-agent mib-view

4.1.5. display snmp-agent statistics

Use **display snmp-agent statistics** to display SNMP message statistics.

Syntax

display snmp-agent statistics

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display SNMP message statistics.

```
<Switch> display snmp-agent statistics
  1684 messages delivered to the SNMP entity.
  5 messages were for an unsupported version.
  0 messages used an unknown SNMP community name.
  0 messages represented an illegal operation for the community supplied.
  0 ASN.1 or BER errors in the process of decoding.
  1679 messages passed from the SNMP entity.
  0 SNMP PDUs had badValue error-status.
  0 SNMP PDUs had genErr error-status.
  0 SNMP PDUs had noSuchName error-status.
  0 SNMP PDUs had tooBig error-status (Maximum packet size 1500).
  16544 MIB objects retrieved successfully.
  2 MIB objects altered successfully.
  7 GetRequest-PDU accepted and processed.
  7 GetNextRequest-PDU accepted and processed.
  1653 GetBulkRequest-PDU accepted and processed.
  1669 GetResponse-PDU accepted and processed.
  2 SetRequest-PDU accepted and processed.
  0 Trap PDUs accepted and processed.
```

```
0 alternate Response Class PDUs dropped silently.
0 forwarded Confirmed Class PDUs dropped silently.
```

Table 4-4 Command output

Field	Description
messages delivered to the SNMP entity	Number of messages that the SNMP agent has received.
messages were for an unsupported version	Number of messages that are not supported by the SNMP agent version.
messages used an unknown SNMP community name	Number of messages that used an unknown SNMP community name.
messages represented an illegal operation for the community supplied	Number of messages carrying an operation that the community has no right to perform.
ASN.1 or BER errors in the process of decoding	Number of messages that had ASN.1 or BER errors during decoding.
messages passed from the SNMP entity	Number of messages sent by the SNMP agent.
SNMP PDUs had badValue error-status	Number of PDUs with a BadValue error.
SNMP PDUs had genErr error-status	Number of PDUs with a genErr error.
SNMP PDUs had noSuchName error-status	Number of PDUs with a NoSuchName error.
SNMP PDUs had tooBig error-status	Number of PDUs with a TooBig error (the maximum packet size is 1500 bytes).
MIB objects retrieved successfully	Number of MIB objects that have been successfully retrieved.
MIB objects altered successfully	Number of MIB objects that have been successfully modified.
GetRequest-PDU accepted and processed	Number of GetRequest requests that have been received and processed.
GetNextRequest-PDU accepted and processed	Number of getNext requests that have been received and processed.
GetBulkRequest-PDU accepted and processed	Number of getBulk requests that have been received and processed.
GetResponse-PDU accepted and processed	Number of get responses that have been received and processed.
SetRequest-PDU accepted and processed	Number of set requests that have been received and processed.
Trap PDUs accepted and processed	Number of notifications that have been received and processed.
alternate Response Class PDUs dropped silently	Number of dropped response packets.
forwarded Confirmed Class PDUs dropped silently	Number of forwarded packets that have been dropped.

4.1.6. display snmp-agent sys-info

Use **display snmp-agent sys-info** to display SNMP agent system information.

Syntax

display snmp-agent sys-info [**contact** | **location** | **version**] *

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

contact: Displays the system contact.

location: Displays the physical location of the device.

version: Displays the SNMP agent version.

Usage guidelines

If you do not specify any keywords, this command displays all SNMP agent system information.

Examples

Display all SNMP agent system information.

```
<Switch> display snmp-agent sys-info
   The contact information of the agent:
       The contact is not configured.

   The location information of the agent:
       The contact is not configured.

   The SNMP version of the agent:
       SNMPv3
```

Related commands

snmp-agent sys-info

4.1.7. display snmp-agent trap queue

Use **display snmp-agent trap queue** to display basic information about the trap queue.

Syntax

display snmp-agent trap queue

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display the trap queue configuration and usage status.

```
<Switch> display snmp-agent trap queue
   Queue size: 100
   Message number: 6
```

Related commands

snmp-agent trap life

snmp-agent trap queue-size

4.1.8. display snmp-agent trap-list

Use **display snmp-agent trap-list** to display SNMP notifications enabling status for modules.

Syntax

display snmp-agent trap-list

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

If a module has multiple sub-modules and SNMP notifications are enabled for one of its sub-modules, the command output shows that the module is SNMP notifications-enabled.

To determine whether a module supports SNMP notifications, execute the **snmp-agent trap enable ?** command.

The **display snmp-agent trap-list** command output varies by the **snmp-agent trap enable** command configuration and the module configuration.

Examples

Display SNMP notifications enabling status for modules.

```
<Switch> display snmp-agent trap-list
arp notification is disabled.
   bfd notification is enabled.
   bgp notification is enabled.
   configuration notification is enabled.
   isis notification is enabled.
   l3vpn notification is enabled.
   mac-address notification is enabled.
   ospf notification is enabled.
   radius notification is disabled.
   standard notification is enabled.
   stp notification is disabled.
   syslog notification is disabled.
   system notification is enabled.
```

```
Enabled notifications: 9; Disabled notifications: 4
```

Related commands

snmp-agent trap enable

4.1.9. display snmp-agent usm-user

Use **display snmp-agent usm-user** to display SNMPv3 user information.

Syntax

display snmp-agent usm-user [**engineid** *engineid* | **group** *group-name* | **username** *user-name*] *

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

engineid *engineid*: Specifies an SNMP engine ID. The engine ID is case insensitive. When a SNMPv3 user is created, the system records the local SNMP entity engine ID. The user becomes invalid when the engine ID changes, and it becomes valid again when the recorded engine ID is restored.

group *group-name*: Specifies an SNMP group by its name. The group name is case sensitive.

username *user-name*: Specifies a SNMPv3 user by its name. The username is case sensitive.

Usage guidelines

This command displays only SNMPv3 users that you have created by using the **snmp-agent usm-user v3** command. To display SNMPv1 or SNMPv2c users created by using the **snmp-agent usm-user** { **v1** | **v2c** } command, use the **display snmp-agent community** command.

Examples

Display information about all SNMPv3 users.

```
<Switch> display snmp-agent usm-user
   Username: userv3
   Group name: mygroupv3
       Engine ID: 800063A203000FE240A1A6
       Storage-type: nonVolatile
       UserStatus: active
       ACL: 2000

   Username: userv3
   Group name: mygroupv3
       Engine ID: 8000259503000BB3100A508
       Storage-type: nonVolatile
       UserStatus: active
       ACL name: testacl
```

```
Username: userv3code
Role name: groupv3code
           network-operator
    Engine ID: 800063A203000FE240A1A6
    Storage-type: nonVolatile
    UserStatus: active

Username: userv3code
Role name: snmprole
           network-operator
    Engine ID: 800063A280000002BB0001
    Storage-type: nonVolatile
    UserStatus: active
```

Table 4-5 Command output

Field	Description
Username	SNMP username.
Group name	SNMP group name.
Role name	SNMP user role name.
Engine ID	Engine ID that the SNMP agent used when the SNMP user was created.
Storage-type	Storage type: • **volatile**. • **nonvolatile**. • **permanent**. • **readOnly**. • **other**. For more information about these storage types, see Table 4-1 .
UserStatus	SNMP user status: • **active**—The SNMP user is effective. • **notInService**—The SNMP user is correctly configured but not activated. • **notReady**—The SNMP user configuration is incomplete. • **other**—Any other status.
ACL	Number of the ACL. This field appears only when an ACL is specified for the SNMPv3 user. It is exclusive with the **ACL name** field.
ACL name	Name of the ACL. This field appears only when an ACL is specified for the SNMPv3 user. It is exclusive with the **ACL** field.

Related commands

snmp-agent usm-user v3

4.1.10. enable snmp trap updown

Use **enable snmp trap updown** to enable link state notifications on an interface.

Use **undo enable snmp trap updown** to disable link state notifications on an interface.

Syntax

enable snmp trap updown

undo enable snmp trap updown

Default

Link state notifications are enabled.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

For an interface to generate linkUp/linkDown notifications when its state changes, you must also enable the linkUp/linkDown notification function globally by using the **snmp-agent trap enable standard** [**linkdown** | **linkup**] * command.

Examples

Enable GigabitEthernet 1/0/1 to send linkUp/linkDown SNMP traps to 10.1.1.1 in the community **public**.

```
<Switch> system-view
[Switch] snmp-agent trap enable
[Switch] snmp-agent target-host trap address udp-domain 10.1.1.1 params securityname
public
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] enable snmp trap updown
```

Related commands

snmp-agent target-host

snmp-agent trap enable

4.1.11. snmp-agent

Use **snmp-agent** to enable the SNMP agent.

Use **undo snmp-agent** to disable the SNMP agent.

Syntax

snmp-agent

undo snmp-agent

Default

The SNMP agent is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

The SNMP agent is automatically enabled when you execute any command that begins with **snmp-agent** except for the **snmp-agent calculate-password** command.

Examples

Enable the SNMP agent.

```
<Switch> system-view
[Switch] snmp-agent
```

4.1.12. snmp-agent { inform | trap } source

Use **snmp-agent** { **inform** | **trap** } **source** to specify a source IP address for the informs or traps sent by the SNMP agent.

Use **undo snmp-agent** { **inform** | **trap** } **source** to restore the default.

Syntax

snmp-agent { **inform** | **trap** } **source** *interface-type interface-number*

undo snmp-agent { **inform** | **trap** } **source**

Default

The SNMP agent uses the IP address of the outgoing interface as the source IP address of notifications.

Views

System view

Predefined user roles

network-admin

Parameters

inform: Specifies informs.

trap: Specifies traps.

interface-type interface-number: Specifies an interface by its type and number.

Usage guidelines

The **snmp-agent source** command enables the SNMP agent to use the primary IP address of an interface as the source IP address in all its SNMP informs or traps, regardless of their outgoing interfaces. An NMS can use this IP address to filter all the informs or traps sent by the SNMP agent.

Make sure the specified interface has been created and assigned a valid IP address. The configuration will fail if the interface has not been created and will take effect only after a valid IP address is assigned to the specified interface.

Examples

Configure the primary IP address of GigabitEthernet 1/0/1 as the source address of SNMP traps.

```
<Switch> system-view
[Switch] snmp-agent trap source gigabitethernet 1/0/1
```

Configure the primary IP address of GigabitEthernet 1/0/2 as the source address of SNMP informs.

```
<Switch> system-view
```

```
[Switch] snmp-agent inform source gigabitethernet 1/0/2
```

Related commands

snmp-agent target-host

snmp-agent trap enable

4.1.13. snmp-agent calculate-password

Use **snmp-agent calculate-password** to calculate the encrypted form for a key in plaintext form.

Syntax

snmp-agent calculate-password *plain-password* **mode** { **3desmd5** | **3dessha** | **md5** | **sha** } { **local-engineid** | **specified-engineid** *engineid* }

Views

System view

Predefined user roles

network-admin

Parameters

plain-password: Specifies a key in plaintext form. The *plain-password* argument is a case-sensitive string of 1 to 64 characters.

mode: Specifies an authentication algorithm and encryption algorithm. The device supports the HMAC-MD5 and HMAC-SHA1 authentication algorithms. The HMAC-MD5 algorithm is faster than the HMAC-SHA1 algorithm. The HMAC-SHA1 algorithm provides more security than the HMAC-MD5 algorithm. The 3DES, and DES encryption algorithms (in descending order of security strength) are available for the device. A more secure algorithm calculates slower. DES is enough to meet general security requirements.

- **3desmd5**: Calculates the encrypted form for the encryption key by using the 3DES encryption algorithm and HMAC-MD5 authentication algorithm.
- **3dessha**: Calculates the encrypted form for the encryption key by using the 3DES encryption algorithm and HMAC-SHA1 authentication algorithm.
- **md5**: Calculates the encrypted form for the authentication key or encryption key by using the HMAC-MD5 authentication algorithm and AES or DES encryption algorithm. When the HMAC-MD5 authentication algorithm is used, you can get the same authentication key or encryption key in encrypted form regardless of whether the AES or DES encryption algorithm is used.
- **sha**: Calculates the encrypted form for the authentication key or encryption key by using HMAC-SHA1 authentication algorithm and AES or DES encryption algorithm. When the HMAC-SHA1 authentication algorithm is used, you can get the same authentication key or encryption key in encrypted form regardless of whether the AES or DES encryption algorithm is used.

local-engineid: Uses the local engine ID to calculate the encrypted form for the key. You can configure the local engine ID by using the **snmp-agent local-engineid** command.

specified-engineid *engineid*: Uses a user-defined engine ID to calculate the encrypted form for the key. The *engineid* argument is an even number of case-insensitive hexadecimal characters. All-zero and all-F strings are invalid. The even number is in the range of 10 to 64.

Usage guidelines

Make sure the SNMP agent is enabled before you execute the **snmp-agent calculate-password** command.

For security purposes, use the encrypted-form key generated by using this command when you create SNMPv3 users by specifying the **cipher** keyword in the **snmp-agent usm-user v3** command.

The encrypted form of the key is valid only under the engine ID specified for key conversion.

Examples

Use the local engine ID and the HMAC-SHA1 algorithm to calculate the encrypted form for key **authkey**.

```
<Switch> system-view
[Switch] snmp-agent calculate-password authkey mode sha local-engineid
The encrypted key is: 09659EC5A9AE91BA189E5845E1DDE0CC
```

Related commands

snmp-agent local-engineid

snmp-agent usm-user v3

4.1.14. snmp-agent community

Use **snmp-agent community** to configure a SNMPv1 or SNMPv2c community.

Use **undo snmp-agent community** to delete a SNMPv1 or SNMPv2c community.

Syntax

snmp-agent community { **read** | **write** } [**simple** | **cipher**] *community-name* [**mib-view** *view-name*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] *

undo snmp-agent community [**cipher**] *community-name*

Default

No SNMPv1 or SNMPv2c communities exist.

Views

System view

Predefined user roles

network-admin

Parameters

read: Assigns the specified community read-only access to MIB objects. A read-only community can only inquire MIB information.

write: Assigns the specified community read and write access to MIB objects. A read and write community can configure MIB information.

simple: Specifies a community name in plaintext form. For security purposes, the community name specified in plaintext form will be stored in encrypted form.

cipher: Specifies a community name in encrypted form.

community-name: Specifies the community name. The plaintext form is a case-sensitive string of 1 to 32 characters. The encrypted form is a case-sensitive string of 33 to 73 characters. Input a string as escape characters after a backslash (\).

mib-view *view-name*: Specifies the MIB view available for the community. The *view-name* argument represents a MIB view name, a case-sensitive string of 1 to 32 characters. A MIB view represents a set of accessible MIB objects. If you do not specify a view, the specified community can access the MIB objects in the default MIB view **ViewDefault**.

user-role *role-name*: Specifies a user role name for the community, a case-sensitive string of 1 to 63 characters.

acl: Specifies a basic or advanced IPv4 ACL for the community.

ipv4-acl-number: Specifies a basic or advanced IPv4 ACL by its number. The basic IPv4 ACL number is in the range of 2000 to 2999. The advanced IPv4 ACL number is in the range of 3000 to 3999.

name *ipv4-acl-name*: Specifies a basic or advanced IPv4 ACL by its name, a case-insensitive string of 1 to 63 characters.

acl ipv6: Specifies a basic or advanced IPv6 ACL for the community.

ipv6-acl-number: Specifies a basic or advanced IPv6 ACL by its number. The basic IPv6 ACL number is in the range of 2000 to 2999. The advanced IPv6 ACL number is in the range of 3000 to 3999.

name *ipv6-acl-name*: Specifies a basic or advanced IPv6 ACL by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

Only users with the network-admin or level-15 user role can execute this command. Users with other user roles cannot execute this command even if these roles are granted access to commands of the SNMP feature or this command.

An SNMP community is identified by a community name. It contains a set of NMSs and SNMP agents. Devices in an SNMP community authenticate each other by using the community name. An NMS and an SNMP agent can communicate only when they use the same community name.

Typically, **public** is used as the read-only community name and **private** is used as the read and write community name. To enhance security, you can assign your SNMP communities a name other than **public** and **private**.

The **snmp-agent community** command allows you to use either of the following modes to control SNMP community access to MIB objects:

- **View-based access control model**—The VACM mode controls access to MIB objects by assigning MIB views to SNMP communities.

You can create a maximum of 10 SNMP communities by using the **snmp-agent community** command.

If you execute the command multiple times to specify the same community name but different other settings each time, the most recent configuration takes effect.

To set and save a community name in plain text, do not specify the **simple** or **cipher** keyword.

The ACL is used to filter illegitimate NMSs.

- If you do not specify an ACL, the specified ACL does not exist, or the specified ACL does not have any rules, all NMSs that use the community name can access the SNMP agent.
- If you specify an ACL and the ACL has rules, only NMSs permitted by the ACL can access the SNMP agent.

For more information about ACL, see *ACL and QoS Configuration Guide*.

You can also create an SNMP community by using the **snmp-agent usm-user** { **v1** | **v2c** } and **snmp-agent group** { **v1** | **v2c** } commands. These two commands create a SNMPv1 or SNMPv2c user and the group to which the user is assigned. The system automatically creates an SNMP community by using the SNMPv1 or SNMPv2c username.

Examples

Create the read-only community with the plaintext form name **readaccess** so a SNMPv1 or SNMPv2c NMS can use the community name **readaccess** to read the MIB objects in the default view **ViewDefault**.

```
<Switch> system-view
[Switch] snmp-agent sys-info version v1 v2c
[Switch] snmp-agent community read simple readaccess
```

Create the read and write community with the plaintext form name **writeaccess** so only the SNMPv2c NMS at 1.1.1.1 can use the community name **writeaccess** to read or set the MIB objects in the default view **ViewDefault**.

```
<Switch> system-view
[Switch] acl basic 2001
[Switch-acl-ipv4-basic-2001] rule permit source 1.1.1.1 0.0.0.0
[Switch-acl-ipv4-basic-2001] rule deny source any
[Switch-acl-ipv4-basic-2001] quit
[Switch] snmp-agent sys-info version v2c
[Switch] snmp-agent community write simple writeaccess acl 2001
```

Create the read and write community with the plaintext form name **writeaccess** so only the SNMPv2c NMS at 1.1.1.2 can use the community name **writeaccess** to read or set the MIB objects in the default view **ViewDefault**.

```
<Switch> system-view
[Switch] acl basic name testacl
[Switch-acl-ipv4-basic-testacl] rule permit source 1.1.1.2 0.0.0.0
[Switch-acl-ipv4-basic-testacl] rule deny source any
[Switch-acl-ipv4-basic-testacl] quit
[Switch] snmp-agent sys-info version v2c
[Switch] snmp-agent community write simple writeaccess acl name testacl
```

Create the read and write community with the plaintext form name **wr-sys-acc** so a SNMPv1 or SNMPv2c NMS can use the community name **wr-sys-acc** to read or set the MIB objects in the system subtree (OID 1.3.6.1.2.1.1).

```
<Switch> system-view
[Switch] snmp-agent sys-info version v1 v2c
[Switch] undo snmp-agent mib-view ViewDefault
[Switch] snmp-agent mib-view included test system
[Switch] snmp-agent community write simple wr-sys-acc mib-view test
```

Related commands

display snmp-agent community

snmp-agent mib-view

4.1.15. snmp-agent group

Use **snmp-agent group** to create an SNMP group.

Use **undo snmp-agent group** to delete an SNMP group.

Syntax

SNMPv1 and SNMP v2c:

snmp-agent group { **v1** | **v2c** } *group-name* [**read-view** *view-name*] [**write-view** *view-name*] [**notify-view** *view-name*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] *

undo snmp-agent group { **v1** | **v2c** } *group-name*

SNMPv3:

snmp-agent group v3 *group-name* [**authentication** | **privacy**] [**read-view** *read-view*] [**write-view** *write-view*] [**notify-view** *notify-view*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] *

undo snmp-agent group v3 *group-name* [**authentication** | **privacy**]

Default

No SNMP groups exist.

Views

System view

Predefined use roles

network-admin

Parameters

v1: Specifies SNMPv1.

v2c: Specifies SNMPv2c.

v3: Specifies SNMPv3.

group-name: Specifies an SNMP group name, a case-sensitive string of 1 to 32 characters.

authentication: Specifies the authentication without privacy security model for the SNMPv3 group.

privacy: Specifies the authentication with privacy security model for the SNMPv3 group.

read-view *view-name*: Specifies a read-only MIB view. The *view-name* represents a MIB view name, a case-sensitive string of 1 to 32 characters. If you do not specify a read-only MIB view, the SNMP group has read access to the default view **ViewDefault**.

write-view *view-name:* Specifies a read and write MIB view. The *view-name* represents a MIB view name, a case-sensitive string of 1 to 32 characters. If you do not specify a read and write view, the SNMP group cannot set any MIB object on the SNMP agent.

notify-view *view-name*: Specifies a notify MIB view. The *view-name* represents a MIB view name, a case-sensitive string of 1 to 32 characters. The SNMP agent sends notifications to the users in the specified group only for the MIB objects included in the notify view. If you do not specify a notify view, the SNMP agent does not send any notification to the users in the specified group.

acl: Specifies a basic or advanced IPv4 ACL for the group.

ipv4-acl-number: Specifies a basic or advanced IPv4 ACL by its number. The basic IPv4 ACL number is in the range of 2000 to 2999. The advanced IPv4 ACL number is in the range of 3000 to 3999.

name *ipv4-acl-name*: Specifies a basic or advanced IPv4 ACL by its name, a case-insensitive string of 1 to 63 characters.

acl ipv6: Specifies a basic or advanced IPv6 ACL for the group.

ipv6-acl-number: Specifies a basic or advanced IPv6 ACL by its number. The basic IPv6 ACL number is in the range of 2000 to 2999. The advanced IPv6 ACL number is in the range of 3000 to 3999.

name *ipv6-acl-name*: Specifies a basic or advanced IPv6 ACL by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

Only users with the network-admin or level-15 user role can execute this command. Users with other user roles cannot execute this command even if these roles are granted access to commands of the SNMP feature or this command.

All users in an SNMP group share the security model and access rights of the group.

You can create a maximum of 20 SNMP groups, including SNMPv1, SNMPv2c, and SNMPv3 groups.

All SNMPv3 users in a group share the same security model, but can use different authentication and encryption key settings. To implement a security model for a user and avoid SNMP communication failures, make sure the security model configuration for the group and the security key settings for the user are compliant with Table 4-6 and match the settings on the NMS.

Table 4-6 Basic security setting requirements for different security models

Security model	Security model keyword for the group	Security key settings for the user	Remarks
Authentication with privacy	**privacy**	Authentication key, encryption key	If the authentication key or the encryption key is not configured, SNMP communication will fail.
Authentication without privacy	**authentication**	Authentication key	If no authentication key is configured, SNMP communication will fail. The encryption key (if any) for the user does not take effect.
No authentication, no privacy	Neither **authentication** nor **privacy**	None	The authentication and encryption keys, if configured, do not take effect.

You can specify an ACL for the user and group, respectively, to filter illegitimate NMSs. Only the NMSs permitted by the ACLs for both the user and group can access the SNMP agent. The following rules apply to the ACLs for the user and group:

- If you do not specify an ACL, the specified ACL does not exist, or the specified ACL does not have any rules, all NMSs that use the username can access the SNMP agent.
- If you have specified an ACL and the ACL has rules, only the NMSs permitted by the ACL can access the agent.

For more information about ACL, see *ACL and QoS Configuration Guide*.

Examples

Create the SNMPv3 group **group1**.

```
<Switch> system-view
[Switch] snmp-agent group v3 group1
```

Related commands

display snmp-agent group

snmp-agent mib-view

snmp-agent usm-user

4.1.16. snmp-agent local-engineid

Use **snmp-agent local-engineid** to set an SNMP engine ID.

Use **undo snmp-agent local-engineid** to restore the default.

Syntax

snmp-agent local-engineid *engineid*

undo snmp-agent local-engineid

Default

The engine ID of a device is the combination of the company ID and the device ID. Each device has a unique device ID.

Views

System view

Predefined user roles

network-admin

Parameters

engineid: Specifies an SNMP engine ID, a case-insensitive hexadecimal string. Its length is an even number in the range of 10 to 64. All-zero and all-F strings are invalid.

Usage guidelines

An SNMP engine ID uniquely identifies a device in an SNMP managed network. Make sure the local SNMP engine ID is unique within your SNMP managed network to avoid communication problems.

If you have configured SNMPv3 users, change the local SNMP engine ID only when necessary. The change can void the SNMPv3 usernames and encrypted keys you have configured.

You can use the default engine ID or configure an easy-to-remember engine ID based on the network plan. For example, you can set the engine ID for device 1 on the first floor of building A to 000Af0010001 and device 2 to 000Af0010002.

Examples

Set the local SNMP engine ID to **123456789A**.

```
<Switch> system-view
[Switch] snmp-agent local-engineid 123456789A
```

Related commands

display snmp-agent local-engineid

snmp-agent usm-user

4.1.17. snmp-agent log

Use **snmp-agent log** to enable SNMP logging.

Use **undo snmp-agent log** to disable SNMP logging.

Syntax

snmp-agent log { **all** | **authfail** | **get-operation** | **set-operation** }

undo snmp-agent log { **all** | **authfail** | **get-operation** | **set-operation** }

Default

SNMP logging operations are disabled.

Views

System view

Predefined user roles

network-admin

Parameters

all: Enables logging SNMP authentication failures, Get operations, and Set operations.

authfail: Enables logging SNMP authentication failures.

get-operation: Enables logging SNMP Get operations.

set-operation: Enables logging SNMP Set operations.

Usage guidelines

Use SNMP logging to record the SNMP operations performed on the SNMP agent or authentication failures from the NMS to the agent for auditing NMS behaviors. The SNMP agent sends log data to the information center. You can configure the information center to output the data to a destination as needed.

Examples

Enable logging SNMP Get operations.

```
<Switch> system-view
[Switch] snmp-agent log get-operation
```

Enable logging SNMP Set operations.

```
<Switch> system-view
[Switch] snmp-agent log set-operation
```

Enable logging SNMP authentication failures.

```
<Switch> system-view
[Switch] snmp-agent log authfail
```

4.1.18. snmp-agent mib-view

Use **snmp-agent mib-view** to create or update a MIB view.

Use **undo snmp-agent mib-view** to delete a MIB view.

Syntax

snmp-agent mib-view { **excluded** | **included** } *view-name oid-tree* [**mask** *mask-value*]

undo snmp-agent mib-view *view-name*

Default

The system creates the **ViewDefault** view when the SNMP agent is enabled. In this default MIB view, all MIB objects in the **iso** subtree but the **snmpUsmMIB**, **snmpVacmMIB**, and **snmpModules.18** subtrees are accessible.

Views

System view

Predefined user roles

network-admin

Parameters

excluded: Denies access to any node in the specified MIB subtree.

included: Permits access to all the nodes in the specified MIB subtree.

view-name: Specifies a view name, a case-sensitive string of 1 to 32 characters.

oid-tree: Specifies a MIB subtree by its root node's OID (for example, **1.3.6.1.2.1.1**) or object name (for example, **system**). The *oid-tree* argument is a case-sensitive string of 1 to 255 characters. An OID is a dotted numeric string that uniquely identifies an object in the MIB tree.

mask *mask-value*: Sets a MIB subtree mask, a case-insensitive hexadecimal string. Its length is an even number in the range of 1 to 32.

Usage guidelines

A MIB view represents a set of MIB objects (or MIB object hierarchies) with certain access privilege. The MIB objects included in the MIB view are accessible while those excluded from the MIB view are inaccessible.

Each *view-name oid-tree* pair represents a view record. If you specify the same record with different MIB subtree masks multiple times, the most recent configuration takes effect.

Be cautious with deleting the default MIB view. The operation blocks the access to any MIB object on the device from NMSs that use the default view.

Examples

Include the **mib-2** (OID 1.3.6.1.2.1) subtree in the **mibtest** view and exclude the **system** subtree from this view.

```
<Switch> system-view
[Switch] snmp-agent sys-info version v1
[Switch] snmp-agent mib-view included mibtest 1.3.6.1.2.1
[Switch] snmp-agent mib-view excluded mibtest system
[Switch] snmp-agent community read public mib-view mibtest
```

A SNMPv1 NMS in the **public** community can query the objects in the **mib-2** subtree but not any object (for example, the **sysDescr or sysObjectID** node) in the **system** subtree.

Related commands

display snmp-agent mib-view

snmp-agent group

4.1.19. snmp-agent packet max-size

Use **snmp-agent packet max-size** to set the maximum size (in bytes) of SNMP packets that the SNMP agent can receive or send.

Use **undo snmp-agent packet max-size** to restore the default.

Syntax

snmp-agent packet max-size *byte-count*

undo snmp-agent packet max-size

Default

An SNMP agent can process SNMP packets with a maximum size of 1500 bytes.

Views

System view

Predefined user roles

network-admin

Parameters

byte-count: Sets the maximum size (in bytes) of SNMP packets that the SNMP agent can receive or send. The value range is 484 to 17940.

Usage guidelines

If any device on the path to the NMS does not support packet fragmentation, limit the SNMP packet size to prevent large-sized packets from being discarded. For most networks, the default value is sufficient.

Examples

Set the maximum SNMP packet size to 1024 bytes.

```
<Switch> system-view
[Switch] snmp-agent packet max-size 1024
```

4.1.20. snmp-agent packet response dscp

Use **snmp-agent packet response dscp** to set the DSCP value for SNMP responses.

Use **undo snmp-agent packet response dscp** to restore the default.

Syntax

snmp-agent packet response dscp *dscp-value*

undo snmp-agent packet response dscp

Default

The DSCP value for SNMP responses is 0.

Views

System view

Predefined user roles

network-admin

Parameters

dscp-value: Sets the DSCP value for SNMP responses, in the range of 0 to 63. A greater DSCP value represents a higher priority.

Usage guidelines

The DSCP value is encapsulated in the ToS field of an IP packet. It specifies the priority level of the packet and affects the transmission priority of the packet.

Examples

Set the DSCP value to 40 for SNMP responses.

```
<Switch> system-view
[Switch] snmp-agent packet response dscp 40
```

4.1.21. snmp-agent sys-info contact

Use **snmp-agent sys-info contact** to configure the system contact.

Use **undo snmp-agent sys-info contact** to restore the default contact.

Syntax

snmp-agent sys-info contact *sys-contact*

undo snmp-agent sys-info contact

Default

The contact is not configured.

Views

System view

Predefined user roles

network-admin

Parameters

sys-contact: Specifies the system contact, a case-sensitive string of 1 to 255 characters.

Usage guidelines

Configure the system contact for system maintenance and management.

Examples

Configure the system contact as **Dial System Operator # 27345**.

```
<Switch> system-view
[Switch] snmp-agent sys-info contact Dial System Operator # 27345
```

Related commands

display snmp-agent sys-info

4.1.22. snmp-agent sys-info location

Use **snmp-agent sys-info location** to configure the system location.

Use **undo snmp-agent sys-info location** to restore the default location.

Syntax

snmp-agent sys-info location *sys-location*

undo snmp-agent sys-info location

Default

The system location is not configured.

Views

System view

Predefined user roles

network-admin

Parameters

sys-location: Specifies the system location, a case-sensitive string of 1 to 255 characters.

Usage guidelines

Configure the location of the device for system maintenance and management.

Examples

Configure the system location as **Room524-row1-3**.

```
<Switch> system-view
[Switch] snmp-agent sys-info location Room524-row1-3
```

Related commands

display snmp-agent sys-info

4.1.23. snmp-agent sys-info version

Use **snmp-agent sys-info version** to enable SNMP versions.

Use **undo snmp-agent sys-info version** to disable SNMP versions.

Syntax

snmp-agent sys-info contact version { **all** | { **v1** | **v2c** | **v3** } * }

undo snmp-agent sys-info version { **all** | { **v1** | **v2c** | **v3** } * }

Default

SNMPv3 is enabled.

Views

System view

Predefined user roles

network-admin

Parameters

all: Specifies SNMPv1, SNMPv2c, and SNMPv3.

v1: Specifies SNMPv1.

v2c: Specifies SNMPv2c.

v3: Specifies SNMPv3.

Usage guidelines

Configure the SNMP agent with the same SNMP version as the NMS for successful communications between them.

Examples

Enable SNMPv3.

```
<Switch> system-view
[Switch] snmp-agent sys-info version v3
```

Related commands

display snmp-agent sys-info

4.1.24. snmp-agent target-host

Use **snmp-agent target-host** to configure an SNMP notification target host.

Use **undo snmp-agent target-host** to remove an SNMP notification target host.

Syntax

snmp-agent target-host inform address udp-domain { *ipv4-address* | **ipv6** *ipv6-address* } [**udp-port** *port-number*] [**vpn-instance** *vpn-instance-name*] **params securityname** *security-string* { **v2c** | **v3** [**authentication** | **privacy**] }

snmp-agent target-host trap address udp-domain { *ipv4-address* | **ipv6** *ipv6-address* } [**udp-port** *port-number*] [**dscp** *dscp-value*] [**vpn-instance** *vpn-instance-name*] **params securityname** *security-string* [**v1** | **v2c** | **v3** [**authentication** | **privacy**]]

undo snmp-agent target-host { **trap** | **inform** } **address udp-domain** { *ipv4-address* | **ipv6** *ipv6-address* } **params securityname** *security-string* [**vpn-instance** *vpn-instance-name*]

Default

No SNMP notification target hosts exist.

Views

System view

Predefined user roles

network-admin

Parameters

inform: Specifies a host that receives informs.

trap: Specifies a host that receives traps.

address: Specifies the destination address of SNMP notifications.

udp-domain: Specifies UDP as the transport protocol.

ipv4-address: Specifies a target host by its IPv4 address or host name. The host name is a case-insensitive string of 1 to 253 characters. The string can only contain letters, numbers, hyphens (-), underscores (_), and dots (.). If you specify a host name, the IPv4 address of the target host can be obtained.

ipv6 *ipv6-address*: Specifies a target host by its IPv6 address or host name. The host name is a case-insensitive string of 1 to 253 characters, which only contains letters, numbers, hyphens (-),

underscores (_), and dots (.). If you specify a host name, the IPv6 address of the target host can be obtained. If you specify an IPv6 address, the address cannot be a link local address.

udp-port *port-number*: Specifies the UDP port for SNMP notifications. The default port number is 162.

dscp-value: Sets the DSCP value for traps sent to the target host, in the range of 0 to 63. The DSCP value is encapsulated in the ToS field of an IP packet. It specifies the priority level of the packet and affects the transmission priority of the packet. A greater DSCP value represents a higher priority. The default DSCP value for traps is 0.

vpn-instance *vpn-instance-name*: Specifies the VPN instance to which the target host belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. If the target host belongs to the public network, do not specify this option.

params securityname *security-string*: Specifies the authentication parameter. The *security-string* argument specifies a SNMPv1 or SNMPv2c community name or a SNMPv3 username, a case-sensitive string of 1 to 32 characters.

v1: Specifies SNMPv1.

v2c: Specifies SNMPv2c.

v3: Specifies SNMPv3.

- **authentication**: Specifies the security model to be authentication without privacy. You must specify the authentication key when you create the SNMPv3 user.
- **privacy**: Specifies the security model to be authentication with privacy. You must specify the authentication key and encryption key when you create the SNMPv3 user.

Usage guidelines

You can specify multiple SNMP notification target hosts.

Make sure the SNMP agent uses the same UDP port for SNMP notifications as the target host. Typically, NMSs, for example, MIB Browser, use port 162 for SNMP notifications as defined in the SNMP protocols.

If none of the keywords **v1**, **v2c**, or **v3** is specified, SNMPv1 is used. Make sure the SNMP agent uses the same SNMP version as the target host so the host can receive the notification.

If neither **authentication** nor **privacy** is specified, the security model is no authentication, no privacy.

Examples

Configure the SNMP agent to send SNMPv3 traps to 10.1.1.1 by using the username **public**.

```
<Switch> system-view
[Switch] snmp-agent trap enable standard
[Switch] snmp-agent target-host trap address udp-domain 10.1.1.1 params securityname
public v3
```

Related commands

snmp-agent { **inform** | **trap** } **source**

snmp-agent trap enable

snmp-agent trap life

4.1.25. snmp-agent trap enable

Use **snmp-agent trap enable** to enable SNMP notifications.

Use **undo snmp-agent trap enable** to disable SNMP notifications.

Syntax

snmp-agent trap enable [**configuration** | *protocol* | **standard** [**authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart**] * | **system**]

undo snmp-agent trap enable [**configuration** | *protocol* | **standard** [**authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart**] * | **system**]

Default

SNMP configuration notifications, standard notifications, and system notifications are enabled. Whether other SNMP notifications are enabled varies by module.

Views

System view

Predefined user roles

network-admin

Parameters

configuration: Specifies configuration notifications. If configuration notifications are enabled, the system checks the running configuration and the startup configuration every 10 minutes for any change and generates a notification for the most recent change.

protocol: Specifies protocol module notifications. You can use the **snmp-agent trap enable ?** command to obtain the value of this argument. For more information about this argument, see the command reference for each module.

standard: Specifies SNMP standard notifications.

Table 4-7 Standard SNMP notifications

Keyword	Definition
authentication	Authentication failure notification sent when an NMS fails to be authenticated by the SNMP agent.
coldstart	Notification sent when the device restarts.
linkdown	Notification sent when the link of a port goes down.
linkup	Notification sent when the link of a port comes up.
warmstart	Notification sent when the SNMP agent restarts.

system: Specifies system notifications sent when the system time is modified, the system reboots, or the main system software image is not available.

Usage guidelines

To report critical protocol events to an NMS, enable SNMP notifications for the protocol. For SNMP notifications to be sent correctly, you must also configure the notification sending parameters as required.

If no optional parameters are specified, this command or its **undo** form enables or disables all SNMP notifications supported by the device.

Examples

Enable the SNMP agent to send SNMP authentication failure notifications.

```
<Switch> system-view
[Switch] snmp-agent trap enable standard authentication
```

Related commands

snmp-agent target-host

4.1.26. snmp-agent trap if-mib link extended

Use **snmp-agent trap if-mib link extended** to configure the SNMP agent to send extended linkUp/linkDown notifications.

Use **undo snmp-agent trap if-mib link extended** to restore the default.

Syntax

snmp-agent trap if-mib link extended

undo snmp-agent trap if-mib link extended

Default

The SNMP agent sends standard linkUp/linkDown notifications.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Extended linkUp and linkDown notifications add interface description and interface type to the standard linkUp/linkDown notifications for fast failure point identification.

When you use this command, make sure the NMS supports the extended linkup and linkDown notifications.

Examples

Enable extended linkUp/linkDown notifications.

```
<Switch> system-view
[Switch] snmp-agent trap if-mib link extended
```

4.1.27. snmp-agent trap life

Use **snmp-agent trap life** to set the lifetime of notifications in the SNMP notification queue.

Use **undo snmp-agent trap life** to restore the default notification lifetime.

Syntax

snmp-agent trap life *seconds*

undo snmp-agent trap life

Default

The SNMP notification lifetime is 120 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

seconds: Sets a lifetime in the range of 1 to 2592000, in seconds.

Usage guidelines

When congestion occurs, the SNMP agent buffers notifications in a queue. The notification lifetime sets how long a notification can stay in the queue. A notification is deleted when its lifetime expires.

Examples

Set the SNMP notification lifetime to 60 seconds.

```
<Switch> system-view
[Switch] snmp-agent trap life 60
```

Related commands

snmp-agent target-host

snmp-agent trap enable

snmp-agent trap queue-size

4.1.28. snmp-agent trap log

Use **snmp-agent trap log** to enable SNMP notification logging.

Use **undo snmp-agent trap log** to disable SNMP notification logging.

Syntax

snmp-agent trap log

undo snmp-agent trap log

Default

SNMP notification logging is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Use SNMP notification logging to record SNMP notifications sent by the SNMP agent for notification tracking. The SNMP agent sends the logs to the information center. You can configure the information center to output the logs to a destination as needed.

Examples

Enable SNMP notification logging.

```
<Switch> system-view
[Switch] snmp-agent trap log
```

4.1.29. snmp-agent trap periodical-interval

Use **snmp-agent trap periodical-interval** to enable SNMP alive traps and set the sending interval.

Use **undo snmp-agent trap periodical-interval** to set 60 seconds.

Syntax

snmp-agent trap periodical-interval *interval*

undo snmp-agent trap periodical-interval

Default

SNMP notification logging is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies an interval for sending SNMP alive traps. The value is 0 or is in the range of 10 to 3600, in seconds. Setting this argument to 0 disables SNMP alive traps.

Usage guidelines

This command enables the device to send SNMP alive traps to the NMS at the specified intervals to inform the NMS that SNMP is operating correctly on the device.

Using **undo snmp-agent trap periodical-interval** cannot restore the default. You must use the **snmp-agent trap periodical-interval 0** command to reconfigure the sending interval.

Examples

Enable SNMP alive traps and set the sending interval to 10 seconds.

```
<Switch> system-view
[Switch] snmp-agent trap periodical-interval 10
```

Disable SNMP alive traps.

```
<Switch> system-view
[Switch] snmp-agent trap periodical-interval 0
```

Related commands

snmp-agent target-host

snmp-agent trap enable

4.1.30. snmp-agent trap queue-size

Use **snmp-agent trap queue-size** to set the SNMP notification queue size.

Use **undo snmp-agent trap queue-size** to restore the default queue size.

Syntax

snmp-agent trap queue-size *size*

undo snmp-agent trap queue-size

Default

The SNMP notification queue can store a maximum of 100 notifications.

Views

System view

Predefined user roles

network-admin

Parameters

size: Specifies the maximum number of notifications that the SNMP notification queue can hold. The value range is 1 to 1000.

Usage guidelines

When congestion occurs, the SNMP agent buffers notifications in a queue. SNMP notification queue size sets the maximum number of notifications that this queue can hold. When the queue size is reached, the oldest notifications are dropped for new notifications.

Examples

Set the SNMP notification queue size to 200.

```
<Switch> system-view
[Switch] snmp-agent trap queue-size 200
```

Related commands

snmp-agent target-host

snmp-agent trap enable

snmp-agent trap life

4.1.31. snmp-agent usm-user { v1 | v2c }

Use **snmp-agent usm-user** { **v1** | **v2c** } to create a SNMPv1 or SNMPv2c user.

Use **undo snmp-agent usm-user** { **v1** | **v2c** } to delete a SNMPv1 or SNMPv2c user.

Syntax

snmp-agent usm-user { **v1** | **v2c** } *user-name group-name* [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] *

undo snmp-agent usm-user { **v1** | **v2c** } *user-name*

Default

No SNMPv1 or SNMPv2c users exist.

Views

System view

Predefined user roles

network-admin

Parameters

v1: Specifies SNMPv1.

v2c: Specifies SNMPv2c.

user-name: Specifies a SNMP username, a case-sensitive string of 1 to 32 characters.

group-name: Specifies a SNMPv1 or SNMPv2c group name, a case-sensitive string of 1 to 32 characters. The group can be one that has been created or not. The user takes effect only after you create the group.

acl: Specifies a basic or advanced IPv4 ACL for the user.

ipv4-acl-number: Specifies a basic or advanced IPv4 ACL by its number. The basic IPv4 ACL number is in the range of 2000 to 2999. The advanced IPv4 ACL number is in the range of 3000 to 3999.

name *ipv4-acl-name*: Specifies a basic or advanced IPv4 ACL by its name, a case-insensitive string of 1 to 63 characters.

acl ipv6: Specifies a basic or advanced IPv6 ACL for the user.

ipv6-acl-number: Specifies a basic or advanced IPv6 ACL by its number. The basic IPv6 ACL number is in the range of 2000 to 2999. The advanced IPv6 ACL number is in the range of 3000 to 3999.

name *ipv6-acl-name*: Specifies a basic or advanced IPv6 ACL by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

Only users with the network-admin or level-15 user role can execute this command. Users with other user roles cannot execute this command even if these roles are granted access to commands of the SNMP feature or this command.

On a SNMPv1 or SNMPv2c network, NMSs and agents authenticate each other by using the community name. On a SNMPv3 network, NMSs and agents authenticate each other by using the username.

You can create a SNMPv1 or SNMPv2c community by using either of the following ways:

- Execute the **snmp-agent community** command.
- Execute the **snmp-agent usm-user** { **v1** | **v2c** } and **snmp-agent group** { **v1** | **v2c** } commands to create a SNMPv1 or SNMPv2c user and the group that the user is assigned to. The system automatically creates an SNMP community by using the SNMPv1 or SNMPv2c username.

You can specify an ACL for the user and group, respectively, to filter illegitimate NMSs. Only the NMSs permitted by the ACLs for both the user and group can access the SNMP agent. The following rules apply to the ACLs for the user and group:

- If you do not specify an ACL, the specified ACL does not exist, or the specified ACL does not have any rules, all NMSs that use the username can access the SNMP agent.
- If you have specified an ACL and the ACL has rules, only the NMSs permitted by the ACL can access the agent.

For more information about ACL, see *ACL and QoS Configuration Guide*.

Examples

Add the user **userv2c** to the SNMPv2c group **readCom** so an NMS can use the protocol SNMPv2c and the read-only community name **userv2c** to access the device.

```
<Switch> system-view
[Switch] snmp-agent sys-info version v2c
[Switch] snmp-agent group v2c readCom
[Switch] snmp-agent usm-user v2c userv2c readCom
```

Add the user **userv2c** in the SNMPv2c group **readCom** so only the NMS at 1.1.1.1 can use the protocol SNMPv2c and read-only community name **userv2c** to access the device.

```
<Switch> system-view
```

```
[Switch] acl basic 2001
[Switch-acl-ipv4-basic-2001] rule permit source 1.1.1.1 0.0.0.0
[Switch-acl-ipv4-basic-2001] rule deny source any
[Switch-acl-ipv4-basic-2001] quit
[Switch] snmp-agent sys-info version v2c
[Switch] snmp-agent group v2c readCom
[Switch] snmp-agent usm-user v2c userv2c readCom acl 2001
```

Add the user **userv2c** in the SNMPv2c group **readCom** so only the NMS at 1.1.1.2 can use the protocol SNMPv2c and read-only community name **userv2c** to access the device.

```
[Switch] acl basic name testacl
[Switch-acl-ipv4-basic-testacl] rule permit source 1.1.1.2 0.0.0.0
[Switch-acl-ipv4-basic-testacl] rule deny source any
[Switch-acl-ipv4-basic-testacl] quit
[Switch] snmp-agent sys-info version v2c
[Switch] snmp-agent group v2c readCom
[Switch] snmp-agent usm-user v2c userv2c readCom acl name testacl
```

Related commands

display snmp-agent community

snmp-agent community

snmp-agent group

4.1.32. snmp-agent usm-user v3

Use **snmp-agent usm-user v3** to create a SNMPv3 user.

Use **undo snmp-agent usm-user v3** to delete a SNMPv3 user.

Syntax

snmp-agent usm-user v3 *user-name group-name* [{ **cipher** | **simple** } **authentication-mode** { **md5** | **sha** } *auth-password* [**privacy-mode** { **3des** | **aes128** | **des56** } *priv-password*]] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] *

undo snmp-agent usm-user v3 *user-name* { **local** | **engineid** *engineid-string* }

Default

No SNMPv3 users exist.

Views

System view

Predefined user roles

network-admin

Parameters

user-name: Specifies a SNMPv3 username, a case-sensitive string of 1 to 32 characters.

group-name: Specifies a SNMPv3 group name, a case-sensitive string of 1 to 32 characters. The group can be one that has been created or not. The user takes effect only after you create the group.

cipher: Specifies an authentication key and an encryption key in encrypted form. The keys will be converted to a digest in encrypted form and stored in the device.

simple: Specifies an authentication key and an encryption key in plaintext from. The keys will be converted to a digest in encrypted form and stored in the device.

authentication-mode: Specifies an authentication algorithm. If you do not specify the keyword, the system does not perform authentication.

- **md5**: Specifies the HMAC-MD5 authentication algorithm.
- **sha**: Specifies the HMAC-SHA1 authentication algorithm.

auth-password: Specifies an authentication key. This argument is case sensitive.

- The plaintext form of the key is a string of 1 to 64 characters, which must contain numbers, uppercase letters, lowercase letters, and special characters.
- The encrypted form of the key can be calculated by using the **snmp-agent calculate-password** command.

privacy-mode: Specifies an encryption algorithm. If you do not specify this keyword, the system does not perform encryption.

- **3des**: Specifies the 3DES encryption algorithm that uses a 168-bit key.
- **aes128**: Specifies the AES encryption algorithm that uses a 128-bit key.
- **des56**: Specifies the DES encryption algorithm that uses a 56-bit key.

priv-password: Specifies an encryption key. This argument is case sensitive.

- The plaintext form of the key is a string of 1 to 64 characters, which must contain numbers, uppercase letters, lowercase letters, and special characters.
- The encrypted form of the key can be calculated by using the **snmp-agent calculate-password** command.

acl: Specifies a basic or advanced IPv4 ACL for the user.

ipv4-acl-number: Specifies a basic or advanced IPv4 ACL by its number. The basic IPv4 ACL number is in the range of 2000 to 2999. The advanced IPv4 ACL number is in the range of 3000 to 3999.

name *ipv4-acl-name*: Specifies a basic or advanced IPv4 ACL by its name, a case-insensitive string of 1 to 63 characters.

acl ipv6: Specifies a basic or advanced IPv6 ACL for the user.

ipv6-acl-number: Specifies a basic or advanced IPv6 ACL by its number. The basic IPv6 ACL number is in the range of 2000 to 2999. The advanced IPv6 ACL number is in the range of 3000 to 3999.

name *ipv6-acl-name*: Specifies a basic or advanced IPv6 ACL by its name, a case-insensitive string of 1 to 63 characters.

local: Specifies the local SNMP engine. By default, a SNMPv3 user is associated with the local SNMP engine.

engineid *engineid-string*: Specifies an SNMP engine ID. The *engineid-string* argument is an even number of hexadecimal characters. All-zero and all-F strings are invalid. The even number is in the range of 10 to 64. If you change the local engine ID, the existing SNMPv3 users and keys become invalid. To delete an invalid username, specify the engine ID associated with the username in the **undo snmp-agent usm-user v3** command.

Usage guidelines

Only users with the network-admin or level-15 user role can execute this command. Users with other user roles cannot execute this command even if these roles are granted access to commands of the SNMP feature or this command.

You can use either of the following modes to control SNMPv3 user access to MIB objects.

- **VACM**—Controls user access to MIB objects by assigning the user to an SNMP group. To make sure the user takes effect, make sure the group has been created. An SNMP group contains one or multiple users and specifies the MIB views and security model for the users. The authentication and encryption algorithms for each user are specified when they are created.

You can execute the **snmp-agent usm-user v3** command multiple times to create different SNMPv3 users in VACM mode. If you do not change the username each time, the most recent configuration takes effect.

You can specify an ACL for the user and group, respectively, to filter illegitimate NMSs from accessing the agent. Only the NMSs permitted by the ACLs for both the user and group can access the SNMP agent. The following rules apply to the ACLs for the user and group:

- If you do not specify an ACL, the specified ACL does not exist, or the specified ACL does not have any rules, all NMSs that use the username can access the SNMP agent.
- If you have specified an ACL and the ACL has rules, only the NMSs permitted by the ACL can access the agent.

For more information about ACL, see *ACL and QoS Configuration Guide*.

Examples

Add user **testUser** to SNMPv3 group **testGroup**, and enable authentication for the group. Specify authentication algorithm **HMAC-SHA1** and plaintext-form authentication key **123456TESTplat&!** for the user.

```
<Switch> system-view
[Switch] snmp-agent group v3 testGroup authentication
[Switch] snmp-agent usm-user v3 testUser testGroup simple authentication-mode sha
123456TESTplat&!
```

For an NMS to access the MIB objects in the default view **ViewDefault**, make sure the following configurations on the NMS are the same as the SNMP agent:

- SNMPv3 username.
- SNMP protocol version.
- Authentication algorithm and key.

Add user **testUser** to SNMPv3 group **testGroup**, and enable authentication and encryption for the group. Specify authentication algorithm **HMAC-SHA1**, encryption algorithm **AES**, plaintext-form authentication key **123456TESTauth&!**, and plaintext-form encryption key **123456TESTencr&!** for the user.

```
<Switch> system-view
[Switch] snmp-agent group v3 testGroup privacy
[Switch] snmp-agent usm-user v3 testUser testGroup simple authentication-mode sha
123456TESTauth&! privacy-mode aes128 123456TESTencr&!
```

For an NMS to access the MIB objects in the default view **ViewDefault**, make sure the following configurations on the NMS are the same as the SNMP agent:

- SNMPv3 username.
- SNMP protocol version.
- Authentication algorithm.
- Privacy algorithm.
- Plaintext authentication and encryption keys.

Related commands

display snmp-agent usm-user

snmp-agent calculate-password

snmp-agent group

Contents

A page of this section is **11-x-x**

5. RMON commands 5-1
5.1. RMON commands 5-1
5.1.1. display rmon alarm 5-1
5.1.2. display rmon event 5-2
5.1.3. display rmon eventlog 5-3
5.1.4. display rmon history 5-5
5.1.5. display rmon prialarm 5-7
5.1.6. display rmon statistics 5-8
5.1.7. rmon alarm 5-10
5.1.8. rmon event 5-12
5.1.9. rmon history 5-13
5.1.10. rmon prialarm 5-14
5.1.11. rmon statistics 5-16

5. RMON commands

5.1. RMON commands

5.1.1. display rmon alarm

Use **display rmon alarm** to display information about RMON alarm entries.

Syntax

display rmon alarm [*entry-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

entry-number: Specifies an alarm entry by its index in the range of 1 to 65535. If you do not specify an entry, the command displays all RMON alarm entries.

Examples

Display information about all RMON alarm entries.

```
<Switch> display rmon alarm
AlarmEntry 1 owned by user1 is VALID.
  Sample type                    : absolute
  Sampled variable               : 1.3.6.1.2.1.16.1.1.1.4.1<etherStatsOctets.1>
  Sampling interval (in seconds) : 10
  Rising threshold               : 50(associated with event 1)
  Falling threshold              : 5(associated with event 2)
  Alarm sent upon entry startup  : risingOrFallingAlarm
  Latest value                   : 0
```

Table 5-1 Command output

Field	Description

AlarmEntry *entry-number* owned by *owner* is *status*.	Alarm entry owner and status:
	• *entry-number*—Alarm entry index.
	• *owner*—Entry owner.
	• *status*—Entry status:
	  ○ **VALID**—The entry is valid.
	  ○ **UNDERCREATION**—The entry is invalid.
	The *status* field is not configurable at the CLI. All alarm entries created from the CLI are valid by default.
	The **display rmon alarm** command can display invalid entries, but the **display current-configuration** and **display this** commands do not display their settings.

Field	Description
Sample type	Sample type: • absolute. • delta.
Sampled variable	Monitored variable.
Sampling interval	Interval (in seconds) at which data is sampled.
Rising threshold	Alarm rising threshold.
associated with event	Event index associated with the alarm..
Falling threshold	Alarm falling threshold.
Alarm sent upon entry startup	Alarm that can be generated at the first sampling: • **risingAlarm**. • **fallingAlarm**. • **risingOrFallingAlarm**. The default is **risingOrFallingAlarm**.
Latest value	Most recent sampled value.

Related commands

rmon alarm

5.1.2. display rmon event

Use **display rmon event** to display information about RMON event entries.

Syntax

display rmon event [*entry-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

entry-number: Specifies an event entry by its index in the range of 1 to 65535. If you do not specify an entry, the command displays all event entries.

Usage guidelines

An event entry includes the following information:

- Event index.
- Event owner.
- Event description.
- Action triggered by the event (such as logging the event or sending an SNMP notification).
- Last time when the event occurred (seconds that elapsed since the system startup).

Examples

Display information about all RMON event entries.

```
<Switch> display rmon event
EventEntry 1 owned by user1 is VALID.
  Description: N/A
  Community: Security
  Take the action log-trap when triggered, last triggered at 0days 00h:02m:27s uptime.
```

Table 5-2 Command output

Field	Description

EventEntry *entry-number* owned by *owner* is *status*.	Event entry owner and status:
	• *entry-number*—Event entry index.
	• *owner*—Entry owner.
	• *status*—Entry status:
	  ○ **VALID**—The entry is valid.
	  ○ **UNDERCREATION**—The entry is invalid.
	The *status* field is not configurable at the CLI. All alarm entries created from the CLI are valid by default.
	The **display rmon event** command can display invalid entries, but the **display current-configuration** and **display this** commands do not display their settings.

Description	Event description.
Community	SNMP community name for the RMON event.
Take the action *action* when triggered	Actions that the system takes when the event is triggered: • **none**—Takes no action. • **log**—Logs the event. • **trap**—Sends an SNMP notification. • **log-trap**—Logs the event and sends an SNMP notification.
last triggered at *time* uptime	Last time when the event occurred, which is represented as the amount of time that elapsed since the system startup.

Related commands

rmon event

5.1.3. display rmon eventlog

Use **display rmon eventlog** to display information about event log entries.

Syntax

display rmon eventlog [*entry-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

entry-number: Specifies an event entry by its index in the range of 1 to 65535. If you do not specify an entry, the command displays log entries for all event entries.

Usage guidelines

If the log action is specified for an event, the system adds a record in the event log table each time the event occurs. Each record contains the log entry index, time when the event was logged (the amount of time that elapsed since system startup), and event description.

The system can maintain a maximum of 10 records for an event. The most recent record replaces the oldest record if the number of records reaches 10.

Examples

Display the RMON log for event entry **99**.

```
<Switch> display rmon eventlog 99
EventEntry 99 owned by ww is VALID.
  LogEntry 99.1 created at 50days 08h:54m:44s uptime.
  Description: The 1.3.6.1.2.1.16.1.1.1.4.5 defined in alarmEntry 77,
     uprise 16760000 with alarm value 16776314. Alarm sample type is absolute.
  LogEntry 99.2 created at 50days 09h:11m:13s uptime.
  Description: The 1.3.6.1.2.1.16.1.1.1.4.5 defined in alarmEntry 77,
     less than(or =) 20000000 with alarm value 16951648. Alarm sample type is absolute.
  LogEntry 99.3 created at 50days 09h:18m:43s uptime.
  Description: The alarm formula defined in prialarmEntry 777,
     less than(or =) 15000000 with alarm value 14026493. Alarm sample type is absolute.
  LogEntry 99.4 created at 50days 09h:23m:28s uptime.
  Description: The alarm formula defined in prialarmEntry 777,
     uprise 17000000 with alarm value 17077846. Alarm sample type is absolute.
```

This example shows that the event log table has four records for event 99:

- Two records were created when event 99 was triggered by alarm entry 77.
- Two records were created when event 99 was triggered by private alarm entry 777.

Table 5-3 Command output

Field	Description

EventEntry *entry-number* owned by *owner* is *status*.	Event log entry owner and status:
	• *entry-number*—Event log entry index, which is the same as the event entry index for which this log entry is generated.
	• *owner*—Entry owner.
	• *status*—Entry status:
	  ○ **VALID**—The entry is valid (default value).
	  ○ **UNDERCREATION**—The entry is invalid.
	The *status* field is not configurable at the CLI. All event log entries are valid by default.
	The **`display rmon eventlog`** command can display invalid entries, but the **`display current-configuration`** and **`display this`** commands do not display their settings.

LogEntry *entry-number* created at *created-time* uptime.	Time when an event record was created: • *entry-number*—Event record index, represented as logEventIndex.logIndex, where logEventIndex and logIndex are MIB objects. A record index uniquely identifies a record among all records for the event. • *created-time*—Time when the event entry was created.
Description	Record description.

Related commands

rmon event

5.1.4. display rmon history

Use **display rmon history** to display RMON history control entries and history samples of Ethernet statistics for Ethernet interfaces.

Syntax

display rmon history [*interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type i*nterface-number*: Specifies an interface by its type and number. If you do not specify an interface, the command displays history samples for all interfaces that have an RMON history control entry.

Usage guidelines

RMON uses the etherHistoryTable object to store the history samples of Ethernet statistics for Ethernet interfaces.

To collect history samples for an Ethernet interface, you must first create a history control entry on the interface.

To configure the number of history samples that can be displayed and the history sampling interval, use the **rmon history** command.

Examples

Display the RMON history control entry and history samples for GigabitEthernet 1/0/1.

```
<Switch> display rmon history gigabitethernet 1/0/1
HistoryControlEntry 6 owned by user1 is VALID.
  Sampled interface     : GigabitEthernet1/0/1<ifIndex.117>
  Sampling interval     : 8(sec) with 3 buckets max
  Sampling record 1 :
    dropevents        : 0         , octets               : 5869
    packets           : 54        , broadcast packets    : 9
    multicast packets : 23        , CRC alignment errors : 0
    undersize packets : 0         , oversize packets     : 0
    fragments         : 0         , jabbers              : 0
    collisions        : 0         , utilization          : 0
```

Table 5-4 Command output

Field	Description
HistoryControlEntry *entry-number* owned by *owner* is *status*.	Status and owner of the history control entry: • *entry-number*—History control entry index. • *owner*—Entry owner.

Field	Description
	• *status*—Entry status: ○ **VALID**—The entry is valid. ○ **UNDERCREATION**—The entry is invalid. The *status* field is not configurable at the CLI. All history control entries created from the CLI are valid by default. The **`display rmon history`** command can display invalid entries, but the **`display current-configuration`** and **`display this`** commands do not display their settings.
Sampled Interface	Sampled interface.
Sampling interval	Sampling interval in seconds.
buckets max	Maximum number of samples that can be saved for the history control entry. If the expected bucket size specified with the **`rmon history`** command exceeds the available history table size, RMON sets the bucket size as closely to the expected bucket size as possible. If the bucket has been full, RMON overwrites the oldest sample with the new sample.
Sampling record	History sample index.
dropevents	Total number of events in which packets were dropped during the sampling interval. **NOTE:** This statistic is the number of times that a drop condition occurred. It is not necessarily the total number of dropped packets.
octets	Total number of octets received during the sampling interval.
packets	Total number of packets (including bad packets) received during the sampling interval.
broadcast packets	Number of broadcast packets received during the sampling interval.
multicast packets	Number of multicast packets received during the sampling interval.
CRC alignment errors	Number of packets received with CRC alignment errors during the sampling interval.
undersize packets	Number of undersize packets received during the sampling interval. Undersize packets are shorter than 64 octets (excluding framing bits but including FCS octets).
oversize packets	Number of oversize packets received during the sampling interval. Oversize packets are longer than 1518 octets (excluding framing bits but including FCS octets).
fragments	Number of undersize packets with CRC errors received during the sampling interval.
jabbers	Number of oversize packets with CRC errors received during the sampling interval.
collisions	Number of colliding packets received during the sampling interval.
utilization	Bandwidth utilization (in hundreds of a percent) during the sampling period.

Related commands

rmon history

5.1.5. display rmon prialarm

Use **display rmon prialarm** to display information about RMON private alarm entries.

Syntax

display rmon prialarm [*entry-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

entry-number: Specifies an alarm entry index in the range of 1 to 65535. If you do not specify an entry, the command displays all private alarm entries.

Examples

Display information about all RMON private alarm entries.

```
<Switch> display rmon prialarm
PrialarmEntry 1 owned by user1 is VALID.
  Sample type                    : absolute
  Variable formula          : (.1.3.6.1.2.1.16.1.1.1.6.1*100/.1.3.6.1.2.1.16.1.1.1.5.1)
  Description                      : ifUtilization.GigabitEthernet1/0/1
  Sampling interval (in seconds) : 10
  Rising threshold                 : 80(associated with event 1)
  Falling threshold                : 5(associated with event 2)
  Alarm sent upon entry startup  : risingOrFallingAlarm
  Entry lifetime                   : forever
  Latest value                     : 85
```

Table 5-5 Command output

Field	Description

PrialarmEntry *entry-number* owned by *owner* is *status*.	Alarm entry owner and status:
	• *entry-number*—Alarm entry index.
	• *owner*—Entry owner.
	• *status*—Entry status:
	  ○ **VALID**—The entry is valid.
	  ○ **UNDERCREATION**—The entry is invalid.
	The *status* field is not configurable at the CLI. All alarm entries created from the CLI are valid by default.
	The **display rmon prialarm** command can display invalid entries, but the **display current-configuration** and **display this** commands do not display their settings.

Sample type	Sample type:

Field	Description
	• absolute. • delta.
Variable formula	Variable formula.
Description	Description of the alarm.
Sampling interval	Interval (in seconds) at which data is sampled.
Rising threshold	Alarm rising threshold.
Falling threshold	Alarm falling threshold.
associated with event	Event index associated with the alarm..
Alarm sent upon entry startup	Alarm that can be generated at the first sampling: • **risingAlarm**. • **fallingAlarm**. • **risingOrFallingAlarm**. The default is **risingOrFallingAlarm**.
Entry lifetime	Lifetime of the entry. • If the lifetime is set to **forever**, the entry never expires. • If the lifetime is set to an amount of time, the entry is removed when the timer expires.
Latest value	Most recent sampled value.

Related commands

rmon prialarm

5.1.6. display rmon statistics

Use **display rmon statistics** to display RMON statistics.

Syntax

display rmon statistics [*interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number: Specifies an interface by its type and number. If you do not specify an interface, the command displays RMON statistics for all interfaces.

Usage guidelines

This command displays the cumulative interface statistics for the period from the time the statistics entry was created to the time the command was executed. The statistics are cleared when the device reboots.

Examples

Display RMON statistics for GigabitEthernet 1/0/1.

```
<Switch> display rmon statistics gigabitethernet 1/0/1
EtherStatsEntry 1 owned by user1 is VALID.
  Interface : GigabitEthernet1/0/1<ifIndex.3>
  etherStatsOctets         : 43393306  , etherStatsPkts          : 619825
  etherStatsBroadcastPkts  : 503581    , etherStatsMulticastPkts : 44013
  etherStatsUndersizePkts  : 0         , etherStatsOversizePkts  : 0
  etherStatsFragments      : 0         , etherStatsJabbers       : 0
  etherStatsCRCAlignErrors : 0         , etherStatsCollisions    : 0
  etherStatsDropEvents (insufficient resources): 0
  Incoming packets by size:
  64     : 0         ,  65-127  : 0         ,  128-255  : 0
  256-511: 0         ,  512-1023: 0         ,  1024-1518: 0
```

Table 5-6 Command output

Field	Description

EtherStatsEntry *entry-number* owned by *owner* is *status*.	Statistics entry owner and status:
	• *entry-number*—Statistics entry index.
	• *owner*—Entry owner.
	• *status*—Entry status:
	  ○ **VALID**—The entry is valid.
	  ○ **UNDERCREATION**—The entry is invalid.
	The *status* field is not configurable at the CLI. All alarm entries created from the CLI are valid by default.
	The **display rmon statistics** command can display invalid entries, but the **display current-configuration** and **display this** commands do not display their settings.

Interface	Interface on which statistics are gathered.
etherStatsOctets	Total number of octets received on the interface.
etherStatsPkts	Total number of packets received on the interface.
etherStatsBroadcastPkts	Total number of broadcast packets received on the interface.
etherStatsMulticastPkts	Total number of multicast packets received on the interface.
etherStatsUndersizePkts	Total number of undersize packets received on the interface.
etherStatsOversizePkts	Total number of oversize packets received on the interface.
etherStatsFragments	Total number of undersize packets received with CRC errors on the interface.
etherStatsJabbers	Total number of oversize packets received with CRC errors on the interface.
etherStatsCRCAlignErrors	Total number of packets received with CRC errors on the interface.
etherStatsCollisions	Total number of colliding packets received on the interface.
etherStatsDropEvents	Total number of events in which packets were dropped. **NOTE:** This statistic is the number of times that a drop condition occurred. It is not necessarily the total number of dropped packets.

Field	Description
Incoming packets by size:	Incoming-packet statistics by packet length: • **64**—Number of packets with a lengthequal to 64 bytes. • **65-127**—Number of 65- to 127-byte packets. • **128-255**—Number of 128- to 255-byte packets. • **256-511**—Number of 256- to 511-byte packets. • **512-1023**—Number of 512- to 1023-byte packets. • **1024-1518**—Number of 1024- to 1518-byte packets.

Related commands

rmon statistics

5.1.7. rmon alarm

Use **rmon alarm** to create an RMON alarm entry.

Use **undo rmon alarm** to remove an RMON alarm entry.

Syntax

rmon alarm *entry-number alarm-variable sampling-interval* { **absolute** | **delta** } [**startup-alarm** { **falling** | **rising** | **rising-falling** }] **rising-threshold** *threshold-value1 event-entry1* **falling-threshold** *threshold-value2 event-entry2* [**owner** *text*]

undo rmon alarm *entry-number*

Default

No RMON alarm entries exist.

Views

System view

Predefined user roles

network-admin

Parameters

entry-number: Specifies an alarm entry index in the range of 1 to 65535.

alarm-variable: Specifies an alarm variable, a string of 1 to 255 characters. You can only specify variables that can be parsed as an ASN.1 INTEGER value (INTEGER, INTEGER32, Unsigned32, Counter32, Counter64, Gauge, or TimeTicks) for the *alarm-variable* argument. The alarm variables must use one of the formats in Table 5-7 .

Table 5-7 Alarm variable formats

Format	Examples
Dotted OID format: *entry.integer.instance*	1.3.6.1.2.1.2.1.10.1
Object name.instance	etherStatsOctets.1 etherStatsPkts.1 etherStatsBroadcastPkts.1 ifInOctets.1

Format	Examples
	ifInUcastPkts.1 ifInNUcastPkts.1

sampling-interval: Sets the sampling interval in the range of 5 to 65535 seconds.

absolute: Specifies absolute sampling. RMON compares the value of the variable with the rising and falling thresholds.

delta: Specifies delta sampling. RMON subtracts the value of the variable at the previous sample from the current sampled value, and then compares the difference with the rising and falling thresholds.

startup-alarm: Specifies alarms that can be generated at the first sampling when a rising or falling threshold is reached or exceeded. By default, a **rising-falling** alarm is generated.

rising: Generates a rising alarm.

falling: Generates a falling alarm.

rising-falling: Generates a rising or falling alarm.

rising-threshold *threshold-value1 event-entry1*: Sets the rising threshold. The *threshold-value1* argument represents the rising threshold in the range of –2147483648 to 2147483647. The *event-entry1* argument represents the index of the event that is triggered when the rising threshold is crossed. The value range for the *event-entry1* argument is 0 to 65535. If 0 is specified, the alarm does not trigger any event.

falling-threshold *threshold-value2 event-entry2*: Sets the falling threshold. The *threshold-value2* argument represents the falling threshold in the range of –2147483648 to 2147483647. The *event-entry2* argument represents the index of the event that is triggered when the falling threshold is crossed. The value range for the *event-entry2* argument is 0 to 65535. If 0 is specified, the alarm does not trigger any event.

owner *text*: Specifies the entry owner, a case-sensitive string of 1 to 127 characters.

Usage guidelines

You can create a maximum of 60 RMON alarm entries.

Each alarm entry must have a unique alarm variable, sampling interval, sample type, rising threshold, or falling threshold. You cannot create an alarm entry if all these parameters for the entry are the same as an existing entry.

To trigger the event associated with an alarm condition, you must create the event with the **rmon event** command.

RMON samples the monitored alarm variable at the specified sampling interval, compares the sampled value with the predefined thresholds, and performs one of the following operations:

- Triggers the event associated with the rising alarm if the sampled value is equal to or greater than the rising threshold.
- Triggers the event associated with the falling alarm if the sampled value is equal to or less than the falling threshold.

Examples

Create an alarm entry to perform absolute sampling on the number of octets received on GigabitEthernet 1/0/1 (object instance 1.3.6.1.2.1.16.1.1.1.4.1) at 10-seconds intervals. If the sampled value reaches or exceeds 5000, log the rising alarm event. If the sampled value is equal to or less than 5, take no actions.

```
<Switch> system-view
```

```
[Switch] rmon event 1 log
[Switch] rmon event 2 none
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] rmon statistics 1
[Switch-GigabitEthernet1/0/1] quit
[Switch] rmon alarm 1 1.3.6.1.2.1.16.1.1.1.4.1 10 absolute rising-threshold 5000 1
falling-threshold 5 2 owner user1
```

In this example, you can replace 1.3.6.1.2.1.16.1.1.1.4.1 with etherStatsOctets.1, where 1 is the statistics entry index for the interface. If you execute the **rmon statistics 5** command, you can use etherStatsOctets.5 to replace 1.3.6.1.2.1.16.1.1.1.4.5.

Related commands

display rmon alarm

rmon event

5.1.8. rmon event

Use **rmon event** to create an RMON event entry.

Use **undo rmon event** to remove an RMON event entry.

Syntax

rmon event *entry-number* [**description** *string*] { **log** | **log-trap** *security-string* | **none** | **trap** *security-string* } [**owner** *text*]

undo rmon event *entry-number*

Default

No RMON event entries exist.

Views

System view

Predefined user roles

network-admin

Parameters

entry-number: Specifies an event entry index in the range of 1 to 65535.

description *string*: Configures an event description, a case-sensitive string of 1 to 127 characters.

log: Logs the event .

log-trap: Logs the event and sends an SNMP notification.

security-string: Specifies the SNMP community name carried in the SNMP notifications. The *security-string* argument is a case-sensitive string of 1 to 127 characters and is determined by the SNMP configuration. This argument is supported but does not take effect in the current software version.

none: Performs no action.

trap: Sends an SNMP notification.

owner *text*: Specifies the entry owner, a case-sensitive string of 1 to 127 characters.

NOTE:

The SNMP community name setting for the *security-string* argument does not take effect even though you can configure it with the command. Instead, the system uses the settings you configure with SNMP when it sends RMON SNMP notifications. For more information about SNMP notifications, see *Network Management and Monitoring Configuration Guide*.

Usage guidelines

You can create a maximum of 60 event entries.

You can associate an event entry with a standard or private alarm entry to specify the action to take when an alarm condition occurs. Depending on your configuration, the system logs the event, sends an SNMP notification, does both, or does neither.

You can associate an event with multiple alarm entries.

Examples

Create an RMON log event entry. Specify its index as **10** and the entry owner as **user1**.

```
<Switch> system-view
[Switch] rmon event 10 log owner user1
```

Related commands

display rmon event

rmon alarm

rmon prialarm

5.1.9. rmon history

Use **rmon history** to create an RMON history control entry.

Use **undo rmon history** to remove an RMON history control entry.

Syntax

rmon history *entry-number* **buckets** *number* **interval** *interval* [**owner** *text*]

undo rmon history *entry-number*

Default

No RMON history control entries exist.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

entry-number: Specifies a history control entry index in the range of 1 to 65535.

buckets *number*: Specifies the expected maximum number of samples to be retained for the entry, in the range of 1 to 65535. RMON can retain a maximum of 50 samples for each history control entry. If the expected bucket size exceeds the available history table size, RMON sets the bucket size as closely to the expected bucket size as is possible. However, the granted bucket size will not exceed 50. For example, the bucket size for a history control entry will be 30 if the expected bucket size is set to 55, but the available bucket size is only 30.

interval *interval*: Specifies the sampling interval in the range of 5 to 3600 seconds.

owner *text*: Specifies the entry owner, a case-sensitive string of 1 to 127 characters.

Usage guidelines

The system supports a maximum of 100 history control entries.

If an Ethernet interface has a history control entry, RMON periodically samples packet statistics on the interface and stores the samples to the history table. When the bucket size for the history control entry is reached, RMON overwrites the oldest sample with the most recent sample.

You can create multiple RMON history control entries for an Ethernet interface.

Examples

Create RMON history control entry 1 for GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] rmon history 1 buckets 10 interval 5 owner user1
```

Related commands

display rmon history

5.1.10. rmon prialarm

Use **rmon** *prialarm* to create an RMON private alarm entry.

Use **undo rmon** *prialarm* to remove an RMON private alarm entry.

Syntax

rmon prialarm *entry-number prialarm-formula prialarm-des sampling-interval* { **absolute** | **delta** } [**startup-alarm** { **falling** | **rising** | **rising-falling** }] **rising-threshold** *threshold-value1 event-entry1* **falling-threshold** *threshold-value2 event-entry2* **entrytype** { **forever** | **cycle** *cycle-period* } [**owner** *text*]

undo rmon prialarm *entry-number*

Default

No RMON private alarm entries exist.

Views

System view

Predefined user roles

network-admin

Parameters

entry-number: Specifies a private alarm entry index in the range of 1 to 65535.

prialarm-formula: Configures a private alarm variable formula, a string of 1 to 255 characters. The variables in the formula must be represented in OID format that starts with a dot (.), for example, (.1.3.6.1.2.1.2.1.10.1)*8. You can configure a formula to perform the basic math operations of addition, subtraction, multiplication, and division on these variables. To get a correct calculation result, make sure the following conditions are met:

- The values of the variables in the formula are positive integers.
- The result of each calculating step is in the value range for long integers.

prialarm-des: Configures an entry description, a case-sensitive string of 1 to 127 characters.

sampling-interval: Sets the sampling interval in the range of 10 to 65535 seconds.

absolute: Specifies absolute sampling. RMON compares the value of the variable with the rising and falling thresholds.

delta: Specifies delta sampling. RMON subtracts the value of the variable at the previous sample from the current sampled value, and then compares the difference with the rising and falling thresholds.

startup-alarm: Specifies alarms that can be generated at the first sampling when a rising or falling threshold is reached or exceeded. By default, a **rising-falling** alarm is generated.

rising: Generates a rising alarm.

falling: Generates a falling alarm.

rising-falling: Generates a rising or falling alarm.

rising-threshold *threshold-value1 event-entry1*: Sets the rising threshold. The *threshold-value1* argument represents the rising threshold in the range of –2147483648 to 2147483647. The *event-entry1* argument represents the index of the event that is triggered when the rising threshold is crossed. The value range for the *event-entry1* argument is 0 to 65535. If 0 is specified, the alarm does not trigger any event.

falling-threshold *threshold-value2 event-entry2*: Sets the falling threshold. The *threshold-value2* argument represents the falling threshold in the range of –2147483648 to 2147483647. The *event-entry2* argument represents the index of the event that is triggered when the falling threshold is crossed. The value range for the *event-entry2* argument is 0 to 65535. If 0 is specified, the alarm does not trigger any event.

forever: Configures the entry as a permanent entry. RMON retains a permanent private alarm entry until it is manually deleted.

cycle *cycle-period*: Sets the lifetime of the entry, in the range of 0 to 4294967 seconds. RMON deletes the entry when its lifetime expires.

owner *text*: Specifies the entry owner, a case-sensitive string of 1 to 127 characters.

Usage guidelines

You can create a maximum of 50 private alarm entries.

Each alarm entry must have a unique alarm variable, sampling interval, sample type, rising threshold, or falling threshold. You cannot create an alarm entry if all these parameters for the entry are the same as an existing entry.

To trigger the event associated with an alarm condition, you must create the event with the **rmon event** command.

The RMON agent samples variables and takes an alarm action based on a private alarm entry as follows:

1. Periodically samples the variables specified in the private alarm formula.
2. Processes the sampled values with the formula.
3. Compares the calculation result with the predefined thresholds, and then takes one of the following actions:
   - Triggers the event associated with the rising alarm event if the result is equal to or greater than the rising threshold.
   - Triggers the event associated with the falling alarm event if the result is equal to or less than the falling threshold.

Examples

Add a permanent private alarm entry to monitor the ratio of incoming broadcasts to the total number of incoming packets on GigabitEthernet 1/0/1. Log the rising alarm event when the ratio exceeds 80%, and take no actions when the ratio drops to 5%. The formula is (1.3.6.1.2.1.16.1.1.1.6.1*100/.1.3.6.1.2.1.16.1.1.1.5.1), where 1.3.6.1.2.1.16.1.1.1.6.1 is the OID of the object instance etherStatsBroadcastPkts.1, and 1.3.6.1.2.1.16.1.1.1.5.1 is the OID of the object instance etherStatsPkts.1.

```
<Switch> system-view
[Switch] rmon event 1 log
[Switch] rmon event 2 none
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] rmon statistics 1
[Switch-GigabitEthernet1/0/1] quit
[Switch] rmon prialarm 1 (.1.3.6.1.2.1.16.1.1.1.6.1*100/.1.3.6.1.2.1.16.1.1.1.5.1)
BroadcastPktsRatioOfGE1/0/1 10 absolute rising-threshold 80 1 falling-threshold 5 2
entrytype forever owner user1
```

The last number in the OID forms of variables must be the same as the statistics entry index for the interface. For example, if you execute the **rmon statistics 5** command, you must replace 1.3.6.1.2.1.16.1.1.1.6.1 and 1.3.6.1.2.1.16.1.1.1.5.1 with 1.3.6.1.2.1.16.1.1.1.6.5 and 1.3.6.1.2.1.16.1.1.1.5.5, respectively.

Related commands

display rmon prialarm

rmon event

5.1.11. rmon statistics

Use **rmon statistics** to create an RMON statistics entry.

Use **undo rmon statistics** to remove an RMON statistics entry.

Syntax

rmon statistics *entry-number* [**owner** *text*]

undo rmon statistics *entry-number*

Default

No RMON statistics entries exist.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

entry-number: Specifies a statistics entry index in the range of 1 to 65535.

owner *text*: Specifies the entry owner, a case-sensitive string of 1 to 127 characters.

Usage guidelines

Each RMON statistics entry provides a set of cumulative traffic statistics collected up to the present time for an interface. Statistics include number of collisions, CRC alignment errors, number of

undersize or oversize packets, number of broadcasts, number of multicasts, number of bytes received, and number of packets received. The statistics are cleared at a reboot.

To display the RMON statistics table, use the **display rmon statistics** command.

You can create only one RMON statistics entry for an Ethernet interface.

Examples

Create an RMON statistics entry for GigabitEthernet 1/0/1. The index is 20 and the owner is **user1**.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] rmon statistics 20 owner user1
```

Related commands

display rmon statistics

Contents

A page of this section is **11-x-x**

6. NETCONF commands ····· 6-1
6.1. NETCONF commands ····· 6-1
6.1.1. netconf log ····· 6-1
6.1.2. netconf soap enable ····· 6-2
6.1.3. netconf ssh server enable ····· 6-2
6.1.4. xml ····· 6-3

6. NETCONF commands

6.1. NETCONF commands

6.1.1. netconf log

Use **netconf log** to enable NETCONF logging.

Use **undo netconf log** to remove the configuration for the specified NETCONF operation sources and NETCONF operations.

Syntax

netconf log source { { **agent** | **soap** } * } { **protocol-operation** { **all** | { **action** | **config** | **get** | **session** | **set** | **syntax** | **others** } * } | **verbose** }

undo netconf log source { { **agent** | **soap** } * } { **protocol-operation** { **all** | { **action** | **config** | **get** | **session** | **set** | **syntax** | **others** } * } | **verbose** }

Default

NETCONF logging is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

source: Specifies a NETCONF operation source that represents clients that use a protocol.

- **agent**: Specifies clients that use Telnet, SSH, console, or NETCONF over SSH.
- **soap**: Specifies clients that use SOAP over HTTP, or SOAP over HTTPS.

protocol-operation: Logs requests and replies for specific types of NETCONF operations.

- **all**: Specifies all types of NETCONF operations.
- **action**: Specifies the <action> operation.
- **config**: Specifies the configuration-related NETCONF operations, including the <CLI>, <save>, <load>, <rollback>, <lock>, <unlock>, and <save-point> operations.
- **get**: Specifies the data retrieval-related NETCONF operations, including the <get>, <get-config>, <get-bulk>, <get-bulk-config>, and <get-sessions> operations.
- **session**: Specifies session-related NETCONF operations, including the <kill-session> and <close-session> operations, and capability exchanges by hello messages.
- **set**: Specifies all <edit-config> operations.
- **syntax**: Specifies the requests that include XML and schema errors.
- **others**: Specifies NETCONF operations except for those specified by keywords **action**, **config**, **get**, **set**, **session**, and **syntax**.

verbose: Logs detailed information about requests and replies for types of NETCONF operations, including packet contents of format-correct requests and error information about failed <edit-config> operations.

Usage guidelines

If you specify the **protocol-operation** keyword, the device logs each of the matching operation and the operation result. For example, if you perform a NETCONF operation to create VLANs 3 through 5, the device outputs the following log messages:

```
%Mar 21 17:11:34:479 2017 NEC XMLSOAP/6/XML_REQUEST: test from 192.168.100.198, session id 2,message-id 100, receive edit-config request.
%Mar 21 17:11:34:483 2017 NEC XMLSOAP/6/EDIT-CONFIG: test from 192.168.100.198, session id 2,message-id 100, execute success.
```

For NETCONF to correctly send the generated logs to the information center, you must also configure the information center. For information about information center configuration, see *Network Management and Monitoring Configuration Guide*.

Examples

Configure the device to log NETCONF edit-config information sourced from agent clients.

```
<Switch> system-view
[Switch] netconf log source agent protocol-operation set
```

6.1.2. netconf soap enable

Use **netconf soap enable** to enable NETCONF over SOAP.

Use **undo netconf soap enable** to disable NETCONF over SOAP.

Syntax

netconf soap { **http** | **https** } **enable**

undo netconf soap { **http** | **https** } **enable**

Default

NETCONF over SOAP is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

http: Specifies NETCONF over SOAP over HTTP.

https: Specifies NETCONF over SOAP over HTTPS.

Usage guidelines

This command enables the device to resolve NETCONF messages that are encapsulated with SOAP in HTTP or HTTPS packets.

Examples

Enable NETCONF over SOAP over HTTP.

```
<Switch> system-view
[Switch] netconf soap http enable
```

6.1.3. netconf ssh server enable

Use **netconf ssh server enable** to enable NETCONF over SSH.

Use **undo netconf ssh server enable** to disable NETCONF over SSH.

Syntax

netconf ssh server enable

undo netconf ssh server enable

Default

NETCONF over SSH is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This feature allows you to use an SSH client to invoke NETCONF as an SSH subsystem. Then, you can directly use XML messages to perform NETCONF operations without using the **xml** command.

Before you execute this command, configure the authentication mode for users as **scheme** on the device. Then, the NETCONF-over-SSH-enabled user terminals can access the device through NETCONF over SSH.

Only capability set **urn:ietf:params:netconf:base:1.0** is available. It is supported by both the device and user terminals.

Examples

Enable NETCONF over SSH.

```
<Switch> system-view
[Switch] netconf ssh server enable
```

NOTE:

The **netconf ssh server enable** command are only supported when used in combination with UNIVERGE Network Operation Engine Overlay Network Extension.

6.1.4. xml

Use **xml** to enter XML view.

Syntax

xml

Views

User view

Predefined user roles

network-admin

network-operator

Usage guidelines

In XML view, use NETCONF messages to configure the device or obtain data from the device. The NETCONF operations you can perform depend on the user roles you have, as shown in Table 6-1 .

Table 6-1 NETCONF operations available for the predefined user roles

User role	NETCONF operations
network-admin	All NETCONF operations
network-operator	• Get • Get-bulk • Get-bulk-config • Get-config • Get-sessions • Close-session

To ensure the format correctness of NETCONF messages in XML view, do not enter NETCONF messages manually. Copy and paste the messages.

While the device is performing a NETCONF operation, do not perform any other operations, such as pasting a NETCONF message or pressing **Enter**.

For the device to identify NETCONF messages, you must add end mark **]]>]]>** at the end of each NETCONF message.

After you enter XML view, the device automatically advertises its NETCONF capabilities to the client. In response, you must configure the client to notify the device of its supported NETCONF capabilities. After the capability exchange, you can use the client to configure the device.

NETCONF messages must comply with the XML format requirements and semantic and syntactic requirements in the NETCONF XML API reference for the device. As a best practice, use third-party software to generate NETCONF messages to ensure successful configuration.

To quit XML view, use a NETCONF message instead of the **quit** command.

If you have configured a shortcut key (**Ctrl + C**, by default) by using the **escape-key** command in user line/user line class view, the NETCONF message should not contain the shortcut key string. If the NETCONF message contains the shortcut key string, relevant configurations in XML view might be affected. For example, in user line view, you configured "a" as the shortcut key by using the **escape-key a** command. When a NETCONF message includes the character "a," only the contents after the last "a" in the message can be processed.

Examples

Enter XML view.

```
<Switch> xml
<?xml version="1.0" encoding="UTF-8"?><hello
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"><capabilities><capability>urn:ietf:pa
rams:netconf:base:1.1</capability><capability>urn:ietf:params:netconf:writable-runnin
g</capability><capability>urn:ietf:params:netconf:capability:notification:1.0</capabi
lity><capability>urn:ietf:params:netconf:capability:validate:1.1</capability><capabil
ity>urn:ietf:params:netconf:capability:interleave:1.0</capability><capability>urn:nec
:params:netconf:capability:nec-netconf-ext:1.0</capability></capabilities><session-id
>1</session-id></hello>]]>]]>
```

Notify the device of the NETCONF capabilities supported on the client.

```
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <capabilities>
    <capability>
            urn:ietf:params:netconf:base:1.0
    </capability>
  </capabilities>
</hello>]]>]]>
```

Quit XML view.

```
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <close-session>
  </close-session>
</rpc>]]>]]>
<Switch>
```

Contents

A page of this section is **11-x-x**

7. Process monitoring and maintenance commands 7-1
7.1. Process monitoring and maintenance commands 7-1
7.1.1. display exception context 7-1
7.1.2. display exception filepath 7-5
7.1.3. exception filepath 7-6
7.1.4. process core 7-6
7.1.5. reset exception context 7-7

7. Process monitoring and maintenance commands

7.1. Process monitoring and maintenance commands

7.1.1. display exception context

Use **display exception context** to display context information for process exceptions.

Syntax

display exception context [**count** *value*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

Parameters

count *value*: Specifies the number of context information entries, in the range of 1 to 20. The default value is 1.

slot *slot-number*: Specifies an IRF member device by its ID. If you do not specify this option, the command displays context information for process exceptions on the IRF master device.

Usage guidelines

The system generates a context information entry for each process exception. A context information entry includes the process ID, the crash time, the core file directory, stack information, and register information.

Examples

Display the exception context information on the x86-based 32-bit terminal.

```
<Switch> display exception context
Index 1 of 1
------------------------------
Crashed PID: 120 (routed)
Crash signal: SIGBUS
Crash time: Tue Apr  9 17:14:30 2013
Core file path:
flash:/core/node0_routed_120_7_20130409-171430_1365527670.core
#0  0xb7caba4a
#1  0x0804cb79
#2  0xb7cd77c4
#3  0x08049f45
Backtrace stopped.
                          Registers' content
```

```
  eax:0xfffffffc   ebx:0x00000003   ecx:0xbfe244ec   edx:0x0000000a
  esp:0xbfe244b8   ebp:0xbfe244c8   esi:0xffffffff   edi:0xbfe24674
  eip:0xb7caba4a eflag:0x00000292    cs:0x00000073    ss:0x0000007b
   ds:0x0000007b    es:0x0000007b    fs:0x00000000    gs:0x00000033
```

Display the exception context information on the x86-based 64-bit terminal.

```
<Switch> display exception context
Index 1 of 1
------------------------------
Crashed PID: 121 (routed)
Crash signal: SIGBUS
Crash time: Sun Mar 31 11:12:21 2013
Core file path:
flash:/core/node0_routed_121_7_20130331-111221_1364728341.core
#0  0x00007fae7dbad20c
#1  0x00000000004059fa
#2  0x00007fae7dbd96c0
#3  0x0000000000402b29
Backtrace stopped.
                         Registers' content
       rax:0xfffffffffffffffc       rbx:0x00007fff88a5dd10
       rcx:0xffffffffffffffff       rdx:0x000000000000000a
       rsi:0x00007fff88a5dd10       rdi:0x0000000000000003
       rbp:0x00007fff88a5dcf0       rsp:0x00007fff88a5dcf0
        r8:0x00007fae7ea587e0        r9:0x0000000000000079
       r10:0xffffffffffffffff       r11:0x0000000000000246
       r12:0x0000000000405b18       r13:0x00007fff88a5ff7a
       r14:0x00007fff88a5de30       r15:0x0000000000000000
       rip:0x00007fae7dbad20c      flag:0x0000000000000246
        cs:0x0000000000000033        ss:0x000000000000002b
        ds:0x0000000000000000        es:0x0000000000000000
        fs:0x0000000000000000        gs:0x0000000000000000
   fs_base:0x00007fae80a5d6a0   gs_base:0x0000000000000000
   orig_ax:0x00000000000000e8
```

Display the exception context information on the PowerPC-based 32-bit terminal.

```
<Switch> display exception context
Index 1 of 1
------------------------------
Crashed PID: 133 (routed)
Crash signal: SIGBUS
Crash time: Wed Apr 10 15:47:49 2013
Core file path:
flash:/core/node0_routed_133_7_20130410-154749_1365608869.core
#0  0x184720bc
#1  0x10006b4c
Backtrace stopped.
                         Registers' content
grp00: 0x000000ee 0x7ffd6ad0 0x1800f440 0x00000004
```

```
grp04: 0x7ffd6af8 0x0000000a 0xffffffff 0x184720bc
grp08: 0x0002d200 0x00000003 0x00000001 0x1847209c
grp12: 0x10006b4c 0x10020534 0xd6744100 0x00000000
grp16: 0x00000000 0xa0203ff0 0xa028b12c 0xa028b13c
grp20: 0xa028b148 0xa028b168 0xa028b178 0xa028b190
grp24: 0xa028b1a8 0xa028b1b8 0x00000000 0x7ffd6c08
grp28: 0x10006cac 0x7ffd6f92 0x184c1b84 0x7ffd6ae0

  nip:0x184720bc    lr:0x10006b4c    cr:0x38000022   ctr:0x1847209c
  msr:0x0002db00   xer:0x00000000   ret:0xfffffffc dsisr:0x08000000
  gr3:0x00000003    mq:0x00000000  trap:0x00000c00   dar:0x1833114c
```

Display the exception context information on the PowerPC-based 64-bit terminal.

```
<Switch> display exception context
Index 1 of 1
------------------------------
Crashed PID: 172 (routed)
Crash signal: SIGBUS
Crash time: Sat Sep 15 16:53:16 2007
Core file path:
flash:/core/node1_routed_172_7_20070915-165316_1189875196.core
#0  0x00000fff803c66b4
#1  0x0000000010009b94
#2  0x00000fff80401814
Backtrace stopped.
                         Registers' content
     grp00: 0x00000000000000ee 0x00000fffffd04840
     grp02: 0x00000fff80425c28 0x0000000000000004
     grp04: 0x00000fffffd048c0 0x000000000000000a
     grp06: 0xffffffffffffffff 0x00000fff803c66b4
     grp08: 0x000000008002d000 0x0000000000000000
     grp10: 0x0000000000000000 0x0000000000000000
     grp12: 0x0000000000000000 0x00000fff80a096b0
     grp14: 0x000000007b964c00 0x000000007b7d0000
     grp16: 0x0000000000000001 0x000000000000000b
     grp18: 0x0000000000000031 0x0000000000a205b8
     grp20: 0x0000000000a20677 0x0000000000000000
     grp22: 0x000000007bb91014 0x0000000000000000
     grp24: 0xc0000000005ae1c8 0x0000000000000000
     grp26: 0xc0000001f00bff20 0xc0000001f00b0000
     grp28: 0x00000fffffd04a30 0x000000001001aed8
     grp30: 0x00000fffffd04fae 0x00000fffffd04840

       nip:0x00000fff803c66b4        lr:0x0000000010009b94
        cr:0x0000000058000482       ctr:0x00000fff803c66ac
       msr:0x000000008002d000       xer:0x0000000000000000
       ret:0xfffffffffffffffc     dsisr:0x0000000000000000
       gr3:0x0000000000000003     softe:0x0000000000000001
```

```
      trap:0x0000000000000c00       dar:0x00000fff8059d14c
```

Display the exception context information on the MIPS-based 32-bit terminal.

```
<Switch> display exception context
Index 1 of 1
-----------------------------
Crashed PID: 182 (routed)
Crash signal: SIGBUS
Crash time: Sun Jan  2 08:11:38 2013
Core file path:
flash:/core/node4_routed_182_10_20130102-081138_1293955898.core
#0  0x2af2faf4
#1  0x00406d8c
Backtrace stopped.
                        Registers' content
 zero:0x00000000   at:0x1000dc00   v0:0x00000004   v1:0x00000003
   a0:0x00000003   a1:0x7fd267e8   a2:0x0000000a   a3:0x00000001
   t0:0x00000000   t1:0xcf08fa14   t2:0x80230510   t3:0xfffffff8
   t4:0x69766520   t5:0x00000000   t6:0x63cc6000   t7:0x44617461
   s0:0x7fd26f81   s1:0x00401948   s2:0x7fd268f8   s3:0x803e1db0
   s4:0x803e1da0   s5:0x803e1d88   s6:0x803e1d70   s7:0x803e1d60
   t8:0x00000008   t9:0x2af2fae0   k0:0x00000000   k1:0x00000000
   gp:0x2af9a3a0   sp:0x7fd267c0   s8:0x7fd267c0   ra:0x00406d8c
   sr:0x0000dc13   lo:0xef9db265   hi:0x0000003f  bad:0x2add2010
cause:0x00800020   pc:0x2af2faf4
```

Display the exception context information on the MIPS-based 64-bit terminal.

```
<Switch> display exception context
Index 1 of 1
-----------------------------
Crashed PID: 270 (routed)
Crash signal: SIGBUS
Crash time: Wed Mar 27 12:39:12 2013
Core file path:
flash:/core/node16_routed_270_10_20130327-123912_1364387952.core
#0  0x0000005555a3bcb4
#1  0x0000000120006c1c
Backtrace stopped.
                        Registers' content
      zero:0x0000000000000000        at:0x0000000000000014
        v0:0x0000000000000004        v1:0x0000000000000003
        a0:0x0000000000000003        a1:0x000000ffff899d90
        a2:0x000000000000000a        a3:0x0000000000000001
        a4:0x0000005555a9b4e0        a5:0x0000000000000000
        a6:0xffffffff8021349c        a7:0x20696e206368616e
        t0:0x0000000000000000        t1:0xffffffff80105068
        t2:0xffffffff80213890        t3:0x0000000000000008
        s0:0x0000005555a99c40        s1:0x000000ffff89af5f
        s2:0x0000000120007320        s3:0x0000005555a5f470
```

```
        s4:0x000000ffff899f80        s5:0xffffffff803cc6c0
        s6:0xffffffff803cc6a8        s7:0xffffffff803cc690
        t8:0x0000000000000002        t9:0x0000005555a3bc98
        k0:0x0000000000000000        k1:0x0000000000000000
        gp:0x0000000120020460        sp:0x000000ffff899d70
        s8:0x000000ffff899d80        ra:0x0000000120006c1c
        sr:0x000000000400fff3        lo:0xdf3b645a1cac08c9
        hi:0x000000000000007f       bad:0x000000555589ba84
     cause:0x0000000000800020        pc:0x0000005555a3bcb4
```

Table 7-1 Command output

Filed	Description
Crashed PID	ID of the crashed process.
Crash signal	Signals that led to the crash: • **SIGABRT**—Abort. • **SIGBUS**—Bus error. • **SIGFPE**—Erroneous arithmetic operation. • **SIGILL**—Illegal hardware instructions. • **SIGQUIT**—Quit signal sent by the controlling terminal. • **SIGSEGV**—Invalid memory access. • **SIGSYS**—Invalid system call. • **SIGTRAP**—Trap message. • **SIGXCPU**—CPU usage limit exceeded. • **SIGXFSZ**—File size limit exceeded. • **SIGUNKNOW**—Unknown reason.
Crash time	Time when the crash occurred.
Core file path	Directory where the core file is saved.
Backtrace stopped	All stack information has been displayed.

Related commands

reset exception context

7.1.2. display exception filepath

Use **display exception filepath** to display the core file directory.

Syntax

display exception filepath [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its ID. If you do not specify this option, the command displays the core file directory on the IRF master device.

Examples

Display the core file directory on the specified slot.

```
<Switch> display exception filepath slot 1
The exception filepath on slot 1 is flash:.
```

7.1.3. exception filepath

Use **exception filepath** to specify the directory for saving core files.

Use **undo exception filepath** to remove the specified directory.

Syntax

exception filepath *directory*

undo exception filepath *directory*

Default

The directory for saving core files is **flash:/**.

Views

User view

Predefined user roles

network-admin

Parameters

directory: Specifies the directory for saving core files.

Usage guidelines

The specified directory must be the root directory of a file system on the master.

You can use the command to change the directory if there are different types of storage media on the device.

The system saves core files to the **core** directory in the specified directory. If the **core** directory does not exist in the specified directory, the system creates the **core** directory before saving core files.

If no directory is specified or the specified directory is not accessible, the system cannot save core files.

Examples

Set the directory for saving core files to flash:/.

```
<Switch> exception filepath flash:/
```

Related commands

display exception filepath

process core

7.1.4. process core

Use **process core** to enable or disable a process to generate core files for exceptions and set the maximum number of core files.

Syntax

process core { **maxcore** *value* | **off** } { **job** *job-id* | **name** *process-name* } [**slot** *slot-number*]

Views

User view

Default

A process generates a core file for the first exception and does not generate any core files for subsequent exceptions.

Predefined user roles

network-admin

Parameters

off: Disables core file generation.

maxcore *value*: Enables core file generation and sets the maximum number of core files, in the range of 1 to 10.

name *process-name*: Specifies a process by its name, a case-insensitive string of 1 to 15 characters.

job *job-id*: Specifies a process by its job ID, in the range of 1 to 2147483647. The job ID does not change after the process restarts.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information for the master device.

Usage guidelines

The command applies to all instances of a process.

The command enables the system to generate a core file each time the specified process crashes until the maximum number of core files is reached. A core file records the exception information.

Because the core files consume system storage resources, you can disable core file generation for processes for which you do not need to review exception information.

Examples

Disable core file generation for process **routed**.

```
<Switch> process core off name routed
```

Enable core file generation for process **routed** and set the maximum number of core files to 5.

```
<Switch> process core maxcore 5 name routed
```

Related commands

display exception context

exception filepath

7.1.5. reset exception context

Use **reset exception context** to clear context information for process exceptions.

Syntax

reset exception context [**slot** *slot-number*]

Views

User view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its ID. If you do not specify this option, the command clears context information for process exceptions on the IRF master device.

Examples

Clear context information for exceptions.

```
<Switch> reset exception context
```

Related commands

display exception context

Contents

A page of this section is **11-x-x**

8. Port mirroring commands 8-1
8.1. Port mirroring commands 8-1
8.1.1. display mirroring-group 8-1
8.1.2. mirroring-group 8-2
8.1.3. mirroring-group mirroring-port (interface view) 8-2
8.1.4. mirroring-group mirroring-port (system view) 8-3
8.1.5. mirroring-group monitor-egress 8-5
8.1.6. mirroring-group monitor-port (interface view) 8-6
8.1.7. mirroring-group monitor-port (system view) 8-7
8.1.8. mirroring-group reflector-port 8-8
8.1.9. mirroring-group remote-probe vlan 8-9

8. Port mirroring commands

8.1. Port mirroring commands

8.1.1. display mirroring-group

Use **display mirroring-group** to display mirroring group information.

Syntax

display mirroring-group { *group-id* | **all** | **local** | **remote-destination** | **remote-source** }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

group-id: Specifies a mirroring group by its ID. The value range for this argument is 1 to 7.

all: Specifies all mirroring groups.

local: Specifies local mirroring groups.

remote-destination: Specifies remote destination groups.

remote-source: Specifies remote source groups.

Usage guidelines

Mirroring group information includes the type, status, and content of a mirroring group. It is sorted by mirroring group number.

Examples

Display information about all mirroring groups.

```
<Switch> display mirroring-group all
Mirroring group 1:
    Type: Local
    Status: Active
    Mirroring port:
        GigabitEthernet1/0/1  Inbound
    Monitor port: GigabitEthernet1/0/2
```

Table 8-1 Command output

Field	Description
Mirroring group	Number of the mirroring group.
Type	Type of the mirroring group: • Local. • Remote source.

Field	Description
	• Remote destination.
Status	Status of the mirroring group: • **Active**—The mirroring group has taken effect. • **Incomplete**—The mirroring group configuration is not complete and does not take effect.
Mirroring port	Source port.
Monitor port	Destination port.

8.1.2. mirroring-group

Use **mirroring-group** to create a mirroring group.

Use **undo mirroring-group** to delete mirroring groups.

Syntax

mirroring-group *group-id* { **local** | **remote-destination** | **remote-source** }

undo mirroring-group { *group-id* | **all** | **local** | **remote-destination** | **remote-source** }

Default

No mirroring groups exist.

Views

System view

Predefined user roles

network-admin

Parameters

group-id: Specifies a mirroring group ID. The value range for this argument is 1 to 7.

local: Specifies local mirroring groups.

remote-destination: Specifies remote destination groups.

remote-source: Specifies remote source groups.

all: Specifies all mirroring groups.

Examples

Create local mirroring group 1.

```
<Switch> system-view
[Switch] mirroring-group 1 local
```

8.1.3. mirroring-group mirroring-port (interface view)

Use **mirroring-group mirroring-port** to configure a port as a source port for a mirroring group.

Use **undo mirroring-group mirroring-port** to restore the default.

Syntax

mirroring-group *group-id* **mirroring-port** { **both** | **inbound** | **outbound** }

undo mirroring-group *group-id* **mirroring-port**

Default

A port does not act as a source port for any mirroring groups.

Views

Interface view

Predefined user roles

network-admin

Parameters

group-id: Specifies a mirroring group by its ID. The value range for this argument is 1 to 7.

both: Mirrors both received and sent packets.

inbound: Mirrors only received packets.

outbound: Mirrors only sent packets.

Usage guidelines

You can configure source ports only for local mirroring groups and remote source groups.

On a Layer 2 aggregate interface configured as a source port, only the overlay traffic of the VXLAN network can be mirrored.

On a member port of a Layer 2 aggregate interface configured as a source port, VXLAN traffic cannot be mirrored.

Do not assign a source port of a mirroring group to the remote probe VLAN of the mirroring group.

A port can act as a source port for only one mirroring group. If you assign a port as a source port to multiple mirroring groups, the most recent configuration takes effect.

A source port cannot be used as a reflector port, monitor port, or egress port.

Examples

Create local mirroring group 1 to monitor the bidirectional traffic of the port GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] mirroring-group 1 local
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] mirroring-group 1 mirroring-port both
```

Create remote source group 2 to monitor the bidirectional traffic of the port GigabitEthernet 1/0/2.

```
<Switch> system-view
[Switch] mirroring-group 2 remote-source
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] mirroring-group 2 mirroring-port both
```

Related commands

mirroring-group

8.1.4. mirroring-group mirroring-port (system view)

Use **mirroring-group mirroring-port** to configure source ports for a mirroring group.

Use **undo mirroring-group mirroring-port** to remove source ports from a mirroring group.

Syntax

mirroring-group *group-id* **mirroring-port** *interface-list* { **both** | **inbound** | **outbound** }

undo mirroring-group *group-id* **mirroring-port** *interface-list*

Default

No source port is configured for a mirroring group.

Views

System view

Predefined user roles

network-admin

Parameters

group-id: Specifies a mirroring group by its ID. The value range for this argument is 1 to 7.

interface-list: Specifies a space-separated list of up to eight interface items. Each item specifies an interface by its type and number or specifies a range of interfaces in the form of *interface-type interface-number1* **to** *interface-type interface-number2*. When you specify a range of interfaces, the interfaces must be of the same type and on the same slot. The start interface number must be identical to or lower than the end interface number.

both: Mirrors both received and sent packets.

inbound: Mirrors only received packets.

outbound: Mirrors only sent packets.

Usage guidelines

You can configure source ports only for local mirroring groups and remote source groups.

On a Layer 2 aggregate interface configured as a source port, only the overlay traffic of the VXLAN network can be mirrored.

On a member port of a Layer 2 aggregate interface configured as a source port, VXLAN traffic cannot be mirrored.

Do not assign a source port of a mirroring group to the remote probe VLAN of the mirroring group.

A port can act as a source port for only one mirroring group. If you assign a port as a source port to multiple mirroring groups, the most recent configuration takes effect.

A source port cannot be used as a reflector port, monitor port, or egress port.

Examples

Create local mirroring group 1 to monitor the bidirectional traffic of GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] mirroring-group 1 local
[Switch] mirroring-group 1 mirroring-port gigabitethernet 1/0/1 both
```

Create remote source group 2 to monitor the bidirectional traffic of GigabitEthernet 1/0/2.

```
<Switch> system-view
[Switch] mirroring-group 2 remote-source
[Switch] mirroring-group 2 mirroring-port gigabitethernet 1/0/2 both
```

Related commands

mirroring-group

8.1.5. mirroring-group monitor-egress

Use **mirroring-group monitor-egress** to configure the egress port for a remote source group.

Use **undo mirroring-group monitor-egress** to restore the default.

Syntax

In system view:

mirroring-group *group-id* **monitor-egress** *interface-type interface-number*

undo mirroring-group *group-id* **monitor-egress** *interface-type interface-number*

In interface view:

mirroring-group *group-id* **monitor-egress**

undo mirroring-group *group-id* **monitor-egress**

Default

No egress port is configured for a remote source group.

Views

System view

Interface view

Predefined user roles

network-admin

Parameters

group-id: Specifies a mirroring group by its ID. The value range for this argument is 1 to 7.

interface-type interface-number: Specifies a port by its type and number.

Usage guidelines

You can configure egress ports only for remote source groups.

For port mirroring to work correctly, disable the following features on the egress port of a mirroring group:

- Spanning tree.
- 802.1X.
- IGMP snooping.
- Static ARP.
- MAC address learning.

The member port of an existing mirroring group cannot be configured as an egress port.

The member port of an aggregate interface cannot be configured as an egress port.

Examples

Create remote source group 1. Configure GigabitEthernet 1/0/1 as its egress port in system view.

```
<Switch> system-view
```

```
[Switch] mirroring-group 1 remote-source
[Switch] mirroring-group 1 monitor-egress gigabitethernet 1/0/1
```

Create remote source group 2. Configure GigabitEthernet 1/0/2 as its egress port in interface view.

```
<Switch> system-view
[Switch] mirroring-group 2 remote-source
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] mirroring-group 2 monitor-egress
```

Related commands

mirroring-group

8.1.6. mirroring-group monitor-port (interface view)

Use **mirroring-group monitor-port** to configure a port as the monitor port for a mirroring group.

Use **undo mirroring-group monitor-port** to restore the default.

Syntax

mirroring-group *group-id* **monitor-port**

undo mirroring-group *group-id* **monitor-port**

Default

A port does not act as the monitor port for any mirroring groups.

Views

Interface view

Predefined user roles

network-admin

Parameters

group-id: Specifies a mirroring group by its ID. The value range for this argument is 1 to 7.

Usage guidelines

You can configure monitor ports only for local mirroring groups and remote destination groups.

Do not enable the spanning tree feature on the monitor port of a mirroring group.

A Layer 2 interface cannot be configured as the monitor port for a mirroring group.

Use a monitor port only for port mirroring, so the data monitoring device receives and analyzes only the mirrored traffic.

The member port of an existing mirroring group cannot be configured as a monitor port.

Examples

Create local mirroring group 1 and configure GigabitEthernet 1/0/1 as its monitor port.

```
<Switch> system-view
[Switch] mirroring-group 1 local
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] mirroring-group 1 monitor-port
```

Create remote destination group 2 and configure GigabitEthernet 1/0/2 as its monitor port.

```
<Switch> system-view
```

```
[Switch] mirroring-group 2 remote-destination
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] mirroring-group 2 monitor-port
```

Related commands

mirroring-group

8.1.7. mirroring-group monitor-port (system view)

Use **mirroring-group monitor-port** to configure the monitor ports for a mirroring group.

Use **undo mirroring-group monitor-port** to remove the monitor ports from a mirroring group.

Syntax

mirroring-group *group-id* **monitor-port** *interface-type interface-number*

undo mirroring-group *group-id* **monitor-port** *interface-type interface-number*

Default

No monitor port is configured for a mirroring group.

Views

System view

Predefined user roles

network-admin

Parameters

group-id: Specifies a mirroring group by its ID. The value range for this argument is 1 to 7.

interface-type interface-number: Specifies an interface by its type and number.

Usage guidelines

You can configure monitor ports only for local mirroring groups and remote destination groups.

Do not enable the spanning tree feature on the monitor port of a mirroring group.

A Layer 2 aggregate interface cannot be configured as the monitor port for a mirroring group.

Use a monitor port only for port mirroring, so the data monitoring device receives only the mirrored traffic.

The member port of an existing mirroring group cannot be configured as a monitor port.

Examples

Create local mirroring group 1 and configure GigabitEthernet 1/0/1 as its monitor port.

```
<Switch> system-view
[Switch] mirroring-group 1 local
[Switch] mirroring-group 1 monitor-port gigabitethernet 1/0/1
```

Create remote destination group 2 and configure GigabitEthernet 1/0/2 as its monitor port.

```
<Switch> system-view
[Switch] mirroring-group 2 remote-destination
[Switch] mirroring-group 2 monitor-port gigabitethernet 1/0/2
```

Related commands

mirroring-group

8.1.8. mirroring-group reflector-port

Use **mirroring-group reflector-port** to configure the reflector port for a remote source group.

Use **undo mirroring-group reflector-port** to restore the default.

Syntax

In system view:

mirroring-group *group-id* **reflector-port** *interface-type interface-number*

undo mirroring-group *group-id* **reflector-port** *interface-type interface-number*

In interface view:

mirroring-group *group-id* **reflector-port**

undo mirroring-group *group-id* **reflector-port**

Default

No reflector port is configured for a mirroring group.

Views

System view

Interface view

Predefined user roles

network-admin

Parameters

group-id: Specifies a mirroring group by its ID. The value range for this argument is 1 to 7.

interface-type interface-number: Specifies a port by its type and number.

Usage guidelines

You can configure reflector ports only for remote source groups.

The port to be configured as a reflector port must be a port not in use. Do not connect a network cable to a reflector port.

When a port is configured as a reflector port, the port restores to the factory default settings. You cannot configure other features on a reflector port.

If an IRF port is bound to only one physical interface, do not configure the physical interface as a reflector port. Otherwise, the IRF might split.

You cannot change the duplex mode, MDI settings, or speed for a reflector port.

The member port of an aggregate interface cannot be configured as a reflector port.

Examples

Create remote source group 1. Configure GigabitEthernet 1/0/1 as its reflector port in system view.

```
<Switch> system-view
[Switch] mirroring-group 1 remote-source
[Switch] mirroring-group 1 reflector-port gigabitethernet 1/0/1
```

```
This operation may delete all settings made on the interface. Continue? [Y/N]: y
```

Create remote source group 2. Configure GigabitEthernet 1/0/2 as its reflector port in interface view.

```
<Switch> system-view
[Switch] mirroring-group 2 remote-source
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] mirroring-group 2 reflector-port
This operation may delete all settings made on the interface. Continue? [Y/N]: y
```

Related commands

mirroring-group

8.1.9. mirroring-group remote-probe vlan

Use **mirroring-group remote-probe vlan** to specify a VLAN as the remote probe VLAN for a mirroring group.

Use **undo mirroring-group remote-probe vlan** to restore the default.

Syntax

mirroring-group *group-id* **remote-probe vlan** *vlan-id*

undo mirroring-group *group-id* **remote-probe vlan** *vlan-id*

Default

No remote probe VLAN is configured for a mirroring group.

Views

System view

Predefined user roles

network-admin

Parameters

group-id: Specifies a mirroring group by its ID. The value range for this argument is 1 to 7.

vlan-id: Specifies a VLAN by its ID.

Usage guidelines

You can configure remote probe VLANs only for remote source groups and remote destination groups.

When a VLAN is configured as a remote probe VLAN, use the VLAN for port mirroring exclusively.

The remote mirroring groups on the source device and destination device must use the same remote probe VLAN.

Only a static VLAN that already exists can be configured as a remote probe VLAN. A VLAN can be configured as the remote probe VLAN for only one mirroring group.

To delete a VLAN that is configured as a remote probe VLAN, remove the remote probe VLAN configuration first.

Examples

Create remote source group 1 and configure VLAN 10 as its remote probe VLAN.

```
<Switch> system-view
[Switch] mirroring-group 1 remote-source
```

```
[Switch] mirroring-group 1 remote-probe vlan 10
```

Create remote destination group 2 and configure VLAN 20 as its remote probe VLAN.

```
<Switch> system-view
[Switch] mirroring-group 2 remote-destination
[Switch] mirroring-group 2 remote-probe vlan 20
```

Related commands

mirroring-group

Contents

A page of this section is **11-x-x**

9. Flow mirroring commands 9-1
9.1. Flow mirroring commands 9-1
9.1.1. mirror-to interface 9-1

9. Flow mirroring commands

9.1. Flow mirroring commands

9.1.1. mirror-to interface

Use **mirror-to interface** to configure a mirroring action that mirrors traffic to an interface.

Use **undo mirror-to interface** to delete a mirroring action that mirrors traffic to an interface.

Syntax

mirror-to interface *interface-type interface-number*

undo mirror-to interface *interface-type interface-number*

Default

No mirroring actions exist to mirror traffic to interfaces.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

*interface-type interface-numbe*r: Specifies an interface by its type and number.

Usage guidelines

You can execute this command multiple times for a traffic behavior to mirror traffic to different interfaces.

You can mirror traffic to only one interface. If you execute this command for a traffic behavior multiple times, the most recent configuration takes effect.

Examples

Create traffic behavior 1 and configure the action of mirroring traffic to GigabitEthernet 1/0/1 for the traffic behavior.

```
<Switch> system-view
[Switch] traffic behavior 1
[Switch-behavior-1] mirror-to interface gigabitethernet 1/0/1
```

Contents

A page of this section is **11-x-x**

10. sFlow commands 10-1
10.1. sFlow commands 10-1
10.1.1. display sflow 10-1
10.1.2. sflow agent 10-2
10.1.3. sflow collector 10-3
10.1.4. sflow counter collector 10-4
10.1.5. sflow counter interval 10-4
10.1.6. sflow flow collector 10-5
10.1.7. sflow flow max-header 10-6
10.1.8. sflow sampling-mode 10-6
10.1.9. sflow sampling-rate 10-7
10.1.10. sflow source 10-8

10. sFlow commands

10.1. sFlow commands

10.1.1. display sflow

Use **display sflow** to display sFlow configuration and operation information.

Syntax

display sflow

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display sFlow configuration and operation information.

```
<Switch> display sflow
sFlow datagram version: 5
Global information:
Agent IP: 10.10.10.1(CLI)
Source address: 10.0.0.1 2001::1
Collector information:
ID    IP              Port  Aging      Size VPN-instance Description
1     22:2:20::10     6535  N/A        1400              netserver
2     192.168.3.5     6543  500        1400              Office
Port information:
Interface      CID   Interval(s) FID   MaxHLen Rate       Mode      Status
GE1/0/1        1     100         1     128     1000       Random    Active
GE1/0/2        2     100         2     128     1000       Random    Active
```

Table 10-1 Command output

Field	Description
sFlow datagram version	sFlow version, which can only take the value of 5. The device can send only sFlow packets whose sFlow version is 5.
Global information	Global sFlow information.
Agent IP	IP address of the sFlow agent: • **CLI**—Manually configured IP address. • **Auto**—Automatically configured IP address.
Source address	Source IP address of sFlow packets.
Collector information	sFlow collector information.
ID	sFlow collector ID.

Field	Description
IP	sFlow collector IP address.
Port	sFlow collector port.
Aging	Remaining lifetime of the sFlow collector. If this field displays **N/A**, the sFlow collector never ages out.
Size	Maximum length of the sFlow data portion in a sFlow packet.
VPN-instance	Name of the VPN instance to which the sFlow collector belongs.
Description	Description of the sFlow collector.
Port information	Information about interfaces configured with sFlow.
Interface	Interface configured with sFlow.
CID	ID of the sFlow collector for receiving counter sampled packets. If no sFlow collector ID is specified, this field displays **0**.
Interval(s)	Counter sampling interval, in seconds.
FID	ID of the sFlow collector for receiving flow sampled packets. If no sFlow collector ID is specified, this field displays **0**.
MaxHLen	Maximum number of bytes that can be copied in a sampled packet (starting from the packet header).
Rate	Number of packets out of which the interface samples a packet by using flow sampling.
Mode	Flow sampling mode.
Status	sFlow status of the port: • **Suspended**—The sFlow feature is suspended because the port is down. • **Active**—The sFlow feature is active because the port is up.

10.1.2. sflow agent

Use **sflow agent** to configure an IP address for the sFlow agent.

Use **undo sflow agent** to restore the default.

Syntax

sflow agent { **ip** *ipv4-address* | **ipv6** *ipv6-address* }

undo sflow agent { **ip** | **ipv6** }

Default

No IP address is configured for the sFlow agent. The device periodically identifies whether the sFlow agent has an IP address. If the sFlow agent does not have an IP address, the device automatically selects an IPv4 address for the sFlow agent. It does not save the IPv4 address in the configuration file.

Views

System view

Predefined user roles

network-admin

Parameters

ip *ipv4-address*: Specifies an IPv4 address for the sFlow agent.

ipv6 *ipv6-address*: Specifies an IPv6 address for the sFlow agent.

Usage guidelines

As a best practice, manually configure an IP address for the sFlow agent.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify IP address 10.10.10.1 for the sFlow agent.

```
<Switch> system-view
[Switch] sflow agent ip 10.10.10.1
```

10.1.3. sflow collector

Use **sflow collector** to configure parameters for a sFlow collector.

Use **undo sflow collector** to remove a sFlow collector.

Syntax

sflow collector *collector-id* [**vpn-instance** *vpn-instance-name*] { **ip** *ipv4-address* | **ipv6** *ipv6-address* } [**port** *port-number*] [**datagram-size** *size*] [**time-out** *seconds*] [**description** *string*]

undo sflow collector *collector-id*

Default

No sFlow collector information is configured.

Views

System view

Predefined user roles

network-admin

Parameters

collector-id: Specifies a sFlow collector by its ID. The value range for this argument is 1 to 10.

vpn-instance *vpn-instance-name*: Specifies a VPN instance to which the sFlow collector belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. The VPN instance name cannot contain spaces. By default, the sFlow collector belongs to the public network.

ip *ipv4-address*: Specifies an IPv4 address for the sFlow collector.

ipv6 *ipv6-address*: Specifies an IPv6 address for the sFlow collector.

port *port-number*: Specifies the UDP port number of the sFlow collector, in the range of 1 to 65535. The default is 6343.

datagram-size *size*: Specifies the maximum length of the sFlow data portion in a sFlow packet. The value range for the *size* argument is 200 to 3000 bytes, and the default value is 1400 bytes.

time-out *seconds*: Specifies the aging timer of the sFlow collector, in the range of 1 to 2147483647 seconds. When the aging timer expires, the sFlow collector settings are deleted. The sFlow collector settings do not age out by default.

description *string*: Specifies a description, a case-sensitive string of 1 to 127 characters. The default description is "CLI Collector."

Examples

Configure the following parameters for sFlow collector 2:

- **IP address**—3.3.3.1.
- **Port number**—Default.
- **Description**—netserver.
- **Aging timer**—1200 seconds.
- **Maximum length of the sFlow data portion in the sFlow packet**—1000 bytes.

```
<Switch> system-view
[Switch] sflow collector 2 ip 3.3.3.1 description netserver time-out 1200 datagram-size
1000
```

10.1.4. sflow counter collector

Use **sflow counter collector** to specify a sFlow collector for counter sampling.

Use **undo sflow counter collector** to restore the default.

Syntax

sflow counter collector *collector-id*

undo sflow counter collector

Default

No sFlow collector is specified for counter sampling.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Predefined user roles

network-admin

Parameters

collector-id: Specifies a sFlow collector by its ID. The value range for this argument is 1 to 10.

Examples

Specify sFlow collector 2 on GigabitEthernet 1/0/1 for counter sampling.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] sflow counter collector 2
```

10.1.5. sflow counter interval

Use **sflow counter interval** to enable counter sampling and set a counter sampling interval.

Use **undo sflow counter interval** to disable counter sampling.

Syntax

sflow counter interval *interval*

undo sflow counter interval

Default

Counter sampling is disabled.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Predefined user roles

network-admin

Parameters

interval: Specifies the counter sampling interval in the range of 2 to 86400 seconds.

Examples

Enable counter sampling and set the counter sampling interval to 120 seconds on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] sflow counter interval 120
```

10.1.6. sflow flow collector

Use **sflow flow collector** to specify a sFlow collector for flow sampling.

Use **undo sflow flow collector** to restore the default.

Syntax

sflow flow collector *collector-id*

undo sflow flow collector

Default

No sFlow collector is specified for flow sampling.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Predefined user roles

network-admin

Parameters

collector-id: Specifies a sFlow collector by its ID. The value range for this argument is 1 to 10.

Examples

Specify sFlow collector 2 on GigabitEthernet 1/0/1 for flow sampling.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] sflow flow collector 2
```

10.1.7. sflow flow max-header

Use **sflow flow max-header** to set the maximum number of bytes (starting from the packet header) that flow sampling can copy per packet.

Use **undo sflow flow max-header** to restore the default.

Syntax

sflow flow max-header *length*

undo sflow flow max-header

Default

Flow sampling can copy up to 128 bytes of a packet.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Predefined user roles

network-admin

Parameters

length: Specifies the maximum number of bytes that can be copied, in the range of 18 to 512. As a best practice, use the default value.

Examples

Set the maximum number of bytes to 60 for flow sampling to copy per packet on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] sflow flow max-header 60
```

10.1.8. sflow sampling-mode

Use **sflow sampling-mode** to specify a flow sampling mode.

Use **undo sflow sampling-mode** to restore the default.

Syntax

sflow sampling-mode random

undo sflow sampling-mode

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Predefined user roles

network-admin

Parameters

random: Specifies the random sampling mode. For example, if the packet sampling interval is set to 4000 (by using the **sflow sampling-rate** command), the device samples packets randomly as follows:

- The device might sample one packet from the first 4000 packets.
- The device might sample multiple packets from the next 4000 packets.
- The device might sample no packets from the third 4000 packets.

However, the device samples one packet from 4000 packets on average.

Examples

Specify random flow sampling mode on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] sflow sampling-mode random
```

Related commands

sflow sampling-rate

10.1.9. sflow sampling-rate

Use **sflow sampling-rate** to enable flow sampling and specify the number of packets out of which flow sampling will sample a packet.

Use **undo sflow sampling-rate** to disable flow sampling.

Syntax

sflow sampling-rate *rate*

undo sflow sampling-rate

Default

Flow sampling is disabled.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Predefined user roles

network-admin

Parameters

rate: Specifies the number of packets out of which flow sampling will sample a packet on the interface. The value range for this argument is 1000 to 500000. As a best practice, set the sampling interval to 2^n that is greater than or equal to 8192, for example, 32768.

Examples

Enable flow sampling to sample a packet out of 32768 packets on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] sflow sampling-rate 32768
```

Related commands

sflow sampling-mode

10.1.10. sflow source

Use **sflow source** to specify the source IP address of sent sFlow packets.

Use **undo sflow source** to restore the default.

Syntax

sflow source { **ip** *ipv4-address* | **ipv6** *ipv6-address* } *

undo sflow source { **ip** | **ipv6** } *

Default

The source IP address of sent sFlow packets is determined by routing.

Views

System view

Predefined user roles

network-admin

Parameters

ip *ipv4-address*: Specifies the source IPv4 address of sent sFlow packets.

ipv6 *ipv6-address*: Specifies the source IPv6 address of sent sFlow packets.

Examples

Specify the source IPv4 address of sent sFlow packets as 10.0.0.1.

```
<Switch> system-view
[Switch] sflow source ip 10.0.0.1
```

Contents

A page of this section is **11-x-x**

11. Information center commands 11-1
11.1. Information center commands 11-1
11.1.1. display info-center 11-1
11.1.2. display logbuffer 11-1
11.1.3. display logbuffer summary 11-3
11.1.4. display logfile summary 11-4
11.1.5. enable log updown 11-5
11.1.6. info-center enable 11-5
11.1.7. info-center logbuffer 11-6
11.1.8. info-center logbuffer size 11-6
11.1.9. info-center logfile directory 11-7
11.1.10. info-center logfile enable 11-7
11.1.11. info-center logfile frequency 11-8
11.1.12. info-center logfile size-quota 11-9
11.1.13. info-center loghost 11-9
11.1.14. info-center loghost source 11-10
11.1.15. info-center source 11-11
11.1.16. info-center synchronous 11-13
11.1.17. info-center syslog min-age 11-14
11.1.18. info-center timestamp 11-14
11.1.19. info-center timestamp loghost 11-15
11.1.20. logfile save 11-16
11.1.21. reset logbuffer 11-16
11.1.22. snmp-agent trap enable syslog 11-17
11.1.23. terminal debugging 11-17
11.1.24. terminal logging level 11-18
11.1.25. terminal monitor 11-19

11. Information center commands

11.1. Information center commands

11.1.1. display info-center

Use **display info-center** to display information center configuration.

Syntax

display info-center

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display information center configuration.

```
<Switch> display info-center
Information Center: Enabled
Console: Enabled
Monitor: Enabled
Log host: Enabled
    192.168.0.1,
    port number: 5000, host facility: local7
Log buffer: Enabled
    Max buffer size 1024, current buffer size 512,
    Current messages 0, dropped messages 0, overwritten messages 0
Log file: Enabled
Security log file: Enabled
Information timestamp format:
    Log host: Date
    Other output destination: Date
```

11.1.2. display logbuffer

Use **display logbuffer** to display the state of the log buffer and the log information in the log buffer.

Syntax

display logbuffer [**reverse**] [**level** *severity* | **size** *buffersize* | **slot** *slot-number*] *

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

reverse: Displays log entries chronologically, with the most recent entry at the top. If you do not specify this keyword, the command displays log entries chronologically, with the oldest entry at the top.

level *severity*: Specifies a severity level in the range of 0 to 7. If you do not specify a severity level, this command displays log information for all levels.

Table 11-1 Log levels

Severity value	Level	Description	Keyword in commands
0	Emergency	The system is unusable. For example, the system authorization has expired.	**emergency**
1	Alert	Action must be taken immediately. For example, traffic on an interface exceeds the upper limit.	**alert**
2	Critical	Critical condition. For example, the device temperature exceeds the upper limit, the power module fails, or the fan tray fails.	**critical**
3	Error	Error condition. For example, the link state changes.	**error**
4	Warning	Warning condition. For example, an interface is disconnected, or the memory resources are used up.	**warning**
5	Notification	Normal but significant condition. For example, a terminal logs in to the device, or the device reboots.	**notification**
6	Informational	Informational message. For example, a command or a **ping** operation is executed.	**informational**
7	Debugging	Debugging message.	**debugging**

size *buffersize*: Specifies the number of latest logs to be displayed. The value range is 1 to 1024. If you do not specify this option, the command displays all logs in the log buffer.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information for all member devices.

Examples

Display the state and log information of the log buffer.

```
<Switch> display logbuffer
Log buffer: Enabled
Max buffer size: 1024
Actual buffer size: 512
Dropped messages: 0
Overwritten messages: 718
```

```
Current messages: 512
%Jun 17 15:57:09:578 2016 Switch SYSLOG/7/SYS_RESTART:System restarted --
…
```

Table 11-2 Command output

Field	Description
Log buffer	Status of the log buffer: • **Enabled**—Logs can be output to the log buffer. • **Disabled**—Logs cannot be output to the buffer.
Max buffer size	Maximum buffer size supported by the device.
Actual buffer size	Maximum buffer size configured by using the **info-center logbuffer size** command.
Dropped messages	Number of dropped messages.
Overwritten messages	Number of overwritten messages.
Current messages	Number of current messages.

Related commands

info-center logbuffer

reset logbuffer

11.1.3. display logbuffer summary

Use **display logbuffer summary** to display the summary of the log buffer.

Syntax

display logbuffer summary [**level** *severity* | **slot** *slot-number*] *

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

level *severity*: Specifies a severity level in the range of 0 to 7. If you do not specify a severity level, this command displays log information of all levels in the log buffer. For more information about log levels, see Table 11-1 .

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information for all member devices.

Examples

Display the summary of the log buffer.

```
<Switch> display logbuffer summary
  Slot EMERG ALERT  CRIT ERROR  WARN NOTIF  INFO DEBUG
```

```
1      0      0      0      7      0      34     38     0
```

Table 11-3 Command output

Field	Description
EMERG	Represents emergency. For more information, see Table 11-1 .
ALERT	Represents alert. For more information, see Table 11-1 .
CRIT	Represents critical. For more information, see Table 11-1 .
ERROR	Represents error. For more information, see Table 11-1 .
WARN	Represents warning. For more information, see Table 11-1 .
NOTIF	Represents notification. For more information, see Table 11-1 .
INFO	Represents informational. For more information, see Table 11-1 .
DEBUG	Represents debug. For more information, see Table 11-1 .

11.1.4. display logfile summary

Use **display logfile summary** to display the log file configuration.

Syntax

display logfile summary

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display the log file configuration.

```
<Switch> display logfile summary
  Log file: Enabled.
  Log file size quota: 10 MB
  Log file directory: flash:/logfile
  Writing frequency: 24 hour 0 min 10 sec
```

Table 11-4 Command output

Field	Description
Log file	Log file status: • **Enabled**—Logs can be output to a log file. • **Disabled**—Logs cannot be output to a log file.
Log file size quota	Maximum storage space reserved for a log file, in MB.
Log file directory	Log file directory.
Writing frequency	Log file writing frequency.

11.1.5. enable log updown

Use **enable log updown** to enable an interface to generate link up or link down logs when the interface state changes.

Use **undo enable log updown** to disable an interface from generating link up or link down logs when the interface state changes.

Syntax

enable log updown

undo enable log updown

Default

All interfaces are allowed to generate link up and link down logs.

Views

Interface view

Predefined user roles

network-admin

Examples

Disable GigabitEthernet 1/0/1 from generating link up or link down logs.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] undo enable log updown
```

11.1.6. info-center enable

Use **info-center enable** to enable the information center.

Use **undo info-center enable** to disable the information center.

Syntax

info-center enable

undo info-center enable

Default

The information center is enabled.

Views

System view

Predefined user roles

network-admin

Examples

Enable the information center.

```
<Switch> system-view
[Switch] info-center enable
Information center is enabled.
```

11.1.7. info-center logbuffer

Use **info-center logbuffer** to enable log output to the log buffer.

Use **undo info-center logbuffer** to disable log output to the log buffer.

Syntax

info-center logbuffer

undo info-center logbuffer

Default

Log output to the log buffer is enabled.

Views

System view

Predefined user roles

network-admin

Examples

Enable log output to the log buffer.

```
<Switch> system-view
[Switch] info-center logbuffer
```

Related commands

display logbuffer

info-center enable

11.1.8. info-center logbuffer size

Use **info-center logbuffer size** to set the maximum number of logs that can be stored in the log buffer.

Use **undo info-center logbuffer size** to restore the default.

Syntax

info-center logbuffer size *buffersize*

undo info-center logbuffer size

Default

The log buffer can store a maximum of 512 logs.

Views

System view

Predefined user roles

network-admin

Parameters

buffersize: Specifies the maximum number of logs that can be stored in the log buffer. The value range is 0 to 1024, and the default is 512.

Examples

Set the maximum log buffer size to 50.

```
<Switch> system-view
[Switch] info-center logbuffer size 50
```

Restore the default maximum log buffer size.

```
<Switch> system-view
[Switch] undo info-center logbuffer size
```

Related commands

display logbuffer

info-center enable

11.1.9. info-center logfile directory

Use **info-center logfile directory** to specify the directory to save the log file.

Syntax

info-center logfile directory *dir-name*

Default

The log file directory is **flash:/logfile**.

Views

System view

Predefined user roles

network-admin

Parameters

dir-name: Specifies a directory by its name, a string of 1 to 64 characters.

Usage guidelines

The specified log file directory must have been created.

The log file uses the .log extension.

This command cannot survive an IRF reboot or a master/subordinate switchover.

Examples

Set the log file directory to **flash:/test**.

```
<Switch> mkdir test
Creating directory flash:/test... Done.
<Switch> system-view
[Switch] info-center logfile directory flash:/test
```

Related commands

info-center logfile enable

11.1.10. info-center logfile enable

Use **info-center logfile enable** to enable the log file feature.

Use **undo info-center logfile enable** to disable the log file feature.

Syntax

info-center logfile enable

undo info-center logfile enable

Default

The log file feature is enabled.

Views

System view

Predefined user roles

network-admin

Examples

Enable log output to the log file.

```
<Switch> system-view
[Switch] info-center logfile enable
```

11.1.11. info-center logfile frequency

Use **info-center logfile frequency** to configure the interval at which the system saves logs from the log file buffer to the log file.

Use **undo info-center logfile frequency** to restore the default.

Syntax

info-center logfile frequency *freq-sec*

undo info-center logfile frequency

Default

The log file saving interval is 86400 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

freq-sec: Specifies the log file saving interval in seconds. The value range is 1 to 86400.

Usage guidelines

This command enables the system to automatically save logs in the log file buffer to the log file at the specified interval. NEC recommends that you use this command by the default.

Examples

Set the log file saving interval to 60000 seconds.

```
<Switch> system-view
[Switch] info-center logfile frequency 60000
```

Related commands

info-center logfile enable

11.1.12. info-center logfile size-quota

Use **info-center logfile size-quota** to set the maximum size for the log file.

Use **undo info-center logfile size-quota** to restore the default.

Syntax

info-center logfile size-quota *size*

undo info-center logfile size-quota

Default

The maximum size for the log file is 10 MB.

Views

System view

Predefined user roles

network-admin

Parameters

size: Specifies the maximum size for the log file, in MB. The value range is 1 to 10.

Examples

Set the maximum size to 6 MB for the log file.

```
<Switch> system-view
[Switch] info-center logfile size-quota 6
```

Related commands

info-center logfile enable

CAUTION:
Please check whether the storage has enough space for the log file size before you use this command.

11.1.13. info-center loghost

Use **info-center loghost** to specify a log host and to configure output parameters.

Use **undo info-center loghost** to remove a log host.

Syntax

info-center loghost [**vpn-instance** *vpn-instance-name*] { *hostname* | *ipv4-address* | **ipv6** *ipv6-address* } [**port** *port-number*] [**facility** *local-number*]

undo info-center loghost [**vpn-instance** *vpn-instance-name*] { *hostname* | *ipv4-address* | **ipv6** *ipv6-address* }

Default

No log hosts are specified.

Views

System view

Predefined user roles

network-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. If the log host is on the public network, do not specify this option.

hostname: Specifies a log host by its name, a case-insensitive string of 1 to 253 characters. The host name can contain letters, digits, and special characters including hyphen (-), underscore (_), and dot (.).

ipv4-address: Specifies a log host by its IPv4 address.

ipv6 *ipv6-address*: Specifies a log host by its IPv6 address.

port *port-number*: Specifies the port number of the log host, in the range of 1 to 65535. The default is 514. It must be the same as the value configured on the log host. Otherwise, logs cannot be sent to the log host.

facility *local-number*: Specifies a logging facility from local0 to local7 for the log host. The default value is local7. Logging facilities are used to mark different logging sources, and query and filer logs.

Usage guidelines

The **info-center loghost** command takes effect only after the information center is enabled by using **info-center enable** command.

Examples

Output logs to the log host at 1.1.1.1.

```
<Switch> system-view
[Switch] info-center loghost 1.1.1.1
```

11.1.14. info-center loghost source

Use **info-center loghost source** to specify a source IP address for logs sent to log hosts.

Use **undo info-center loghost source** to restore the default.

Syntax

info-center loghost source *interface-type interface-number*

undo info-center loghost source

Default

The source IP address of logs sent to log hosts is the primary IP address of the outgoing interface.

Views

System view

Predefined user roles

network-admin

Parameters

interface-type interface-number: Specifies an interface by its type and number.

Usage guidelines

The system uses the primary IP address of the specified interface as the source IP address of the logs sent to log hosts.

The **info-center loghost source** command takes effect only after the information center is enabled by using **info-center enable** command.

Examples

Use the IP address of interface Loopback 0 as the source IP address of the logs sent to log hosts.

```
<Switch> system-view
[Switch] interface loopback 0
[Switch-LoopBack0] ip address 2.2.2.2 32
[Switch-LoopBack0] quit
[Switch] info-center loghost source loopback 0
```

11.1.15. info-center source

Use **info-center source** to configure a log output rule for a module.

Use **undo info-center source** to restore the default.

Syntax

info-center source { *module-name* | **default** } { **console** | **logbuffer** | **logfile** | **loghost** | **monitor** } { **deny** | **level** *severity* }

undo info-center source { *module-name* | **default** } { **console** | **logbuffer** | **logfile** | **loghost** | **monitor** }

Default

Table 11-5 lists the default log output rules.

Table 11-5 Default output rules

Destination	Source modules	Common log	Security log	Diagnostic log	Hidden log
Console	All supported modules	debugging	Disabled	Disabled	Disabled
Monitor terminal	All supported modules	debugging	Disabled	Disabled	Disabled
Log host	All supported modules	informational	Disabled	Disabled	informational
Log buffer	All supported modules	informational	Disabled	Disabled	informational
Log file	All supported	informational	Disabled	Disabled	informational

Destination	Source modules	Common log	Security log	Diagnostic log	Hidden log
	modules				
Security log file	All supported modules, cannot be filtered	Disabled	Debugging, which cannot be filtered	Disabled	Disabled
Diagnostic log file	All supported modules, cannot be filtered	Disabled	Disabled	Debugging, which cannot be filtered	Disabled

Views

System view

Predefined user roles

network-admin

Parameters

module-name: Specifies a module by its name. You can use the **info-center source ?** command to view the modules supported by the device.

default: Specifies all supported modules.

console: Outputs logs to the console.

logbuffer: Outputs logs to the log buffer.

logfile: Outputs logs to the log file.

loghost: Outputs logs to the log host.

monitor: Outputs logs to the monitor terminal.

deny: Disables log output.

level *severity*: Specifies a severity level in the range of 0 to 7. The smaller the severity value, the higher the severity level. See Table 11-1 for more information. Logs at the specified severity level and higher levels are allowed or denied to be output.

Usage guidelines

If you do not set an output rule for a module, the module uses the output rule set by using the **default** keyword. If no rule is set by using the **default** keyword, the module uses the default output rule.

To modify or remove an output rule set for a module, you must use the *module-name* argument. A new output rule configured by using the **default** keyword does not take effect on the module.

If you execute this command for a module multiple times, the most recent configuration takes effect.

If you execute this command for the **default** modules multiple times, the most recent configuration takes effect.

Examples

Output only VLAN module's information with the emergency level to the console.

```
<Switch> system-view
[Switch] info-center source default console deny
[Switch] info-center source vlan console level emergency
```

Based on the previous configuration, disable output of VLAN module's information to the console so no system information is output to the console.

```
<Switch> system-view
[Switch] undo info-center source vlan console
```

11.1.16. info-center synchronous

Use **info-center synchronous** to enable synchronous information output.

Use **undo info-center synchronous** to disable synchronous information output.

Syntax

info-center synchronous

undo info-center synchronous

Default

Synchronous information output is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

System log output interrupts ongoing configuration operations, including obscuring previously entered commands. Synchronous information output shows the obscured commands. It also provides a command prompt in command editing mode, or a [Y/N] string in interaction mode so you can continue your operation from where you were stopped.

Examples

Enable synchronous information output, and then execute the **display current-configuration** command to view the current configuration of the device.

```
<Switch> system-view
[Switch] info-center synchronous
Info-center synchronous output is on
[Switch] display current-
```

At this time, the system receives log information. It displays the log information first, and then displays your previous input, which is **display current-** in this example.

```
%May 21 14:33:19:425 2007 Switch SHELL/4/LOGIN: VTY login from 192.168.1.44
[Switch] display current-
```

Enter **configuration** to complete the **display current-configuration** command, and press the **Enter** key to execute the command.

Enable synchronous information output, and then save the current configuration (enter interactive information).

```
<Switch> system-view
```

```
[Switch] info-center synchronous
Info-center synchronous output is on
[Switch] save
The current configuration will be written to the device. Are you sure? [Y/N]:
```

At this time, the system receives the log information. It displays the log information first and then displays [Y/N].

```
%May 21 14:33:19:425 2007 Switch SHELL/4/LOGIN: VTY login from 192.168.1.44
[Y/N]:
```

Enter **Y** or **N** to complete your input.

11.1.17. info-center syslog min-age

Use **info-center syslog min-age** to set the minimum storage period for logs in the log buffer and log file.

Use **undo info-center syslog min-age** to restore the default.

Syntax

info-center syslog min-age *min-age*

undo info-center syslog min-age

Default

The log minimum storage period is not set.

Views

System view

Predefined user roles

network-admin

Parameters

min-age: Sets the minimum storage period in hours. The value range is 1 to 8760.

Examples

Set the log minimum storage period to 168 hours.

```
<Switch> system-view
[Switch] info-center syslog min-age 168
```

11.1.18. info-center timestamp

Use **info-center timestamp** to set the timestamp format for logs sent to the console, monitor terminal, log buffer, and log file.

Use **undo info-center timestamp** to restore the default.

Syntax

info-center timestamp { **boot** | **date** | **none** }

undo info-center timestamp

Default

The timestamp format for logs sent to the console, monitor terminal, log buffer, and log file is **date**.

Views

System view

Predefined user roles

network-admin

Parameters

boot: Sets the timestamp format to xxx.yyy, where xxx is the most significant 32 bits (in milliseconds) and yyy is the least significant 32 bits. For example, 0.21990989 equals Jun 25 14:09:26:881 2007. The **boot** time shows the time since system startup.

date: Sets the timestamp format to MMM DD hh:mm:ss:xxx YYYY, such as Dec 8 10:12:21:708 2007. The **date** time shows the current system time.

- MMM: Abbreviations of the months in English, which could be Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, or Dec.
- DD: Date, starting with a space if it is less than 10, for example " 7".
- hh:mm:ss:xxx: Local time, with hh in the range of 00 to 23, mm and ss in the range of 00 to 59, and xxx in the range of 0 to 999.
- YYYY: Year.

none: Indicates no time information is provided.

Examples

Set the timestamp format to **boot** for logs sent to the console, monitor terminal, log buffer, and log file.

```
<Switch> system-view
[Switch] info-center timestamp boot
```

Related commands

info-center timestamp loghost

11.1.19. info-center timestamp loghost

Use **info-center timestamp loghost** to set the timestamp format for logs sent to log hosts.

Use **undo info-center timestamp loghost** to restore the default.

Syntax

info-center timestamp loghost { **date** | **iso** | **no-year-date** | **none** }

undo info-center timestamp loghost

Default

The timestamp format for logs sent to log hosts is **date**.

Views

System view

Predefined user roles

network-admin

Parameters

date: Sets the timestamp format to mmm dd hh:mm:ss yyyy, such as Dec 8 10:12:21 2007. The **date** time shows the current system time.

iso: Sets the ISO 8601 timestamp format, for example, 2009-09-21T15:32:55.

no-year-date: Sets the timestamp format to the current system date and time without year.

none: Indicates that no timestamp information is provided.

Examples

Set the timestamp format to **no-year-date** for logs sent to log hosts.

```
<Switch> system-view
[Switch] info-center timestamp loghost no-year-date
```

Related commands

info-center timestamp

11.1.20. logfile save

Use **logfile save** to manually save logs in the log file buffer to the log file.

Syntax

logfile save

Views

Any view

Predefined user roles

network-admin

Usage guidelines

You can specify the directory to save the log file by using the **info-center logfile directory** command.

The system clears the log file buffer after saving the buffered logs to the log file automatically or manually.

If the log file buffer is empty, this command displays a success message event though no logs are saved to the log file.

Examples

Manually save logs from the log file buffer to a log file.

```
<Switch> logfile save
The contents in the log file buffer have been saved to the file flash:/logfile/logfile.log.
```

Related commands

info-center logfile enable

info-center logfile directory

11.1.21. reset logbuffer

Use **reset logbuffer** to clear the log buffer.

Syntax

reset logbuffer

Views

User view

Predefined user roles

network-admin

Examples

Clear the log buffer.

```
<Switch> reset logbuffer
```

Related commands

display logbuffer

11.1.22. snmp-agent trap enable syslog

Use **snmp-agent trap enable syslog** to enable SNMP notifications for log messages.

Use **undo snmp-agent trap enable syslog** to disable SNMP notifications for log messages.

Syntax

snmp-agent trap enable syslog

undo snmp-agent trap enable syslog

Default

The device does not send SNMP notifications for log messages.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command enables the device to send an SNMP notification for each log message it outputs. The device encapsulates logs in SNMP notifications and then sends them to the SNMP module and the log trap buffer.

For the SNMP module to send the received SNMP notifications correctly, you must also configure SNMP on the device. For more information about SNMP configuration, see the network management and monitoring configuration guide for the device.

To view the traps in the log trap buffer, access the MIB corresponding to the log trap buffer. The log trap buffer size can be set by using the **info-center syslog trap buffersize** command.

Examples

Enable the device to send SNMP notifications for log messages.

```
<Switch> system-view
[Switch] snmp-agent trap enable syslog
```

Related commands

info-center syslog trap buffersize

11.1.23. terminal debugging

Use **terminal debugging** to enable display of debug information on the current terminal.

Use **undo terminal debugging** to disable display of debug information on the current terminal.

Syntax

terminal debugging

undo terminal debugging

Default

Display of debug information is disabled on the current terminal.

Views

User view

Predefined user roles

network-admin

Usage guidelines

To enable display of debug information on the console, perform the following tasks:

1. Execute the **terminal debugging** command.
2. Enable the information center. The information center is enabled by default.
3. Use a debugging command to enable the related debugging.

To enable display of debug information on the current terminal, perform the following tasks:

1. Execute the **terminal monitor** and **terminal debugging** commands.
2. Enable the information center. The information center is enabled by default.
3. Use a debugging command to enable the related debugging.

This command takes effect only for the current connection between the terminal and the device. If a new connection is established, the default is restored.

You can also enable display of debug information on the current terminal by executing the **terminal logging level 7** command. This command has the following differences from the **terminal debugging** command:

- The **terminal logging level 7** command enables log display for all levels (levels **0** through **7**) on the current terminal.
- The **terminal debugging** command only enables display of logs with the following severity levels:
  - Debug level (level **7**).
  - Severity level higher than or equal to the level specified in the **terminal logging level** command.

Examples

Enable display of debug information on the current terminal.

```
<Switch> terminal debugging
The current terminal is enabled to display debugging information.
```

Related commands

terminal logging level

terminal monitor

11.1.24. terminal logging level

Use **terminal logging level** to set the lowest level of logs that can be output to the current terminal.

Use **undo terminal logging level** to restore the default.

Syntax

terminal logging level *severity*

undo terminal logging level

Default

The lowest level of logs that can be output to the current terminal is 6 (Informational).

Views

User view

Predefined user roles

network-admin

Parameters

severity: Specifies a log severity level. Valid values are alert, critical, debugging, emergency, error, informational, notification, warning, and digits from 0 to 7.

Usage guidelines

This command enables the device to output logs with a severity level higher than or equal to the specified level to the current terminal. For example, if you set the *severity* argument to 6, logs with a severity value from 0 to 6 are output to the current terminal.

This command takes effect only for the current connection between the terminal and the device. If a new connection is established, the default is restored.

Examples

Configure the device to output logs with the debugging level and higher levels to the current terminal.

```
<Switch> terminal logging level 7
```

11.1.25. terminal monitor

Use **terminal monitor** to enable monitoring of logs on the current terminal.

Use **undo terminal monitor** to disable monitoring of logs on the current terminal.

Syntax

terminal monitor

undo terminal monitor

Default

Monitoring of logs is enabled on the console and disabled on the monitor terminal.

Views

User view

Predefined user roles

network-admin

Usage guidelines

This command takes effect only for the current connection between the terminal and the device. If a new connection is established, the default is restored.

Examples

Enable monitoring of logs on the current terminal.

```
<Switch> terminal monitor
The current terminal is enabled to display logs.
```

Contents

A page of this section is **11-x-x**

12. NetMeister commands ····· 12-1
12.1. NetMeister commands ····· 12-1
12.1.1. display netmeister ····· 12-1
12.1.2. netmeister account ····· 12-2
12.1.3. netmeister enable ····· 12-3
12.1.4. netmeister event log enable ····· 12-4
12.1.5. netmeister event syslog enable ····· 12-5
12.1.6. netmeister management ip ····· 12-6
12.1.7. netmeister parent ip ····· 12-6
12.1.8. netmeister proxy ····· 12-7
12.1.9. display netmeister parent-mode statistics ····· 12-8
12.1.10. netmeister mode parent ····· 12-12
12.1.11. netmeister parent-mode sitename ····· 12-13
12.1.12. netmeister parent-mode mqtt port ····· 12-13
12.1.13. reset netmeister parent-mode statistics ····· 12-14
12.1.14. netmeister ngn enable ····· 12-15

12. NetMeister commands

12.1. NetMeister commands

12.1.1. display netmeister

Use **display netmeister** to display NetMeister information.

Syntax

display netmeister

Views

Any view

Predefined user roles

network-admin

Examples

Display NetMeister information.

```
<Sysname> display netmeister
NetMeister state                                  : Enabled
Connection state with NetMeister                : Connected
Account name                                      : nec
Proxy information:
  State                                        : Connected
  URL                                          : http://www.abc.com:80
  Username                                    : admin

Parent 1:
  IP address                                       : 192.168.0.254
  Port number                                      : 443
  Connection state                                : Connected
Parent 2:
  IP address                                       : 192.168.0.255
  Port number                                      : 8443
  Connection state                                : Connected
```

Figure 12-1 Command Output

Field	Description
NetMeister state	• Enabled. • Disabled.
Connection state with NetMeister	• Connected. • Disconnected.
Account name	GroupID of the child device.
Proxy information	Information about connecting to the NetMeister proxy server.

Field	Description
IP address	IP address of the parent device.
Port number	Port number of the parent.
Connection state	State of the connection between the child device and parent device. Options include: • Connected. • Disconnected.
Parent information	Parent device information.
Site name	Name of the site to which the parent device belongs. If no site name is configured, this field displays **--**.
Interval	Interval (in seconds) at which the parent device sends registration packets and update packets to the cloud platform. If the device fails to obtain the interval, this field displays **--**.
MQTT interval	MQTT heartbeat interval in seconds. If the device fails to obtain the interval, this field displays **--**.
MQTT status	MQTT connection state. If no MQTT connection has ever been established, this field displays **--**.
NGN status	Status of NGN. Options include: • Enabled • Disabled

Related commands

netmeister account

netmeister enable

netmeister parent

12.1.2. netmeister account

Use **netmeister account** to specify the GroupID and password used by the child device in authentication and registration.

Use **undo netmeister account** to delete the specified GroupID and password.

Syntax

netmeister account *account* **password { cipher** *cipherPassword* **| simple** *plainPassword* **}**

undo netmeister account

Default

No GroupID and password is specified for the authentication and registration of a child device.

Views

System view

Predefined user roles

network-admin

Parameters

account: Specifies the GroupID, a string of 2 to 31 characters. The string can only contain lower-case letters, digits, and hyphens (-), and cannot start or end with hyphens (-).

password: Specifies the password.

cipher: Sets a password in encrypted form.

cipherPassword: Specifies an encrypted-form password, a string of 41 to 73 characters.

simple: Sets a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

plainPassword: Specifies a plaintext-form password, a string of 8 to 31 characters. The string can contain only letters, digits, and the following special characters: !#$%&'()*+,-./:;<=>@[]^_`{|}~. The string must contain a minimum of one letter and one digit.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect. Every execution will trigger the child device to disconnect from and then reconnect to the NetMeister platform with the newly specified GroupID and password.

To avoid configuration failure, make sure NetMeister is disabled on the device before you specify the GroupID and password.

Make sure the specified GroupID and password already exist on the NetMeister platform.

Make sure that the specified GroupID and password are also used on the parent device.

The username and password specified on the device must be the same as those configured on the parent device and NetMeister.

Examples

Configure the child device to use GroupID **nec** and plaintext-form password **nec1234** in authentication and registration.

```
<Sysname> system-view
[Sysname] netmeister account nec password simple nec1234
```

Related commands

netmeister enable

display netmeister

12.1.3. netmeister enable

Use **netmeister enable** to enable NetMeister.

Use **undo netmeister enable** to disable NetMeister.

Syntax

netmeister enable

undo netmeister enable

Default

NetMeister is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This feature enables a device to act as a child device in a NetMeister network.

- Before you enable this feature, configure the required settings on the child device, parent device, and NetMeister.
- After you enable this feature, only parent device related settings take effect in parent mode, and only child device related settings take effect in child mode.

Examples

Enable NetMeister.

```
<Sysname> system-view
[Sysname] netmeister enable
```

12.1.4. netmeister event log enable

Use `netmeister event log enable` to enable reporting of client connection failure events to NetMeister.

Use `undo netmeister event log enable` to disable reporting of client connection failure events to NetMeister.

Syntax

`netmeister event log enable`

`undo netmeister event log enable`

Default

Enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

When NetMeister is enabled, this command causes the device reportsto report client connection failure events to NetMeister atevery five-minute intervals. An event is minutes. Events are generated when a client fails to connect during the association phase or authentication phase.

You can configure thisThis command whencan be configured while NetMeister is enabled.

Examples

Disable reporting of client connection failure events.

```
<system> system-view
[system] undo netmeister event log enable
```

Related commands

netmeister enable

12.1.5. netmeister event syslog enable

🕮 memo:

This command is supported in software version 7.4.48 and later. It is automatically enabled after an upgrade to a supported version.

Use `netmeister event syslog enable` to enable reporting of logbuffer messages to NetMeister as event logs.

Use `undo netmeister event syslog enable` to disable reporting of logbuffer messages to NetMeister as event logs.

Syntax

netmeister event syslog enable

undo netmeister event syslog enable

Default

Enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

When NetMeister is enabled, this command causes the device reportsto report log messages stored in the logbuffer to NetMeister as event logs atevery five-minute intervals minutes.

You can configure thisThis command whencan be configured while NetMeister is enabled.

The device reportsBecause only log messages stored inoutput to the logbuffer. If are reported, messages from a specific module are not reported if logbuffer output for athat module is disabled by using the following command, messages from that module are not reported:

info-center source module-name logbuffer deny

For more information about the Information Center, see **“"**Information Center**”"** in Section 10, System Management.

Examples

Disable reporting of logbuffer messages as event logs.

```
<system> system-view
[system] undo netmeister event syslog enable
```

Related commands

netmeister enable

info-center source

12.1.6. netmeister management ip

Syntax

netmeister management ip *ip-address*

undo netmeister management ip

Default

disabled.

View

System-view

Predefined user roles

network-admin

Usage guidelines

Use the **netmeister management ip** command to set the management IP address to be displayed in the NetMeister function [Log in remotely with a closed network].

Restore the defaults by **undo netmeister management ip** command.

For more information on NetMeister features, see the NetMeister operating guide.

Examples

Set the management IP address displayed in the NetMeister function [Log in remotely with a closed network] to 10.1.1.10.

```
<Sysname> system-view
[Sysname] netmeister management ip 10.1.1.10
```

🕮 Memo:
netmeister management ip command is supported from later software, including Version 7.4.30.

12.1.7. netmeister parent ip

Use **netmeister parent** to specify the IP address and port number of a parent for the child device.

Use **undo netmeister parent** to delete the IP address and port number of a parent.

Syntax

netmeister parent ip *ip-address* **[port** *port-number* **]**

undo netmeister parent ip *ip-address*

Default

No parent is specified for a child device.

Views

System view

Predefined user roles

network-admin

Parameters

ip *ip-address*: Specifies the IP address of a parent.

port *port-number*: Specifies the port number of the parent, in the range of 1 to 65535. The default port number is 443.

Usage guidelines

To avoid configuration failure, make sure NetMeister is disabled on the device before you specify the IP address and port number of a parent.

After a parent and account are specified and Netmeister is enabled, the child device sends authentication requests to the parent at specific intervals until receiving an authentication response. If you execute this command multiple times, the child device sends requests to all the specified addresses and establishes connections with all the possible parents. This improves network availability by preventing parent failure from causing service interruption. Two parent IP addresses can be configured.

Examples

Specify a parent with IP address 192.168.0.254 and port number 443 for the child device.

```
<Sysname> system-view
[Sysname] netmeister parent ip 192.168.0.254 port 443
```

Specify a parent with IP address 192.168.1.254 for the child device.

```
<Sysname> system-view
[Sysname] netmeister parent ip 192.168.1.254
```

Related commands

netmeister enable

display netmeister

12.1.8. netmeister proxy

🕮 memo:
The **netmeister proxy** command is supported from version 7.2.23 and later software.

Use **netmeister proxy** to specify the proxy over which https communication to NetMiester is routed.

Use **undo netmeister proxy** to delete the proxy.

Syntax

netmeister proxy url *url* [**username** *username* **password** { **cipher | simple** } *string*]

undo netmeister proxy

Default

No netmeister proxy is specified..

Views

System view

Predefined user roles

network-admin

Parameters

url *url*: Specifies the URL of the proxy server. The http://<domain>:<port> format specifies a case-sensitive string of 8 to 128 characters. The <domain> argument represents the domain name or IP address of the proxy server, and the <port> argument represents a port number between 1 and 65535. The default port number is 80.

username *username*: Specifies the user name used to access the proxy server. 1 to 31 case-sensitive characters. Strings may contain backslashes (\), quotation marks ("), and question marks (?), cannot contain spaces.

password: Specifies the password used to access the proxy server.

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 31 characters. Its encrypted form is a case-sensitive string of 33 to 73 characters. Strings cannot include backslashes (\), quotation marks ("), question marks (?), and spaces.

Usage guidelines

The netmeister proxy command causes the device to use the specified proxy server for https communication to NetMeister. No proxy server is used for https communication to the parent. Use undo netmeister proxy to remove the proxy server designation.

Before configuring the netmeister proxy command, make sure that netmeister enable is disabled.

If you run the netmeister proxy multiple times, the latest configuration takes effect.

Examples

Specify a parent with IP address 192.168.0.254 and proxy server with IP address 10.1.1.254 for the child device.

```
<Switch> system-view
[Switch] netmeister parent ip 192.168.1.254
[Switch] netmeister proxy url http://10.1.1.254:8080
```

Related commands

netmeister enable

display netmeister

12.1.9. display netmeister parent-mode statistics

memo:
The **display netmeister parent-mode statistics** command is supported from version 7.4.35 and later software.

Use **display netmeister parent-mode statistics** to display statistics for messages transmitted between the parent device and NetMeister.

Syntax

display netmeister parent-mode statistics [**failed**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

failed: Displays statistics for messages that failed to be sent between the parent device and NetMeister in chorological order. The system can display a maximum of 5 most recent messages. If you do not specify this keyword, this command displays statistics for all messages between the parent device and NetMeister.

Examples

Display statistics for messages between the parent device and NetMeister.

```
<Sysname> display netmeister parent-mode statistics
Tasks and registration:
 145 total, 138 succeeded, 7 failed
 7 connection errors, 0 internal errors
MQTT:
 35 total, 34 succeeded, 1 failed
 1 connection errors, 0 internal errors
Alarm:
 10 occurred, 8 succeeded, 2 failed
 7 recovered, 7 succeeded
Report:
 10 total, 9 succeeded, 1 failed
```

Table 1 Command output

Field	Description
Tasks and registration	Statistics for task and registration messages.
total	Total number of messages.
succeeded	Number of messages that were successfully processed.
failed	Number of messages that failed to be processed.
connection errors	Number of connection error messages among all messages that failed to be processed.
internal errors	Number of internal error messages among all messages that failed to be processed.
MQTT	Statistics for MQTT messages.
Alarm	Statistics for alarm messages.
occurred	Number of messages when an alarm was triggered.
recovered	Number of messages when an alarm was cleared.
Report	Statistics of periodically reported messages.

Display statistics for messages that failed to be sent between the parent device and NetMeister.

```
<Sysname> display netmeister parent-mode statistics failed
```

```
Tasks and registration:
 Count: 1
  Type: register
  HTTP error code:503
  Inner error code:--
  Time: 2021/12/06 14:00
MQTT:
 Count: 1
  Type: subscribe
  HTTP error code:400
  Inner error code:--
  Time: 2021/12/06 15:10
Alarm:
 Count: 1
  Type: cpu
  HTTP error code:400
  Inner error code:--
  Time: 2021/12/06 15:00
Report:
 Count: 1
  Type: report
  HTTP error code:400
  Inner error code:--
  Time: 2021/12/07 15:00
 Count: 2
  Type: report
  HTTP error code:400
  Inner error code:--
  Time: 2021/12/07 15:30
```

Table 2 Command output

Field	Description
Tasks and registration	Statistics for task and registration messages that failed to be processed.
Count	Serial number of messages that failed to be processed.
Type	Type of task and registration messages. Options include: • **register**—Registration message. • **update**—Update message. • **get task**—Task obtaining message. • **update firmware**—Task of firmware update. • **acquire collective information of equipment**—Task of viewing device collective information. • **get running config**—Task of viewing device effective configuration. • **get config**—Task of viewing device running configuration and the startup file for next start. • **get device list**—Task of viewing the device list. • **get tab information**—Task of viewing the effective

Field	Description
	configuration for port and VLAN modules. • **execution display command**—Task of displaying device information. • **set device list**—Task of configuring device list. • **execution setting command**—Task of configuring device information. • **apply config**—Task of configuring the startup file for next start. • **save**—Task of saving the configuration to the startup file for next start. • **reboot**—Task of restarting the device. • **new certificate**—Task of obtaining a new certificate. • **task result**—Task result each time.
HTTP error code	HTTP message error code. Options include: • **1000**—Failed to send the message. • **1001**—Message sent successfully but no response. • **1002**—Invalid contents for MQTT packets. • **200**—Connected successfully but internal processing errors occurred for the device. • **400**—Request error. • **401**—Authentication failed. • **403**—Messages are banned. • **404**—Messages not detected. • **405**—Invalid method. • **406**—Messages denied. • **409**—Message conflict. • **429**—Too many requests. • **500**—Server error. • **502**—Incorrect gateway. • **503**—Service unavailable.
Inner error code	Error code for device internal message. Options include: • **1000**—Failed to send the message. • **1001**—Message sent successfully but no response. • **1002**—Invalid contents for MQTT packets. • **1003**—Client internal error. • **1004**—Unknown client error such as unrecognized error code returned by the service endpoint.
Time	Time when the message is generated.
MQTT	Statistics of MQTT messages that failed to be processed.
Type	MQTT event type. Options include: • **subscribe**—Subscription event. • **unsubscribe**—Unsubscription event. • **publish**—Publishing event. • **keepalive**—Heartbeat event. • **Connect**—Connection event. • **Disconnect**—Disconnection event.
Alarm	Statistics of alarm messages that failed to be processed.
Type	Alarm type. Options include:

Field	Description
	• **cpu**—Processor usage ratio alarm. • **Fan**—Fan alarm. • **Temperature**—Temperature alarm. • **memory**—Memory usage ratio alarm. • **reboot**—Restart exception alarm.
Report	Statistics of periodically reported messages that fail to be processed.
Type	Reported message type. This field displays **report**, which indicates the information of processor usage ratio, temperature, memory usage ratio, and port that the device reports to the cloud platform at intervals of 5 minutes.

Related commands

reset netmeister parent-mode statistics

12.1.10. netmeister mode parent

🕮 memo:
The **netmeister mode parent** command is supported from version 7.4.35 and later software.

Use **netmeister mode parent** to specify the device mode as parent mode.

Use **undo netmeister mode parent** to restore the default.

Syntax

netmeister mode parent

undo netmeister mode parent

Default

The device is in child mode.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This feature enables the device to function as the parent device that connects child devices to NetMeister.

A NetMeister network must include the following roles:

- **Child**—Device to be managed.
- **Parent**—Device that connects all child devices to NetMeister. The parent device authenticates child devices and issues NetMeister messages to authenticated child devices.
- **NetMeister**—Cloud platform for network administrators to manage and maintain child devices from the parent device.

Examples

Specify the device mode as parent mode.

```
<Sysname> system-view
[Sysname] netmeister mode parent
```

12.1.11. netmeister parent-mode sitename

🕮 memo:
The **netmeister parent-mode sitename** command is supported from version 7.4.35 and later software.

Use **netmeister parent-mode sitename** to specify the parent site name.

Use **undo netmeister parent-mode sitename** to restore the default.

Syntax

netmeister parent-mode sitename *name*

undo netmeister parent-mode sitename

Default

No parent site name is specified.

Views

System view

Predefined user roles

network-admin

Parameters

name: Specifies the parent site name, a string of 2 to 31 characters. Only lowercase letters, digits, and hyphens (-) are allowed, and the string cannot start or end with a hyphen.

Usage guidelines

For the parent device, you must specify the parent site name before you enable NetMeister.

Examples

Specify the parent site name as **qx-devel**.

```
<Sysname> system-view
[Sysname] netmeister parent-mode sitename qx-devel
```

Related commands

display netmeister

12.1.12. netmeister parent-mode mqtt port

🕮 memo:
The **netmeister parent-mode mqtt port** command is supported from version 7.4.35 and later software.

Use **netmeister parent-mode mqtt port** to specify the MQTT port number.

Use **undo netmeister parent-mode mqtt port** to restore the default.

Syntax

netmeister parent-mode mqtt port *port-number*

undo netmeister parent-mode mqtt port

Default

The MQTT port number is 8883.

Views

System view

Predefined user roles

network-admin

Parameters

port-number: Specifies the MQTT port number. Options include 443 and 8883.

Usage guidelines

The parent device and NetMeister use Message Queuing Telemetry Transport (MQTT) as the transport protocol to communicate with each other. NetMeister uses the MQTT protocol to deploy events to the parent device, and the parent device uses the MQTT protocol to subscribe to events from NetMeister.

This configuration terminates the session between the parent device and NetMeister. The device then uses the newly specified port to re-establish a connection to the NetMeister platform.

This command takes effect only when NetMeister is enabled.

Examples

Specify the MQTT port number 443 for the parent device.

```
<Sysname> system-view
[Sysname] netmeister parent-mode mqtt port 443
```

Related commands

display netmeister

12.1.13. reset netmeister parent-mode statistics

memo:
The **reset netmeister parent-mode statistics** command is supported from version 7.4.35 and later software.

Use **reset netmeister parent-mode statistic** to clear statistics for messages between the parent device and NetMeister.

Syntax

reset netmeister parent-mode statistic

Views

User view

Predefined user roles

network-admin

Examples

Clear statistics for messages between the parent device and NetMeister.

```
<Sysname> reset netmeister parent-mode statistics
```

Related commands

display netmeister parent-mode statistics

12.1.14. netmeister ngn enable

memo:
The **netmeister ngn enable** command is supported from version 7.4.48 and later software.

Use **netmeister ngn enable** to enable NGN.

Use **undo netmeister ngn enable** to disable NGN.

Syntax

netmeister ngn enable

undo netmeister ngn enable

Views

System view

Predefined user roles

network-admin

Examples

Execute this command on only child devices.

Next Generation Network (NGN) is a comprehensive open network architecture based on packet-switched technology to integrate voice, data, and multimedia services.

With this feature enabled, authentication packets sent by a child device to the parent device carry the NGN-related information. Some subsequent services will use that information for special processing.

Related commands

Enable NGN.

```
<Sysname> system-view
[Sysname] netmeister ngn enable
```

Contents

A page of this section is **11-x-x**

13. VCF fabric commands ····· 13-1
13.1. VCF fabric commands ····· 13-1
13.1.1. vcf-fabric topology enable ····· 13-1
13.1.2. vcf-fabric underlay autoconfigure ····· 13-1

13. VCF fabric commands

13.1. VCF fabric commands

13.1.1. vcf-fabric topology enable

Use **vcf-fabric topology enable** to enable VCF fabric topology discovery.

Use **undo vcf-fabric topology enable** to disable VCF fabric topology discovery.

Syntax

vcf-fabric topology enable

undo vcf-fabric topology enable

Default

VCF fabric topology discovery is disabled.

Views

System view

Predefined user roles

network-admin

Examples

Enable VCF fabric topology discovery.

```
<Switch> system-view
[Switch] vcf-fabric topology enable
```

NOTE:

The **vcf-fabric topology enable** command are only supported when used in combination with UNIVERGE Network Operation Engine Overlay Network Extension.

13.1.2. vcf-fabric underlay autoconfigure

Use **vcf-fabric underlay autoconfigure** to specify the template file for automated underlay network deployment.

Use **undo vcf-fabric underlay autoconfigure** to restore the default.

Syntax

vcf-fabric underlay autoconfigure *template*

undo vcf-fabric underlay autoconfigure

Default

No template file is specified for automated underlay network deployment.

Views

System view

Predefined user roles

network-admin

Parameters

template: Specifies a template file by its name, a case-insensitive string of 1 to 127 characters. A template file is a file ending with the **.template** file extension.

Usage guidelines

After this command is executed, the device uses the specified template file to deploy the underlay network.

Examples

Specify template file **vxlan_leaf.template** for automated underlay network deployment.

```
<Switch> system-view
[Switch] vcf-fabric underlay autoconfigure vxlan_leaf.template
```

NOTE:

The **vcf-fabric underlay autoconfigure** command are only supported when used in combination with UNIVERGE Network Operation Engine Overlay Network Extension.

QX-S5600G Series Ethernet Switches

Command References

12.OpenFlow

This manual is including the following chapters.

01-OpenFlow commands

Contents

A page of this section is **12-x-x**

1. OpenFlow commands ····· 1-1

1. OpenFlow commands

About OpenFlow commands, see "*QX シリーズ Ethernet スイッチ OpenFlow コマンドマニュアル*" (Japanese).

NOTE:

QX-S5600G Series only supports the following commands.

- active instance
- classification global
- controller address
- default table-miss permit
- description
- flow-table
- openflow instance
- tcp dscp

QX-S5600G Series Ethernet Switches

Command References

13. VXLAN

This manual is including the following chapters.

01-VXLAN commands

Contents

A page of this section is **13-x-x**

1. VXLAN commands 1-1
1.1. Basic VXLAN commands 1-1
1.1.1. ac statistics enable 1-1
1.1.2. arp suppression enable 1-1
1.1.3. arp suppression ip-source-binding record 1-2
1.1.4. description 1-3
1.1.5. display arp suppression vsi 1-3
1.1.6. display ipv6 nd suppression vsi 1-4
1.1.7. display l2vpn mac-address 1-5
1.1.8. display l2vpn service-instance 1-8
1.1.9. display l2vpn vsi 1-10
1.1.10. display vxlan tunnel 1-13
1.1.11. encapsulation 1-14
1.1.12. flooding disable 1-15
1.1.13. ipv6 nd suppression enable 1-16
1.1.14. ipv6 nd suppression notify-ipsg 1-17
1.1.15. l2vpn enable 1-17
1.1.16. l2vpn statistics interval 1-18
1.1.17. mac-address static vsi 1-18
1.1.18. reserved vxlan 1-19
1.1.19. reset arp suppression vsi 1-20
1.1.20. reset ipv6 nd suppression vsi 1-20
1.1.21. reset l2vpn mac-address 1-21
1.1.22. reset l2vpn statistics ac 1-21
1.1.23. service-instance 1-22
1.1.24. shutdown 1-23
1.1.25. statistics enable (Ethernet service instance view) 1-23
1.1.26. statistics enable (VSI view) 1-24
1.1.27. tunnel 1-25
1.1.28. tunnel global source-address 1-26
1.1.29. vsi 1-26
1.1.30. vxlan 1-27
1.1.31. vxlan default-decapsulation 1-28
1.1.32. vxlan ip-forwarding 1-28
1.1.33. vxlan local-mac report 1-29
1.1.34. vxlan tunnel mac-learning disable 1-30
1.1.35. vxlan udp-port 1-30
1.1.36. vxlan vlan-based 1-31
1.1.37. vxlan vni 1-32
1.1.38. xconnect vsi 1-32
1.2. VXLAN IP gateway commands 1-34
1.2.1. arp distributed-gateway dynamic-entry synchronize 1-34
1.2.2. arp send-rate 1-34
1.2.3. default 1-35
1.2.4. description 1-36
1.2.5. display interface vsi-interface 1-36
1.2.6. distributed-gateway local 1-40
1.2.7. gateway vsi-interface 1-40
1.2.8. interface vsi-interface 1-41
1.2.9. ipv6 nd distributed-gateway dynamic-entry synchronize 1-42
1.2.10. mac-address 1-42
1.2.11. mtu 1-43

1.2.12. shutdown ····· 1-43
1.2.13. vxlan tunnel arp-learning disable ····· 1-44
1.2.14. vxlan tunnel nd-learning disable ····· 1-44
1.3. OVSDB commands ····· 1-45
1.3.1. ovsdb server enable ····· 1-45
1.3.2. ovsdb server ptcp ····· 1-46
1.3.3. vtep access port ····· 1-47
1.3.4. vtep acl disable ····· 1-47
1.3.5. vtep enable ····· 1-48
1.4. Loop detection command ····· 1-49
1.4.1. display loopback-detection ····· 1-49
1.4.2. loopback-detection action ····· 1-50
1.4.3. loopback-detection enable ····· 1-50
1.4.4. loopback-detection interval-time ····· 1-51
1.4.5. loopback-detection priority ····· 1-52

1. VXLAN commands

1.1. Basic VXLAN commands

1.1.1. ac statistics enable

Use **ac statistics enable** to enable packet statistics for Ethernet service instances of a VLAN.

Use **undo ac statistics enable** to disable packet statistics for Ethernet service instances of a VLAN.

Syntax

ac statistics enable

undo ac statistics enable

Default

The packet statistics feature is disabled for Ethernet service instances of a VLAN.

Views

VLAN view

Predefined user roles

network-admin

Usage guidelines

This command enables packet statistics for the Ethernet service instances automatically created for VLAN-based VXLAN assignment.

Before you enable this feature, you must use the **vxlan vlan-based** command to enable VLAN-based VXLAN assignment.

Examples

Map VLAN 10 to VXLAN 100, and enable packet statistics for Ethernet service instances of VLAN 10.

```
<Switch> system-view
[Switch] vxlan vlan-based
[Switch] vlan 10
[Switch-vlan10] vxlan vni 100
[Switch-vlan10] ac statistics enable
```

Related commands

display l2vpn service-instance

reset l2vpn statistics ac

vxlan vlan-based

1.1.2. arp suppression enable

Use **arp suppression enable** to enable ARP flood suppression.

Use **undo arp suppression enable** to disable ARP flood suppression.

Syntax

arp suppression enable

undo arp suppression enable

Default

ARP flood suppression is disabled.

Views

VSI view

Predefined user roles

network-admin

Usage guidelines

ARP flood suppression reduces ARP request broadcasts by enabling the VTEP to reply to ARP requests on behalf of VMs.

This feature snoops ARP packets to populate the ARP flood suppression table with local and remote MAC addresses. If an ARP request has a matching entry, the VTEP replies to the request on behalf of the VM. If no match is found, the VTEP floods the request to both local and remote sites.

Examples

Enable ARP flood suppression for VSI **vsi1**.

```
<Switch> system-view
[Switch] vsi vsi1
[Switch-vsi-vsi1] arp suppression enable
```

Related commands

display arp suppression vsi

reset arp suppression vsi

1.1.3. arp suppression ip-source-binding record

Use **arp suppression ip-source-binding record** to enable the device to generate dynamic IPv4SG bindings based on ARP flood suppression entries.

Use **undo arp suppression ip-source-binding record** to disable the device from generating dynamic IPv4SG bindings based on ARP flood suppression entries.

Syntax

arp suppression ip-source-binding record

undo arp suppression ip-source-binding record

Default

The device does not generate dynamic IPv4SG bindings based on ARP flood suppression entries.

Views

System view

Predefined user roles

network-admin

Usage guidelines

After you execute this command, the device notifies the IP source guard module of ARP flood suppression entries for it to generate dynamic IPv4SG bindings based on these entries.

For more information about IP source guard, see *Security Configuration Guide*.

Examples

Enable the device to generate dynamic IPv4SG bindings based on ARP flood suppression entries.

```
<Switch> system-view
[Switch] arp suppression ip-source-binding record
```

Related commands

arp suppression enable

reset arp suppression vsi

1.1.4. description

Use **description** to configure a description for a VSI.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

A VSI does not have a description.

Views

VSI view

Predefined user roles

network-admin

Parameters

text: Specifies a description, a case-sensitive string of 1 to 80 characters.

Examples

Configure a description for VSI **vpn1**.

```
<Switch> system-view
[Switch] vsi vpn1
[Switch-vsi-vpn1] description vsi for vpn1
```

Related commands

display l2vpn vsi

1.1.5. display arp suppression vsi

Use **display arp suppression vsi** to display ARP flood suppression entries.

Syntax

display arp suppression vsi [**name** *vsi-name*] [**slot** *slot-number*] [**count**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

name *vsi-name*: Specifies a VSI by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VSI, this command displays entries for all VSIs.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays entries on the master device.

count: Displays the number of ARP flood suppression entries that match the command.

Examples

Display ARP flood suppression entries.

```
<Switch> display arp suppression vsi
IP address      MAC address    VSI Name                        Link ID    Aging(min)
1.1.1.2         000f-e201-0101 vsi1                            0x70000    14
1.1.1.3         000f-e201-0202 vsi1                            0x80000    18
1.1.1.4         000f-e201-0203 vsi2                            0x90000    10
```

Display the number of ARP flood suppression entries.

```
<Switch> display arp suppression vsi count
Total entries: 3
```

Table 1-1 Command output

Field	Description
Link ID	Link ID that uniquely identifies an AC or a VXLAN tunnel on a VSI.
Aging(min)	Remaining lifetime (in minutes) of the ARP flood suppression entry. When the timer expires, the entry is deleted.

Related commands

arp suppression enable

reset arp suppression vsi

1.1.6. display ipv6 nd suppression vsi

Use **display ipv6 nd suppression vsi** to display ND flood suppression entries.

Syntax

display ipv6 nd suppression vsi [**name** *vsi-name*] [**slot** *slot-number*] [**count**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

name *vsi-name*: Specifies a VSI by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VSI, this command displays entries for all VSIs.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays entries on the master device.

count: Displays the number of ND flood suppression entries that match the command.

Examples

Display ND flood suppression entries.

```
<Switch> display ipv6 nd suppression vsi
IPv6 address     MAC address      VSI Name         Link ID      Aging (min)
1000::2          000f-e201-0101   vsi1             0x70000      5
1000::3          000f-e201-0202   vsi1             0x80000      5
1000::4          000f-e201-0203   vsi2             0x90000      5
```

Display the number of ND flood suppression entries.

```
<Switch> display ipv6 nd suppression vsi count
Total entries: 3
```

Table 1-2 Command output

Field	Description
Link ID	Link ID that uniquely identifies an AC or a VXLAN tunnel on a VSI.
Aging (min)	Remaining lifetime (in minutes) of the ND flood suppression entry. When the timer expires, the entry is deleted.

Related commands

ipv6 nd suppression enable

reset ipv6 nd suppression vsi

1.1.7. display l2vpn mac-address

Use **display l2vpn mac-address** to display MAC address entries for VSIs.

Syntax

display l2vpn mac-address [**vsi** *vsi-name*] [**dynamic**] [**count** | **verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vsi *vsi-name*: Specifies a VSI name, a case-sensitive string of 1 to 31 characters. If you do not specify a VSI, this command displays MAC address entries for all VSIs.

dynamic: Specifies dynamic MAC address entries learned in the data plane. If you do not specify this keyword, the command displays all MAC address entries, including:

- Dynamic remote- and local-MAC entries.
- Remote-MAC entries advertised through BGP EVPN.
- Manually added static remote-MAC entries.
- Remote-MAC entries issued through OpenFlow.
- Remote-MAC entries issued through OVSDB.

count: Displays the number of MAC address entries.

verbose: Displays detailed information about MAC address entries.

Usage guidelines

If you do not specify the **count** or **verbose** keyword, this command displays brief information about MAC address entries.

Examples

Display brief information about MAC address entries for all VSIs.

```
<Switch> display l2vpn mac-address
MAC Address : 5237-a625-0e06
VSI Name    : vpna
State       : Dynamic
Link ID/Name      Aging
Tunnel1           Aging

MAC Address : 52f6-bc1e-0d06
VSI Name    : vpna
State       : Dynamic
Link ID/Name      Aging
GE1/0/1           Aging
--- 2 mac address(es) found  ---
```

Display the total number of MAC address entries in all VSIs.

```
<Switch> display l2vpn mac-address count
2 mac address(es) found
```

Table 1-3 Command output

Field	Description
VSI Name	VSI name in one of the following formats: • *vsi-name*—VSI name for the MAC address entry. • *vsi1* (*vsi2*)—The MAC address belongs to *vsi1* and has been issued to *vsi2* by the controller.
State	Entry state: • **Dynamic**—Local- or remote-MAC entry dynamically learned in the data plane. • **Static**—Static remote-MAC entry. • **EVPN**—Remote-MAC entry advertised through BGP EVPN. • **OpenFlow**—Remote-MAC entry issued by a remote controller through OpenFlow. • **OVSDB**—Remote-MAC entry issued by a remote controller

Field	Description
	through OVSDB.
Link ID/Name	For a local MAC address, this field displays the name of the interface that hosts the Ethernet service instance for the MAC address. For a remote MAC address, this field displays the tunnel interface name.
Aging	Entry aging state: • **Aging**. • **NotAging**.

Display detailed information about MAC address entries for all VSIs.

```
<Switch> display l2vpn mac-address verbose
MAC Address : 0000-0000-000b
VSI Name    : vpn1
VXLAN ID    : 123
Interface   : GE1/0/1
Link ID     : 1
State       : Dynamic
Aging       : Aging
```

Table 1-4 Command output

Field	Description
Interface	For a local MAC address, this field displays the name of the interface that hosts the Ethernet service instance for the MAC address. For a remote MAC address, this field displays the tunnel interface name.
VSI Name	VSI name in one of the following formats: • *vsi-name*—VSI name for the MAC address entry. • *vsi1* (*vsi2*)—The MAC address belongs to *vsi1* and has been issued to *vsi2* by the controller.
Link ID	Link ID that uniquely identifies an AC or a VXLAN tunnel on a VSI.
State	Entry state: • **Dynamic**—Local- or remote-MAC entry dynamically learned in the data plane. • **Static**—Static remote-MAC entry. • **EVPN**—Remote-MAC entry advertised through BGP EVPN. • **OpenFlow**—Remote-MAC entry issued by a remote controller through OpenFlow. • **OVSDB**—Remote-MAC entry issued by a remote controller through OVSDB.
Aging	Entry aging state: • **Aging**. • **NotAging**.

Related commands

reset l2vpn mac-address

1.1.8. display l2vpn service-instance

Use **display l2vpn service-instance** to display information about Ethernet service instances.

Syntax

display l2vpn service-instance [**interface** *interface-type interface-number* [**service-instance** *instance-id*]] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies a Layer 2 Ethernet interface or Layer 2 aggregate interface by its interface type and number. If you do not specify an interface, this command displays Ethernet service instance information for all Layer 2 Ethernet interfaces and Layer 2 aggregate interfaces.

service-instance *instance-id*: Specifies an Ethernet service instance by its ID in the range of 1 to 4096. If you do not specify an Ethernet service instance, this command displays information about all Ethernet service instances on the specified Layer 2 Ethernet interface or Layer 2 aggregate interface.

verbose: Displays detailed information about Ethernet service instances. If you do not specify this keyword, the command displays brief information about Ethernet service instances.

Examples

Display brief information about all Ethernet service instances.

```
<Switch> display l2vpn service-instance
Total number of service-instances: 2, 2up, 0 down
Total number of ACs: 2, 2 up, 0 down

Interface                ID   Owner                          LinkID State Type
GE1/0/1                  3     vsi12                          1       Up    VSI
GE1/0/1                  4     vsi13                          1       Up    VSI
```

Table 1-5 Command output

Field	Description
Total number of ACs	Total number of attachment circuits (ACs) and the number of ACs in each state (up or down).
Interface	Name of a Layer 2 Ethernet interface or Layer 2 aggregate interface.
ID	Ethernet service instance ID.
Owner	VSI name. This field is empty if an Ethernet service instance is not mapped to any VSI.
LinkID	Ethernet service instance's link ID on the VSI.
State	Ethernet service instance state:

Field	Description
	• **Up**. • **Down**.
Type	L2VPN type of the Ethernet service instance: • **VSI**. • **VPWS**.

Display detailed information about all Ethernet service instances on GigabitEthernet 1/0/1.

```
<Switch> display l2vpn service-instance interface gigabitethernet 1/0/1 verbose
Interface: GE1/0/1
  Service Instance: 1
    Type          : Manual
    Encapsulation : s-vid 16
    Bandwidth     : -
    VSI Name      : vsi10
    Link ID       : 1
    State         : Up
    Statistics    : Enabled
    Input Statistics:
      Octets   :0
      Packets  :0
    Output Statistics:
      Octets   :0
      Packets  :0
```

Table 1-6 Command output

Field	Description
Interface	Name of a Layer 2 Ethernet interface or Layer 2 aggregate interface.
Service Instance	Ethernet service instance ID.
Type	Type and traffic match mode of the Ethernet service instance: • **Dynamic (MAC-based)**—Dynamic Ethernet service instance in MAC-based traffic match mode. • **Manual**—Static Ethernet service instance in VLAN-based traffic match mode.
Encapsulation	Frame match criterion of the Ethernet service instance. If the Ethernet service instance does not contain a match criterion, the command does not display this field.
Bandwidth	This field is not supported in the current software version. Bandwidth limit in kbps. If no bandwidth limit is set for the Ethernet service instance, **Unlimited** is displayed.
Link ID	Ethernet service instance's link ID on the VSI.
State	Ethernet service instance state: • **Up**. • **Down**.
Statistics	Packet statistics state: • **Enabled**—The packet statistics feature is enabled for the Ethernet service instance.

Field	Description
	• **Disabled**—The packet statistics feature is disabled for the Ethernet service instance.
Input Statistics	Incoming traffic statistics: • **Octets**—Number of incoming bytes. • **Packets**—Number of incoming packets.
Output Statistics	Outgoing traffic statistics: • **Octets**—Number of outgoing bytes. • **Packets**—Number of outgoing packets.

Related commands

service-instance

1.1.9. display l2vpn vsi

Use **display l2vpn vsi** to display information about VSIs.

Syntax

display l2vpn vsi [**name** *vsi-name*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

name *vsi-name*: Specifies a VSI by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VSI, this command displays information about all VSIs.

verbose: Displays detailed information about VSIs. If you do not specify this keyword, the command displays brief information about VSIs.

Examples

Display brief information about all VSIs.

```
<Switch> display l2vpn vsi
Total number of VSIs: 1, 1 up, 0 down, 0 admin down

VSI Name                        VSI Index       MTU     State
vpna                            0               1500    Up
```

Table 1-7 Command output

Field	Description
MTU	MTU on the VSI.
State	VSI state: • **Up**—The VSI is up. • **Down**—The VSI is down. • **Admin down**—The VSI has been manually shut down by using the **shutdown** command.

Display detailed information about all VSIs.

```
<Switch> display l2vpn vsi verbose
VSI Name: vpna
  VSI Index               : 0
  VSI State               : Up
  MTU                     : 1500
  Bandwidth               : -
  Broadcast Restrain      : -
  Multicast Restrain      : -
  Unknown Unicast Restrain: -
  MAC Learning            : Enabled
  MAC Table Limit         : -
  MAC Learning rate       : -
  Drop Unknown            : -
  Flooding                : Enabled
  Statistics              : Enabled
  Input statistics:
    Octets   : 0
    Packets  : 0
    Errors   : 0
    Discards : 0
  Output statistics:
    Octets   : 0
    Packets  : 0
    Errors   : 0
    Discards : 0
  Gateway Interface       : VSI-interface 100
  VXLAN ID                : 10
  Tunnels:
    Tunnel Name          Link ID    State  Type      Flood proxy
    Tunnel1              0x5000001  Up     Manual    Disabled
    Tunnel2              0x5000002  Up     Manual    Disabled
    MTunnel0             0x6002710  Up     Auto      Disabled
  ACs:
    AC                              Link ID    State    Type
    GE1/0/1 srv1000                 0          Up       Manual
```

Table 1-8 Command output

Field	Description
VSI Description	Description of the VSI. If the VSI does not have a description, the command does not display this field.
VSI State	VSI state: • **Up**—The VSI is up. • **Down**—The VSI is down. • **Administratively down**—The VSI has been manually shut down by using the **shutdown** command.

Field	Description
MTU	MTU on the VSI.
Bandwidth	This field is not supported in the current software version. Bandwidth limit in kbps. If no bandwidth limit is set for the VSI, **Unlimited** is displayed.
Broadcast Restrain	This field is not supported in the current software version. Broadcast restraint bandwidth (in kbps). If the broadcast restraint bandwidth is not set, **Unlimited** is displayed.
Multicast Restrain	This field is not supported in the current software version. Multicast restraint bandwidth (in kbps). If the multicast restraint bandwidth is not set, **Unlimited** is displayed.
Unknown Unicast Restrain	This field is not supported in the current software version. Unknown unicast restraint bandwidth (in kbps). If the unknown unicast restraint bandwidth is not set, **Unlimited** is displayed.
MAC Learning	State of the MAC learning feature.
MAC Table Limit	This field is not supported in the current software version. Maximum number of MAC address entries on the VSI.
MAC Learning rate	This field is not supported in the current software version. MAC address entry learning rate of the VSI.
Drop Unknown	This field is not supported in the current software version. Action on source MAC-unknown frames received after the maximum number of MAC entries is reached.
Flooding	State of the VSI's flooding feature: • **Enabled**—Flooding is enabled on the VSI. • **Disabled**—Flooding is disabled on the VSI.
Statistics	Packet statistics state: • **Enabled**—The packet statistics feature is enabled for the VSI. • **Disabled**—The packet statistics feature is disabled for the VSI.
Input statistics	Incoming traffic statistics: • **Octets**—Number of incoming bytes. • **Packets**—Number of incoming packets. • **Errors**—Number of error packets. • **Discards**—Number of discarded packets.
Output statistics	Outgoing traffic statistics: • **Octets**—Number of outgoing bytes. • **Packets**—Number of outgoing packets. • **Errors**—Number of error packets. • **Discards**—Number of discarded packets.
Gateway Interface	VSI interface name.
State	Tunnel state: • **Up**—The tunnel is operating correctly. • **Down**—The tunnel interface is down.

Field	Description
Type	Tunnel assignment method: • **Auto**—The tunnel was automatically assigned to the VXLAN. For an EVPN network, VXLAN tunnels are automatically assigned to VXLANs. • **Manual**—The tunnel was manually assigned to the VXLAN.
Flood proxy	Flood proxy state. This field is not supported in the current software version.
ACs	ACs that are bound to the VSI.
Link ID	AC's link ID on the VSI.
State	AC state: • **Up**. • **Down**.
Type	Type and traffic match mode of the Ethernet service instance: • **Dynamic (DRNI)**—Dynamic Ethernet service instance created on the IPL in VLAN-based traffic match mode. • **Dynamic (MAC-based)**—Dynamic Ethernet service instance in MAC-based traffic match mode. • **Manual**—Static Ethernet service instance in VLAN-based traffic match mode.

1.1.10. display vxlan tunnel

Use **display vxlan tunnel** to display VXLAN tunnel information for VXLANs.

Syntax

display vxlan tunnel [**vxlan-id** *vxlan-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vxlan-id: Specifies a VXLAN ID. The value range for this argument is0 to 16777215. If you do not specify a VXLAN, this command displays VXLAN tunnel information for all VXLANs.

Examples

Display VXLAN tunnel information for all VXLANs.

```
<Switch> display vxlan tunnel
Total number of VXLANs: 1

VXLAN ID: 10, VSI name: vpna, Total tunnels: 3 (3 up, 0 down, 0 defect, 0 blocked)
Tunnel name          Link ID    State  Type         Flood proxy
Tunnel1              0x5000001  Up     Manual       Disabled
Tunnel2              0x5000002  Up     Manual       Disabled
MTunnel0             0x6002710  Up     Auto         Disabled
```

Display VXLAN tunnel information for VXLAN **10**.

```
<Switch> display vxlan tunnel vxlan-id 10
VXLAN ID: 10, VSI name: vpna, Total tunnels: 3 (3 up, 0 down, 0 defect, 0 blocked)
Tunnel name          Link ID    State  Type         Flood proxy
Tunnel1              0x5000001  Up     Manual       Disabled
Tunnel2              0x5000002  Up     Manual       Disabled
MTunnel0             0x6002710  Up     Auto         Disabled
```

Table 1-9 Command output

Field	Description
Link ID	Tunnel's link ID in the VXLAN.
State	Tunnel state: • **Up**—The tunnel is operating correctly. • **Down**—The tunnel interface is down.
Type	Tunnel assignment method: • **Auto**—The tunnel was automatically assigned to the VXLAN. For an EVPN network, VXLAN tunnels are automatically assigned to VXLANs. • **Manual**—The tunnel was manually assigned to the VXLAN.
Flood proxy	Flood proxy state. This field is not supported in the current software version.

Related commands

tunnel

vxlan

1.1.11. encapsulation

Use **encapsulation** to configure a frame match criterion for an Ethernet service instance.

Use **undo encapsulation** to restore the default.

Syntax

encapsulation s-vid *vlan-id* [**only-tagged**]

encapsulation untagged

undo encapsulation

Default

An Ethernet service instance does not contain a frame match criterion.

Views

Ethernet service instance view

Predefined user roles

network-admin

Parameters

s-vid: Matches frames that are tagged with the specified outer 802.1Q VLAN IDs.

vlan-id: Specifies an 802.1Q VLAN ID in the range of 1 to 4094.

only-tagged: Matches tagged frames. If the outer 802.1Q VLAN is not the PVID, the matching result does not differ, whether or not you specify the **only-tagged** keyword. If the outer 802.1Q VLAN is the PVID, the matching result depends on whether or not the **only-tagged** keyword is specified.

- To match only PVID-tagged frames, specify the **only-tagged** keyword.
- To match both untagged frames and PVID-tagged frames, do not specify the **only-tagged** keyword.

untagged: Matches any frames that do not have an 802.1Q VLAN tag.

Usage guidelines

An Ethernet service instance can contain only one match criterion. To change the match criterion, first execute the **undo encapsulation** command to remove the original criterion. When you remove the match criterion in an Ethernet service instance, the mapping between the service instance and the VSI is removed automatically.

Examples

Configure Ethernet service instance 1 on GigabitEthernet 1/0/1 to match frames that have an outer 802.1Q VLAN ID of 111.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] service-instance 1
[Switch-GigabitEthernet1/0/1-srv1] encapsulation s-vid 111
```

Related commands

display l2vpn service-instance

1.1.12. flooding disable

Use **flooding disable** to disable flooding for a VSI.

Use **undo flooding disable** to enable flooding for a VSI.

Syntax

flooding disable { **all** | { **broadcast** | **unknown-multicast** | **unknown-unicast** } * }

undo flooding disable

Default

Flooding is enabled for a VSI.

Views

VSI view

Predefined user roles

network-admin

Parameters

all: Specifies broadcast, unknown unicast, and unknown multicast traffic.

broadcast: Specifies broadcast traffic.

unknown-multicast: Specifies unknown multicast traffic.

unknown-unicast: Specifies unknown unicast traffic.

Usage guidelines

By default, the device floods broadcast, unknown unicast, and unknown multicast frames received from the local site to the following interfaces in the frame's VXLAN:

- All site-facing interfaces except for the incoming interface.
- All VXLAN tunnel interfaces.

To confine a kind of flood traffic to the site-facing interfaces, use this command to disable flooding for that kind of flood traffic on the VSI bound to the VXLAN. The VSI will not flood the corresponding frames to VXLAN tunnel interfaces.

Examples

Disable flooding of broadcast traffic for VSI **vsi1**.

```
<Switch> system-view
[Switch] vsi vsi1
[Switch-vsi-vsi1] flooding disable broadcast
```

1.1.13. ipv6 nd suppression enable

Use **ipv6 nd suppression enable** to enable ND flood suppression.

Use **undo ipv6 nd suppression enable** to disable ND flood suppression.

Syntax

ipv6 nd suppression enable

undo ipv6 nd suppression enable

Default

ND flood suppression is disabled.

Views

VSI view

Predefined user roles

network-admin

Usage guidelines

ND flood suppression reduces ND request multicasts by enabling the VTEP to reply to ND requests on behalf of user terminals.

This feature snoops ND packets to populate the ND flood suppression table with local and remote MAC addresses. If an ND request has a matching entry, the VTEP replies to the request on behalf of the user terminal. If no match is found, the VTEP floods the request to both local and remote sites.

Examples

Enable ND flood suppression for VSI **vsi1**.

```
<Switch> system-view
[Switch] vsi vsi1
[Switch-vsi-vsi1] ipv6 nd suppression enable
```

Related commands

display ipv6 nd suppression vsi

reset ipv6 nd suppression vsi

1.1.14. ipv6 nd suppression notify-ipsg

Use **ipv6 nd suppression notify-ipsg** to enable the device to generate dynamic IPv6SG bindings based on ND flood suppression entries.

Use **undo ipv6 nd suppression notify-ipsg** to disable the device from generating dynamic IPv6SG bindings based on ND flood suppression entries.

Syntax

ipv6 nd suppression notify-ipsg

undo ipv6 nd suppression notify-ipsg

Default

The device does not generate dynamic IPv6SG bindings based on ND flood suppression entries.

Views

System view

Predefined user roles

network-admin

Usage guidelines

After you execute this command, the device notifies the IP source guard module of ND flood suppression entries for it to generate dynamic IPv6SG bindings based on these entries.

For more information about IP source guard, see *Security Configuration Guide*.

Examples

Enable the device to generate dynamic IPv6SG bindings based on ND flood suppression entries.

```
<Switch> system-view
[Switch] ipv6 nd suppression notify-ipsg
```

Related commands

display ipv6 source binding (*Security Command Reference*)

ipv6 nd suppression enable

1.1.15. l2vpn enable

Use **l2vpn enable** to enable L2VPN.

Use **undo l2vpn enable** to disable L2VPN.

Syntax

l2vpn enable

undo l2vpn enable

Default

L2VPN is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

You must enable L2VPN before you can configure L2VPN settings.

Examples

Enable L2VPN.

```
<Switch> system-view
[Switch] l2vpn enable
```

1.1.16. l2vpn statistics interval

Use **l2vpn statistics interval** to set the L2VPN statistics collection interval.

Use **undo l2vpn statistics interval** to restore the default.

Syntax

l2vpn statistics interval *interval*

undo l2vpn statistics interval

Default

The L2VPN statistics collection interval is 900 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

Interval: Sets the L2VPN statistics collection interval in seconds, in the range of 30 to 65535.

Examples

Set the L2VPN statistics collection interval to 30 seconds.

```
<Sysname> system-view
[Sysname] l2vpn statistics interval 30
```

1.1.17. mac-address static vsi

Use **mac-address static vsi** to add a static remote-MAC address entry for a VXLAN VSI.

Use **undo mac-address static vsi** to remove a static remote-MAC address entry for a VXLAN VSI.

Syntax

mac-address static *mac-address* **interface tunnel** *tunnel-number* **vsi** *vsi-name*

undo mac-address static [*mac-address*] **interface tunnel** *tunnel-number* **vsi** *vsi-name*

Default

VXLAN VSIs do not have static remote-MAC address entries.

Views

System view

Predefined user roles

network-admin

Parameters

mac-address: Specifies a MAC address in H-H-H format. Do not specify a multicast MAC address or an all-zeros MAC address. You can omit the consecutive zeros at the beginning of each segment. For example, you can enter **f-e2-1** for **000f-00e2-0001**.

interface tunnel *tunnel-number*: Specifies a VXLAN tunnel interface by its tunnel interface number. The specified tunnel interface must already exist.

vsi *vsi-name*: Specifies a VSI name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

A remote MAC address is the MAC address of a VM in a remote site. Remote MAC entries include manually added MAC entries, dynamically learned MAC entries, and MAC entries advertised through BGP EVPN.

When you add a remote MAC address entry, make sure the VSI's VXLAN has been specified on the VXLAN tunnel.

Do not configure static remote-MAC entries for tunnels that are automatically established by using EVPN.

- EVPN re-establishes tunnels if the transport-facing interface goes down and then comes up. If you have configured static remote-MAC entries, the entries are deleted when the tunnels are re-established.
- EVPN re-establishes tunnels if you perform configuration rollback. If the tunnel IDs change during tunnel re-establishment, configuration rollback fails, and static remote-MAC entries on the tunnels cannot be restored.

The **undo mac-address static vsi** *vsi-name* command removes all static remote-MAC address entries for a VSI.

Examples

Add MAC address **000f-e201-0101** to VSI **vsi1**. Specify Tunnel-interface 1 as the outgoing interface.

```
<Switch> system-view
[Switch] mac-address static 000f-e201-0101 interface tunnel 1 vsi vsi1
```

Related commands

vxlan tunnel mac-learning disable

1.1.18. reserved vxlan

Use **reserved vxlan** to specify a reserved VXLAN.

Use **undo reserved vxlan** to restore the default.

Syntax

reserved vxlan *vxlan-id*

undo reserved vxlan

Default

No VXLAN has been reserved.

Views

System view

Predefined user roles

network-admin

Parameters

vxlan-id: Specifies a VXLAN ID in the range of 0 to 16777215.

Usage guidelines

You can specify only one reserved VXLAN on the VTEP. The reserved VXLAN cannot be the VXLAN created on any VSI.

Examples

Specify VXLAN 10000 as the reserved VXLAN.

```
<Switch> system-view
[Switch] reserved vxlan 10000
```

1.1.19. reset arp suppression vsi

Use **reset arp suppression vsi** to clear ARP flood suppression entries on VSIs.

Syntax

reset arp suppression vsi [**name** *vsi-name*]

Views

User view

Predefined user roles

network-admin

Parameters

name *vsi-name*: Specifies a VSI by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VSI, this command clears ARP flood suppression entries on all VSIs.

Examples

Clear ARP flood suppression entries on all VSIs.

```
<Switch> reset arp suppression vsi
This command will delete all entries. Continue? [Y/N]:y
```

Related commands

arp suppression enable

display arp suppression vsi

1.1.20. reset ipv6 nd suppression vsi

Use **reset ipv6 nd suppression vsi** to clear ND flood suppression entries on VSIs.

Syntax

reset ipv6 nd suppression vsi [**name** *vsi-name*]

Views

User view

Predefined user roles

network-admin

Parameters

name *vsi-name*: Specifies a VSI by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VSI, this command clears ND flood suppression entries on all VSIs.

Examples

Clear ND flood suppression entries on all VSIs.

```
<Switch> reset ipv6 nd suppression vsi
This command will delete all entries. Continue? [Y/N]:y
```

Related commands

display ipv6 nd suppression vsi

ipv6 nd suppression enable

1.1.21. reset l2vpn mac-address

Use **reset l2vpn mac-address** to clear dynamic MAC address entries on VSIs.

Syntax

reset l2vpn mac-address [**vsi** *vsi-name*]

Views

User view

Predefined user roles

network-admin

Parameters

vsi *vsi-name*: Specifies a VSI by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VSI, this command clears all dynamic MAC address entries on all VSIs.

Usage guidelines

Use this command when the number of dynamic MAC address entries reaches the limit or the device learns incorrect MAC addresses.

Examples

Clear the dynamic MAC address entries on VSI **vpn1**.

```
<Switch> reset l2vpn mac-address vsi vpn1
```

Related commands

display l2vpn mac-address vsi

1.1.22. reset l2vpn statistics ac

Use **reset l2vpn statistics ac** to clear packet statistics on ACs.

Syntax

reset l2vpn statistics ac [**interface** *interface-type interface-number* [**service-instance** *instance-id*]]

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number.

service-instance *instance-id*: Specifies an Ethernet service instance ID in the range of 1 to 4096.

Usage guidelines

If you do not specify any parameters, this command clears packet statistics on all ACs.

Examples

Clear packet statistics for Ethernet service instance 1 on GigabitEthernet 1/0/1.

```
<Switch> reset l2vpn statistics ac interface gigabitethernet 1/0/1 service-instance 1
```

Related commands

ac statistics enable

display l2vpn interface

display l2vpn service-instance verbose

statistics enable (Ethernet service instance view)

1.1.23. service-instance

Use **service-instance** to create an Ethernet service instance and enter its view, or enter the view of an existing Ethernet service instance.

Use **undo service-instance** to delete an Ethernet service instance.

Syntax

service-instance *instance-id*

undo service-instance *instance-id*

Default

No Ethernet service instances exist.

Views

Layer 2 aggregate interface view

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

instance-id: Specifies an Ethernet service instance ID in the range of 1 to 4096.

Examples

On Layer 2 Ethernet interface GigabitEthernet 1/0/1, create Ethernet service instance 1 and enter Ethernet service instance view.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] service-instance 1
[Switch-GigabitEthernet1/0/1-srv1]
```

Related commands

display l2vpn service-instance

1.1.24. shutdown

Use **shutdown** to shut down a VSI.

Use **undo shutdown** to bring up a VSI.

Syntax

shutdown

undo shutdown

Default

VSIs are up.

Views

VSI view

Predefined user roles

network-admin

Usage guidelines

Use this command to temporarily disable a VSI to provide Layer 2 switching services. The shutdown action does not change settings on the VSI. You can continue to configure the VSI. After you bring up the VSI again, the VSI provides services based on the latest settings.

Examples

Shut down VSI **vpn1**.

```
<Switch> system-view
[Switch] vsi vpn1
[Switch-vsi-vpn1] shutdown
```

Related commands

display l2vpn vsi

1.1.25. statistics enable (Ethernet service instance view)

Use **statistics enable** to enable packet statistics for an Ethernet service instance.

Use **undo statistics enable** to disable packet statistics for an Ethernet service instance.

Syntax

statistics enable

undo statistics enable

Default

The packet statistics feature is disabled for an Ethernet service instance.

Views

Ethernet service instance view

Predefined user roles

network-admin

Usage guidelines

For this command to take effect, you must configure a frame match criterion for the Ethernet service instance and map it to a VSI. If you modify the frame match criterion or VSI mapping, packet statistics of the instance is cleared.

Examples

Enable packet statistics for Ethernet service instance 200 on GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] service-instance 200
[Switch-GigabitEthernet1/0/1-srv200] statistics enable
```

Related command

display l2vpn service-instance verbose

reset l2vpn statistics ac

1.1.26. statistics enable (VSI view)

Use **statistics enable** to enable packet statistics for a VSI.

Use **undo statistics enable** to disable packet statistics for a VSI.

Syntax

statistics enable

undo statistics enable

Default

The packet statistics feature is disabled for a VSI.

Views

VSI view

Predefined user roles

network-admin

Examples

Enable packet statistics for VSI **vsi1**.

```
<Switch> system-view
[Switch] vsi vsi1
[Switch-vsi-vsi1] statistics enable
```

Related commands

display l2vpn vsi verbose

reset l2vpn statistics vsi

1.1.27. tunnel

Use **tunnel** to assign VXLAN tunnels to a VXLAN.

Use **undo tunnel** to remove VXLAN tunnels from a VXLAN.

Syntax

tunnel { *tunnel-number* [**backup-tunnel** *tunnel-number*] | **all** }

undo tunnel { *tunnel-number* | **all** }

Default

A VXLAN does not contain VXLAN tunnels.

Views

VXLAN view

Predefined user roles

network-admin

Parameters

*tunnel-numb*er: Specifies a tunnel interface number. The value range for this argument is 0 to 511. The tunnel must be a VXLAN tunnel.

backup-tunnel *tunnel-number*: Specifies a backup tunnel by its tunnel interface number. The value range for the *tunnel-number* argument is 0 to 511. The tunnel must be a VXLAN tunnel.

all: Specifies all VXLAN tunnels.

Usage guidelines

This command assigns a VXLAN tunnel to a VXLAN to provide Layer 2 connectivity for the VXLAN between two sites. In unicast mode, the system floods unknown unicast, multicast, and broadcast traffic to each tunnel in the VXLAN.

You can assign multiple VXLAN tunnels to a VXLAN, and configure a VXLAN tunnel to trunk multiple VXLANs.

To assign a pair of primary and backup VXLAN tunnels to the VXLAN, specify the **backup-tunnel** *tunnel-number* option. When the primary VXLAN tunnel is operating correctly, the backup VXLAN tunnel does not forward traffic. When the primary VXLAN tunnel goes down, traffic is switched to the backup VXLAN tunnel.

If the **tunnel all** command is used for a VXLAN, you cannot remove the VXLAN tunnels one by one. You can only use the **undo tunnel all** command to remove all the VXLAN tunnels.

Examples

Assign VXLAN tunnels 1 and 2 to VXLAN 10000.

```
<Switch> system-view
[Switch] vsi vpna
[Switch-vsi-vpna] vxlan 10000
[Switch-vsi-vpna-vxlan-10000] tunnel 1
[Switch-vsi-vpna-vxlan-10000] tunnel 2
```

Related commands

display vxlan tunnel

1.1.28. tunnel global source-address

Use **tunnel global source-address** to specify a global source address for VXLAN tunnels.

Use **undo tunnel global source-address** to restore the default.

Syntax

tunnel global source-address *ip-address*

undo tunnel global source-address

Default

No global source address is specified for VXLAN tunnels.

Views

System view

Predefined user roles

network-admin

Parameters

ip-address: Specifies an IP address.

Usage guidelines

IMPORTANT:
For correct VXLAN deployment and VTEP management, do not manually specify tunnel-specific source addresses for VXLAN tunnels if OVSDB is used.

A VXLAN tunnel uses the global source address if you do not specify a source interface or source address for the tunnel.

The global source address takes effect only on VXLAN tunnels.

Examples

Specify 1.1.1.1 as the global source address for VXLAN tunnels.

```
<Switch> system-view
[Switch] tunnel global source-address 1.1.1.1
```

1.1.29. vsi

Use **vsi** to create a VSI and enter its view, or enter the view of an existing VSI.

Use **undo vsi** to delete a VSI.

Syntax

vsi *vsi-name*

undo vsi *vsi-name*

Default

No VSIs exist.

Views

System view

Predefined user roles

network-admin

Parameters

vsi-name: Specifies a VSI name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

A VSI acts as a virtual switch to provide Layer 2 switching services for a VXLAN on a VTEP. A VSI has all functions of a physical Ethernet switch, including source MAC address learning, MAC address aging, and flooding.

A VSI can provide services only for one VXLAN.

Examples

Create VSI **vxlan10** and enter VSI view.

```
<Switch> system-view
[Switch] vsi vxlan10
[Switch-vsi-vxlan10]
```

Related commands

display l2vpn vsi

1.1.30. vxlan

Use **vxlan** to create a VXLAN and enter its view, or enter the view of an existing VXLAN.

Use **undo vxlan** to restore the default.

Syntax

vxlan *vxlan-id*

undo vxlan

Default

No VXLANs exist.

Views

VSI view

Predefined user roles

network-admin

Parameters

vxlan-id: Specifies a VXLAN ID. The value range for this argument is 0 to 16777215.

Usage guidelines

You can create only one VXLAN for a VSI. The VXLAN ID for each VSI must be unique.

Examples

Create VXLAN 10000 for VSI **vpna** and enter VXLAN view.

```
<Switch> system-view
[Switch] vsi vpna
[Switch-vsi-vpna] vxlan 10000
[Switch-vsi-vpna-vxlan-10000]
```

Related commands

vsi

1.1.31. vxlan default-decapsulation

Use **vxlan default-decapsulation** to enable default IPv4 VXLAN decapsulation.

Use **undo vxlan default-decapsulation** to disable default IPv4 VXLAN decapsulation.

Syntax

vxlan default-decapsulation source interface *interface-type interface-number*

undo vxlan default-decapsulation source interface

Default

Default IPv4 VXLAN decapsulation is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

source interface *interface-type interface-number*: Specifies an interface by its type and number.

Usage guidelines

If an IPv4 VXLAN tunnel is configured on only one VTEP of a pair of VTEPs, the IPv4 VXLAN tunnel is a unidirectional tunnel to the VTEP not configured with the tunnel. In this situation, that VTEP drops the VXLAN packets received from the unidirectional VXLAN tunnel. For a VTEP to receive VXLAN packets from a unidirectional IPv4 VXLAN tunnel, enable default IPv4 VXLAN decapsulation on the interface whose IPv4 address is the tunnel destination address. The VTEP will decapsulate all the VXLAN packets destined for the IPv4 address of that interface.

This command takes effect only when the specified interface has an IPv4 address.

The IP address of the specified interface must meet the following requirements:

- It is the destination address of a unidirectional VXLAN tunnel.
- It is the source address of a minimum of one up VXLAN tunnel.

Default IPv4 VXLAN decapsulation does not take effect on bidirectional VXLAN tunnels. If you remove the one-way communication issue for an IPv4 VXLAN tunnel by configuring the tunnel on both the local and remote VTEPs, this feature no longer takes effect on that tunnel.

Examples

Enable default IPv4 VXLAN decapsulation.

```
<Switch> system-view
[Switch] vxlan default-decapsulation source interface gigabitethernet1/0/1
```

1.1.32. vxlan ip-forwarding

Use **vxlan ip-forwarding** to enable Layer 3 forwarding for all VXLANs.

Use **undo vxlan ip-forwarding** to enable Layer 2 forwarding for all VXLANs.

Syntax

vxlan ip-forwarding

undo vxlan ip-forwarding

Default

Layer 3 forwarding is enabled for all VXLANs.

Views.

System view

Predefined user roles

network-admin

Usage guidelines

If the device is a VTEP, enable Layer 2 forwarding for VXLANs. If the device is a VXLAN IP gateway, enable Layer 3 forwarding for VXLANs.

In Layer 3 forwarding mode, the VTEP uses the ARP table (IPv4 network) or ND table (IPv6 network) to forward traffic for VXLANs. In Layer 2 forwarding mode, the VTEP uses the MAC address table to forward traffic for VXLANs.

You must delete all VSIs, VSI interfaces, and VXLAN tunnel interfaces before you can change the forwarding mode.

Examples

Enable Layer 3 forwarding for all VXLANs.

```
<Switch>system-view
[Switch] vxlan ip-forwarding
```

1.1.33. vxlan local-mac report

Use **vxlan local-mac report** to enable local-MAC logging.

Use **undo vxlan local-mac report** to disable local-MAC logging.

Syntax

vxlan local-mac report

undo vxlan local-mac report

Default

Local-MAC logging is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

When the local-MAC logging feature is enabled, the VXLAN module immediately sends a log message with its local MAC addresses to the information center. When a local MAC address is added or removed, a log message is also sent to the information center to notify the local-MAC change.

With the information center, you can set log message filtering and output rules, including output destinations. For more information about configuring the information center, see *Network Management and Monitoring Configuration Guide*.

Examples

Enable local-MAC logging.

```
<Switch> system-view
[Switch] vxlan local-mac report
```

1.1.34. vxlan tunnel mac-learning disable

Use **vxlan tunnel mac-learning disable** to disable remote-MAC address learning.

Use **undo vxlan tunnel mac-learning disable** to enable remote-MAC address learning.

Syntax

vxlan tunnel mac-learning disable

undo vxlan tunnel mac-learning disable

Default

Remote-MAC address learning is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

When network attacks occur, use this command to prevent the device from learning incorrect remote MAC addresses in the data plane.

Examples

Disable remote-MAC address learning.

```
<Switch> system-view
[Switch] vxlan tunnel mac-learning disable
```

1.1.35. vxlan udp-port

Use **vxlan udp-port** to set the destination UDP port number for VXLAN packets.

Use **undo vxlan udp-port** to restore the default.

Syntax

vxlan udp-port *port-number*

undo vxlan udp-port

Default

The destination UDP port number is 4789 for VXLAN packets.

Views

System view

Predefined user roles

network-admin

Parameters

port-number: Specifies a UDP port number in the range of 1 to 65535. As a best practice, specify a port number in the range of 1024 to 65535 to avoid conflict with well-known ports.

Usage guidelines

You must configure the same destination UDP port number on all VTEPs in a VXLAN.

If you modify the destination UDP port number, only VXLAN tunnels established after the modification use the new port number for sending VXLAN packets. For the new port number to take effect on VXLAN tunnels created before the modification, you must disconnect and re-establish the tunnels.

Examples

Set the destination UDP port number to 6666 for VXLAN packets.

```
<Switch> system-view
[Switch] vxlan udp-port 6666
```

1.1.36. vxlan vlan-based

Use **vxlan vlan-based** to enable VLAN-based VXLAN assignment.

Use **undo vxlan vlan-based** to disable VLAN-based VXLAN assignment.

Syntax

vxlan vlan-based

undo vxlan vlan-based

Default

VLAN-based VXLAN assignment is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

You can assign customer traffic to a VXLAN by using one of the following methods:

- **Ethernet service instance-to-VSI mapping**—This method uses the frame match criterion of an Ethernet service instance to match a list of VLANs on a site-facing Layer 2 interface. The VTEP assigns customer traffic to a VXLAN by mapping the Ethernet service instance to a VSI.
- **VLAN-based VXLAN assignment**—This method maps a VLAN to a VXLAN. When a VLAN is mapped to a VXLAN and VLAN-based VXLAN assignment is enabled, the device automatically performs the following operations:
  a. Creates an Ethernet service instance that uses the VLAN ID as its instance ID on each interface in the VLAN. The matching outer VLAN ID of the Ethernet service instances is the VLAN ID.
  b. Maps the Ethernet service instances to the VSI of the VXLAN.

Do not configure both Ethernet service instance-to-VSI mapping and VLAN-based VXLAN assignment.

Examples

Enable VLAN-based VXLAN assignment.

```
<Switch> system-view
[Switch] vxlan vlan-based
```

1.1.37. vxlan vni

Use **vxlan vni** to map a VLAN to a VXLAN.

Use **undo vxlan vni** to remove the VXLAN mapping for a VLAN.

Syntax

vxlan vni *vxlan-id*

undo vxlan vni

Default

A VLAN is not mapped to a VXLAN.

Views

VLAN view

Predefined user roles

network-admin

Parameters

vxlan-id: Specifies a VXLAN ID in the range of 0 to 16777215.

Usage guidelines

Before you map VLANs to VXLANs, enable VLAN-based VXLAN assignment by using the **vxlan vlan-based** command.

You cannot map VLAN 1 to any VXLAN. Do not map a VLAN to the L3 VXLAN ID of EVPN.

If you map a VLAN to a nonexistent VXLAN, the configuration takes effect after the VXLAN is created.

Examples

Map VLAN 10 to VXLAN 100.

```
<Switch> system-view
[Switch] vlan 10
[Switch-vlan10] vxlan vni 100
```

Related commands

vxlan vlan-based

1.1.38. xconnect vsi

Use **xconnect vsi** to map an AC to a VSI.

Use **undo xconnect vsi** to restore the default.

Syntax

xconnect vsi *vsi-name* [**access-mode** { **ethernet** | **vlan** } | **on-demand**] * [**track** *track-entry-number*&<1-3>]

undo xconnect vsi

Default

An AC is not mapped to any VSI.

Views

Ethernet service instance view

Predefined user roles

network-admin

Parameters

vsi-name: Specifies the VSI name, a case-sensitive string of 1 to 31 characters.

access-mode: Specifies an access mode. The default access mode is VLAN.

vlan: Specifies the VLAN access mode.

ethernet: Specifying Ethernet access mode.

track *track-entry-number*&<1-3>: Specifies a space-separated list of up to three track entry numbers in the range of 1 to 1024. The AC is up only if a minimum of one associated track entry is in positive state.

Usage guidelines

To monitor the status of an AC, associate it with track entries.

To use this command for an Ethernet service instance, you must first use the **encapsulation** command to add a traffic match criterion to the service instance.

For traffic that matches the Ethernet service instance, the system uses the VSI's MAC address table to make a forwarding decision.

The device supports the VLAN access mode. In this mode, Ethernet frames received from or sent to the local site must contain 802.1Q VLAN tags.

- For an Ethernet frame received from the local site, the VTEP removes all its 802.1Q VLAN tags before forwarding the frame.
- For an Ethernet frame destined for the local site, the VTEP adds 802.1Q VLAN tags to the frame before forwarding the frame.

In VLAN access mode, VXLAN packets sent between VXLAN sites do not contain 802.1Q VLAN tags. VXLAN can provide Layer 2 connectivity for different 802.1Q VLANs between sites. You can use different 802.1Q VLANs to provide the same service in different sites.

Examples

On GigabitEthernet 1/0/1, configure Ethernet service instance 200 to match frames with an outer 802.1Q VLAN tag of 200, and map the instance to VSI **vpn1**.

```
<Switch> system-view
[Switch] vsi vpn1
[Switch-vsi-vpn1] quit
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] service-instance 200
[Switch-GigabitEthernet1/0/1-srv200] encapsulation s-vid 200
[Switch-GigabitEthernet1/0/1-srv200] xconnect vsi vpn1
```

Related commands

display l2vpn service-instance

encapsulation

vsi

1.2. VXLAN IP gateway commands

1.2.1. arp distributed-gateway dynamic-entry synchronize

Use **arp distributed-gateway dynamic-entry synchronize** to enable dynamic ARP entry synchronization for distributed VXLAN IP gateways.

Use **undo arp distributed-gateway dynamic-entry synchronize** to disable dynamic ARP entry synchronization for distributed VXLAN IP gateways.

Syntax

arp distributed-gateway dynamic-entry synchronize

undo arp distributed-gateway dynamic-entry synchronize

Default

Dynamic ARP entry synchronization is disabled for distributed VXLAN IP gateways.

Views

System view

Predefined user roles

network-admin

Usage guidelines

When local proxy ARP is enabled on distributed VXLAN IP gateways, each gateway learns ARP information independently. A gateway does not forward ARP packets destined for its local VSI interfaces to other gateways. For distributed VXLAN IP gateways to have the same ARP entries, you must enable dynamic ARP entry synchronization.

A controller or the EVPN feature can also synchronize ARP entries among distributed VXLAN IP gateways. When you use a controller or the EVPN feature, do not enable dynamic ARP entry synchronization.

Examples

Enable dynamic ARP entry synchronization for distributed VXLAN IP gateways.

```
<Switch> system-view
[Switch] arp distributed-gateway dynamic-entry synchronize
```

Related commands

distributed-gateway local

local-proxy-arp enable (*Layer 3—IP Services Command Reference*)

1.2.2. arp send-rate

Use **arp send-rate** to set an ARP packet sending rate limit for a VSI interface.

Use **undo arp send-rate** to remove the ARP packet sending rate limit for a VSI interface.

Syntax

arp send-rate *pps*

undo arp send-rate

Default

The ARP packet sending rate is not limited for a VSI interface.

Views

VSI interface view

Predefined user roles

network-admin

Parameters

pps: Specifies a rate limit in the range of 1 to 500 pps.

Usage guidelines

VMs have limited capacity to process packets. To prevent packet processing from degrading VM performance, limit the ARP packet sending rate of the VSI interface for VMs. The VTEP will drop excess ARP packets if the rate limit is exceeded.

Examples

Set the ARP packet sending rate limit to 50 pps for VSI-interface 1.

```
<Switch> system
[Switch] interface vsi-interface 1
[Switch-Vsi-interface1] arp send-rate 50
```

1.2.3. default

Use **default** to restore the default settings for a VSI interface.

Syntax

default

Views

VSI interface view

Predefined user roles

network-admin

Usage guidelines

CAUTION:
The default command might interrupt ongoing network services. Make sure you are fully aware of the impact of this command when you use it on a live network.

This command might fail to restore the default settings for some commands for reasons such as command dependencies and system restrictions.

To resolve this problem:

1. Use the **display this** command in interface view to identify these commands.
2. Use their **undo** forms or follow the command reference to restore their default settings.
3. If the restoration attempt still fails, follow the error message instructions to resolve the problem.

Examples

Restore the default settings for VSI-interface 100.

```
<Switch> system-view
```

```
[Switch] interface vsi-interface 100
[Switch-Vsi-interface100] default
This command will restore the default settings. Continue? [Y/N]:y
```

1.2.4. description

Use **description** to configure the description of a VSI interface.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

The description of a VSI interface is *interface-name* plus **Interface** (for example, **Vsi-interface100 Interface**).

Views

VSI interface view

Predefined user roles

network-admin

Parameters

text: Specifies a description, a case-sensitive string of 1 to 255 characters.

Examples

Configure the description as gateway for **VXLAN 10** for VSI-interface 100.

```
<Switch> system-view
[Switch] interface vsi-interface 100
[Switch-Vsi-interface100] description gateway for VXLAN 10
```

1.2.5. display interface vsi-interface

Use **display interface vsi-interface** to display information about VSI interfaces.

Syntax

display interface [**vsi-interface** [*vsi-interface-id*]] [**brief** [**description** | **down**]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vsi-interface [*vsi-interface-id*]: Specifies VSI interfaces. If you specify a VSI interface, this command displays information about the specified interface. If you specify only the **vsi-interface** keyword, this command displays information about all VSI interfaces. If you do not specify the **vsi-interface** [*vsi-interface-id*] option, this command displays

information about all interfaces. Make sure the specified VSI interfaces have been created on the device.

brief: Display brief interface information. If you do not specify this keyword, the command displays detailed interface information.

description: Displays complete interface descriptions. If you do not specify this keyword, the command displays only the first 27 characters of interface descriptions.

down: Displays interfaces that are physically down as well as the down reason. If you do not specify this keyword, the command does not filter output by physical interface state.

Examples

Display information about VSI-interface 100.

```
<Switch> display interface vsi-interface 100
Vsi-interface100
Current state: UP
Line protocol state: UP
Description: Vsi-interface100 Interface
Bandwidth: 1000000 kbps
Maximum transmission unit: 1500
Internet address: 10.1.1.1/24 (primary)
IP packet frame type: Ethernet II, hardware address: 0011-2200-0102
IPv6 packet frame type: Ethernet II, hardware address: 0011-2200-0102
Physical: Unknown, baudrate: 1000000 kbps
Last clearing of counters: Never
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops
```

Table 1-10 Command output

Field	Description
Current state	Physical link state of the interface: • **Administratively DOWN**—The interface has been shut down by using the **shutdown** command. • **DOWN**—The interface is administratively up, but its physical state is down. • **UP**—The interface is both administratively and physically up.
Line protocol state	Data link layer state of the interface: • **UP**—The data link layer protocol is up. • **UP(spoofing)**—The data link layer protocol is up, but the link is an on-demand link or does not exist. • **DOWN**—The data link layer protocol is down.
Description	Description of the interface.
Bandwidth	Expected bandwidth of the interface.
Maximum transmission unit	MTU of the interface.
Internet protocol processing: Disabled	The interface is not assigned an IP address and cannot process IP packets.
Internet address: *ip-*	IP address of the interface and type of the address in

Field	Description
address/*mask-length* (*Type*)	parentheses. Possible IP address types include: • **Primary**—Manually configured primary IP address. • **Sub**—Manually configured secondary IP address. If the interface has both primary and secondary IP addresses, the primary IP address is displayed. If the interface has only secondary IP addresses, the lowest secondary IP address is displayed. • **DHCP-Allocated**—DHCP allocated IP address. For more information, see DHCP client configuration in *Layer 3—IP Services Configuration Guide*. • **BOOTP-Allocated**−BOOTP allocated IP address. For more information, see BOOTP client configuration in *Layer 3—IP Services Configuration Guide*. • **PPP-Negotiated**—IP address assigned by a PPP server during PPP negotiation. For more information, see PPP configuration in *Layer 2—WAN Access Configuration Guide*. • **Unnumbered**—IP address borrowed from another interface. • **MAD**—IP address assigned to an IRF member device for MAD on the interface. For more information, see IRF configuration in *Virtual Technologies Configuration Guide*.
IP packet frame type	IPv4 packet framing format.
hardware address	MAC address.
IPv6 packet frame type	IPv6 packet framing format.
Physical	Physical type of the interface, which is fixed at **Unknown**.
baudrate	Interface baudrate in kbps.
Last clearing of counters	Last time when the interface statistics are cleared. The current software version does not support clearing interface statistics. This field always displays **Never.**
Last 300 seconds input rate	Average input rate for the last 300 seconds.
Last 300 seconds output rate	Average output rate for the last 300 seconds.
Input: 0 packets, 0 bytes, 0 drops	Incoming traffic statistics on the interface: • Number of incoming packets. • Number of incoming bytes. • Number of dropped incoming packets.
Output: 0 packets, 0 bytes, 0 drops	Outgoing traffic statistics on the interface: • Number of outgoing packets. • Number of outgoing bytes. • Number of dropped outgoing packets.

Display brief information about all VSI interfaces.

```
<Switch> display interface vsi-interface brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
```

```
Protocol: (s) - spoofing
Interface            Link Protocol Primary IP      Description
Vsi100               DOWN DOWN     --
```

Display brief information and complete description for VSI-interface 100.

```
<Switch> display interface vsi-interface 100 brief description
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Primary IP      Description
Vsi100               UP   UP       1.1.1.1         VSI-interface100
```

Displays interfaces that are physically down and the down reason.

```
<Switch> display interface brief down
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Interface            Link   Cause
Vsi100               DOWN   Administratively
Vsi200               DOWN   Administratively
```

Table 1-11 Command output

Field	Description
Interface	Abbreviated interface name.
Link	Physical link state of the interface: • **UP**—The interface is physically up. • **DOWN**—The interface is physically down. • **ADM**—The interface has been shut down by using the **shutdown** command. To restore the physical state of the interface, use the **undo shutdown** command. • **Stby**—The interface is a backup interface in standby state. To see the primary interface, use the **display interface-backup state** command.
Protocol	Data link layer protocol state of the interface: • **UP**—The data link layer protocol of the interface is up. • **UP (s)**—The data link layer protocol of the interface is up, but the link is an on-demand link or does not exist. The **(s)** attribute represents the spoofing flag. • **DOWN**—The data link layer protocol of the interface is down.
Primary IP	Primary IP address of the interface. This field displays two hyphens (**--**) if the interface does not have an IP address.
Description	Description of the interface.
Cause	Cause for the physical link state of an interface to be **DOWN**: • **Administratively**—The interface has been manually shut down by using the **shutdown** command. To restore the physical state of the interface, use the **undo shutdown** command. • **Not connected**—The interface is not mapped to any VSI, or the mapped VSI does not have any AC or VXLAN tunnel.

Related commands

reset counters interface vsi-interface

1.2.6. distributed-gateway local

Use **distributed-gateway local** to specify a VSI interface as a distributed gateway to provide services for the local site.

Use **undo distributed-gateway local** to restore the default.

Syntax

distributed-gateway local

undo distributed-gateway local

Default

A VSI interface is not a distributed gateway.

Views

VSI interface view

Predefined user roles

network-admin

Usage guidelines

If a VXLAN uses distributed gateway services, you must assign the same IP address to the VXLAN's VSI interfaces on different VTEPs. To avoid IP address conflicts, you must specify the VSI interface on each VTEP as a distributed gateway.

Examples

Specify VSI-interface 100 as a distributed gateway.

```
<Switch> system-view
[Switch] interface vsi-interface 100
[Switch-Vsi-interface100] distributed-gateway local
```

1.2.7. gateway vsi-interface

Use **gateway vsi-interface** to specify a gateway interface for a VSI.

Use **undo gateway vsi-interface** to restore the default.

Syntax

gateway vsi-interface *vsi-interface-id*

undo gateway vsi-interface

Default

No gateway interface is specified for a VSI.

Views

VSI view

Predefined user roles

network-admin

Parameters

vsi-interface-id: Specifies a VSI interface by its number. The VSI interface must already exist.

Usage guidelines

When you delete a VSI interface by using the **undo interface vsi-interface** command, the gateway interface setting of the VSI interface is also deleted.

A VSI can have only one gateway interface.

Examples

Specify VSI-interface 100 as the gateway interface for VSI **vpna**.

```
<Switch> system-view
[Switch] vsi vpna
[Switch-vsi-vpna] gateway vsi-interface 100
```

Related commands

interface vsi-interface

1.2.8. interface vsi-interface

Use **interface vsi-interface** to create a VSI interface and enter its view, or enter the view of an existing VSI interface.

Use **undo interface vsi-interface** to delete a VSI interface.

Syntax

interface vsi-interface *vsi-interface-id*

undo interface vsi-interface *vsi-interface-id*

Default

No VSI interfaces exist.

Views

System view

Predefined user roles

network-admin

Parameters

vsi-interface-id: Specifies a VSI interface number. The value range for this argument is 0 to 16777215.

Usage guidelines

When you delete a VSI interface by using the **undo interface vsi-interface** command, the gateway interface setting of the VSI interface is also deleted.

Examples

Create VSI-interface 100 and enter VSI interface view.

```
<Switch> system-view
[Switch] interface vsi-interface 100
[Switch-Vsi-interface100]
```

Related commands

gateway vsi-interface

1.2.9. ipv6 nd distributed-gateway dynamic-entry synchronize

Use **ipv6 nd distributed-gateway dynamic-entry synchronize** to enable dynamic ND entry synchronization for distributed VXLAN IP gateways.

Use **undo ipv6 nd distributed-gateway dynamic-entry synchronize** to disable dynamic ND entry synchronization for distributed VXLAN IP gateways.

Syntax

ipv6 nd distributed-gateway dynamic-entry synchronize

undo ipv6 nd distributed-gateway dynamic-entry synchronize

Default

Dynamic ND entry synchronization is disabled for distributed VXLAN IP gateways.

Views

System view

Predefined user roles

network-admin

Usage guidelines

When local ND proxy is enabled on distributed VXLAN IP gateways, each gateway learns ND information independently. A gateway does not forward ND packets destined for its local VSI interfaces to other gateways. For distributed VXLAN IP gateways to have the same ND entries, you must enable dynamic ND entry synchronization.

A controller or the EVPN feature can also synchronize ND entries among distributed VXLAN IP gateways. When you use a controller or the EVPN feature, do not enable dynamic ND entry synchronization.

Examples

Enable dynamic ND entry synchronization for distributed VXLAN IP gateways.

```
<Switch> system-view
[Switch] ipv6 nd distributed-gateway dynamic-entry synchronize
```

Related commands

distributed-gateway local

1.2.10. mac-address

Use **mac-address** to assign a MAC address to a VSI interface.

Use **undo mac-address** to restore the default.

Syntax

mac-address *mac-address*

undo mac-address

Default

The MAC address of VSI interfaces is the bridge MAC address + 26.

Views

VSI interface view

Predefined user roles

network-admin

Parameters

mac-address: Specifies a MAC address in H-H-H format.

Examples

Assign MAC address 0001-0001-0001 to VSI-interface 100.

```
<Switch> system-view
[Switch] interface vsi-interface 100
[Switch-Vsi-interface100] mac-address 1-1-1
```

1.2.11. mtu

Use **mtu** to set the MTU for a VSI interface.

Use **undo mtu** to restore the default.

Syntax

mtu *size*

undo mtu

Default

The default MTU of a VSI interface is 1444 bytes.

Views

VSI interface view

Predefined user roles

network-admin

Parameters

size: Specifies an MTU value in the range of 46 to 4096 bytes.

Examples

Set the MTU to 1430 bytes for VSI-interface 100.

```
<Switch> system-view
[Switch] interface vsi-interface 100
[Switch-Vsi-interface100] mtu 1430
```

1.2.12. shutdown

Use **shutdown** to shut down a VSI interface.

Use **undo shutdown** to bring up a VSI interface.

Syntax

shutdown

undo shutdown

Default

A VSI interface is up.

Views

VSI interface view

Predefined user roles

network-admin

Examples

Shut down VSI-interface 100.

```
<Switch> system-view
[Switch] interface vsi-interface 100
[Switch-Vsi-interface100] shutdown
```

1.2.13. vxlan tunnel arp-learning disable

Use **vxlan tunnel arp-learning disable** to disable remote ARP learning for VXLANs.

Use **undo vxlan tunnel arp-learning disable** to enable remote ARP learning for VXLANs.

Syntax

vxlan tunnel arp-learning disable

undo vxlan tunnel arp-learning disable

Default

Remote ARP learning is enabled for VXLANs.

Views

System view

Predefined user roles

network-admin

Usage guidelines

By default, the device learns ARP information of remote VMs from packets received on VXLAN tunnel interfaces. To save resources on VTEPs in an SDN transport network, you can temporarily disable remote ARP learning when the controller and VTEPs are synchronizing entries. After the entry synchronization is completed, use the **undo vxlan tunnel arp-learning disable** command to enable remote ARP learning.

As a best practice, disable remote ARP learning for VXLANs only when the controller and VTEPs are synchronizing entries.

Examples

Disable remote ARP learning for VXLANs.

```
<Switch> system
[Switch] vxlan tunnel arp-learning disable
```

1.2.14. vxlan tunnel nd-learning disable

Use **vxlan tunnel nd-learning disable** to disable remote ND learning for VXLANs.

Use **undo vxlan tunnel nd-learning disable** to enable remote ND learning for VXLANs.

Syntax

vxlan tunnel nd-learning disable

undo vxlan tunnel nd-learning disable

Default

Remote ND learning is enabled for VXLANs.

Views

System view

Predefined user roles

network-admin

Usage guidelines

By default, the device learns ND information of remote VMs from packets received on VXLAN tunnel interfaces. To save resources on VTEPs in an SDN transport network, you can temporarily disable remote ND learning when the controller and VTEPs are synchronizing entries. After the entry synchronization is completed, use the **undo vxlan tunnel nd-learning disable** command to enable remote ND learning.

As a best practice, disable remote ND learning for VXLANs only when the controller and VTEPs are synchronizing entries.

Examples

Disable remote ND learning for VXLANs.

```
<Switch> system
[Switch] vxlan tunnel nd-learning disable
```

1.3. OVSDB commands

1.3.1. ovsdb server enable

Use **ovsdb server enable** to enable the OVSDB server.

Use **undo ovsdb server enable** to disable the OVSDB server.

Syntax

ovsdb server enable

undo ovsdb server enable

Default

The OVSDB server is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

To obtain configuration data from controllers, you must enable the OVSDB server.

Before you enable the OVSDB server, you must establish an OVSDB SSL or TCP connection with a minimum of one controller.

Examples

Enable the OVSDB server.

```
<Switch> system-view
[Switch] ovsdb server enable
```

1.3.2. ovsdb server ptcp

Use **ovsdb server ptcp** to enable the device to listen for OVSDB TCP connection requests.

Use **undo ovsdb server ptcp** to restore the default.

Syntax

ovsdb server ptcp [**port** *port-number*] [**acl** *acl-number*]

undo ovsdb server ptcp

Default

The device does not listen for OVSDB TCP connection requests.

Views

System view

Predefined user roles

network-admin

Parameters

port *port-number*: Specifies a port to listen for OVSDB TCP connection requests. The value range for the *port-number* argument is 1 to 65535. If you do not specify a port, the device uses the port number 6640.

acl *acl-number*: Specifies a basic IPv4 ACL by its ACL number to filter OVSDB TCP connection requests. The value range for the *acl-number* argument is 2000 to 2999.

Usage guidelines

You can specify only one port to listen for OVSDB TCP connection requests. If you execute this command multiple times, the most recent configuration takes effect.

For the specified port setting to take effect, you must execute the **ovsdb server enable** command to enable the OVSDB server. You must disable and then re-enable the OVSDB server if it has been enabled.

If you specify a basic IPv4 ACL for this command, the OVSDB server accepts only the OVSDB TCP connection requests that are permitted by the ACL. The OVSDB server rejects any OVSDB TCP connection requests that do not match the ACL or that are denied by the ACL.

The OVSDB server does not filter OVSDB TCP connection requests in any of the following situations:

- No IPv4 ACL is specified for this command.
- The specified IPv4 ACL does not exist.
- The specified IPv4 ACL does not have rules.

You can specify only one IPv4 ACL to filter OVSDB TCP connection requests. If you execute this command multiple times, the most recent configuration takes effect.

Modification to rules in the specified IPv4 ACL takes effect only on OVSDB TCP connection requests that are received after the modification. If you specify another IPv4 ACL, the IPv4 ACL also takes effect only on OVSDB TCP connection requests that are received after the modification.

Examples

Enable the device to listen for OVSDB TCP connection requests on port 6640.

```
<Switch> system-view
[Switch] ovsdb server ptcp
```

Related commands

ovsdb server enable

1.3.3. vtep access port

Use **vtep access port** to specify a site-facing interface as a VTEP access port.

Use **undo vtep access port** to restore the default.

Syntax

vtep access port

undo vtep access port

Default

An interface is not a VTEP access port.

Views

Layer 2 aggregate interface view

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

For controllers to manage a site-facing interface, you must specify the interface as a VTEP access port.

Examples

Specify GigabitEthernet 1/0/1 as a VTEP access port.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] vtep access port
```

1.3.4. vtep acl disable

Use **vtep acl disable** to disable the ACLs issued by the OVSDB controller.

Use **undo vtep acl disable** to enable the ACLs issued by the OVSDB controller.

Syntax

vtep acl disable

undo vtep acl disable

Default

The ACLs issued by the OVSDB controller are enabled on the device.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Before you use this command, you must use the **vtep enable** command to enable the OVSDB VTEP service.

Use the **vtep acl disable** command on a VTEP to disable all the ACLs issued by the OVSDB controller in order to save ACL resources on the VTEP.

Examples

Disable the ACLs issued by the OVSDB controller.

```
<Switch> system-view
[Switch] vtep enable
[Switch] vtep acl disable
```

Related commands

vtep enable

1.3.5. vtep enable

Use **vtep enable** to enable the OVSDB VTEP service.

Use **undo vtep enable** to disable the OVSDB VTEP service.

Syntax

vtep enable

undo vtep enable

Default

The OVSDB VTEP service is disabled.

Views

System view

Predefined user roles

network-admin

Examples

Enable the OVSDB VTEP service.

```
<Switch> system-view
[Switch] vtep enable
```

1.4. Loop detection command

NOTE:

VXLAN loop detection commands are only supported when used in combination with UNIVERGE Network Operation Engine Overlay Network Extension.

1.4.1. display loopback-detection

Use **display loopback-detection** to display the loop detection configuration and status.

Syntax

display loopback-detection

Views

Any view

Predefined user roles

network-admin

network-operator

Example

Display the loop detection configuration and status.

```
<Switch> display loopback-detection
Loop detection is enable.
Global loop detection interval is 30 second(s).
Loop is detected on following interfaces:
* indicates the loop protection action was not triggered.
# indicates the loop protection action failed.
  Interface                      Action mode     VLANs/VSI
  GigabitEthernet1/0/1 srv100    None            vsi1
  GigabitEthernet1/0/2 srv100    Block*          vsi2
  GigabitEthernet1/0/3 srv100    Block#          vsi3
```

Table 1-12 Command output

Field	Description
Action mode	Loop protection action: • **Block**—When a loop is detected on an interface, the device generates a log, disables the interface from learning MAC addresses, and blocks the interface. An asterisk (*) indicates that the block action is not triggered because the loop detection priority of the AC on the interface is higher than that in received loop detection frames. A pound sign (#) indicates that the system failed to execute the block action. • **None**—When a loop is detected on an interface, the device generates a log but performs no action on the interface.
VLANs/VSI	VLANs or VSI to which the interface belongs and where loops are detected.

1.4.2. loopback-detection action

Use **loopback-detection action** to set the loop protection action on a per-VSI basis.

Use **undo loopback-detection action** to restore the default.

Syntax

loopback-detection action block

undo loopback-detection action

Default

When the device detects a loop on an AC, it generates a log but performs no action on the AC.

Views

VSI view

Predefined user roles

network-admin

Parameters

block: Enables the block mode. If a loop is detected on an AC whose loop detection priority is lower than that in received loop detection frames, the device performs the following operations:

- Generates a log.
- Disables MAC address learning on the AC.
- Blocks the AC.

Usage guidelines

The global loop detection action does not take effect on VSIs.

Example

Set the loop protection action to **block** on VSI **vsi1**.

```
<Switch> system-view
[Switch] l2vpn enable
[Switch] vsi vsi1
[Switch-vsi-vsi1] loopback-detection action block
```

Related commands

display loopback-detection

1.4.3. loopback-detection enable

Use **loopback-detection enable** to enable single-tagged loop detection on a VSI.

Use **undo loopback-detection enable** to disable single-tagged loop detection on a VSI.

Syntax

loopback-detection enable [**vlan** *vlan-id-list*]

undo loopback-detection enable [**vlan** *vlan-id-list*]

Default

Loop detection is disabled on VSIs.

Views

VSI view

Predefined user roles

network-admin

Parameters

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN ID or a range of VLAN IDs in the form of *vlan-id1* to *vlan-id2*. The value range for VLAN IDs is 1 to 4094. The value for *vlan-id2* cannot be smaller than the value for *vlan-id1*. If you do not specify any VLAN IDs, each AC of the VSI sends loop detection frames tagged with the VLAN IDs that the AC matches.

Usage guidelines

This command enables the ACs of a VSI to send loop detection frames with one layer of VLAN tags or without VLAN tags.

If you execute this command multiple times for a VSI, all specified VLAN IDs take effect.

This command is mutually exclusive with the **loopback-detection enable s-vid c-vid** command. Do not use them together on a VSI.

Do not execute both the **loopback-detection enable** and **loopback-detection enable vlan** *vlan-id-list* commands on a VSI.

Example

Enable single-tagged loop detection on VSI **vsi1**.

```
<Switch> system-view
[Switch] l2vpn enable
[Switch] vsi vsi1
[Switch-vsi-vsi1] loopback-detection enable
```

Related commands

display loopback-detection

loopback-detection enable s-vid c-vid

loopback-detection priority

1.4.4. loopback-detection interval-time

Use **loopback-detection interval-time** to set the loop detection interval.

Use **undo loopback-detection interval-time** to restore the default.

Syntax

loopback-detection interval-time *interval*

undo loopback-detection interval-time

Default

The loop detection interval is 30 seconds.

Views

VSI view

Predefined user roles

network-admin

Parameters

interval: Sets the loop detection interval in the range of 1 to 32768 seconds.

Usage guidelines

The global loop detection interval does not take effect on VSIs.

With loop detection enabled, the device sends loop detection frames at the specified interval. A shorter interval offers more sensitive detection but consumes more resources. Consider the system performance and loop detection speed when you set the loop detection interval.

Example

Set the loop detection interval to 10 seconds on VSI **vsi1**.

```
<Switch> system-view
[Switch] l2vpn enable
[Switch] vsi vsi1
[Switch-vsi-vsi1] loopback-detetion interval-time 10
```

Related commands

display loopback-detection

1.4.5. loopback-detection priority

Use **loopback-detection priority** to set the priority value in the loop detection priority of a VSI.

Use **undo loopback-detection priority** to restore the default.

Syntax

loopback-detection priority *priority*

undo loopback-detection priority

Default

The priority value is 7 in the loop detection priority of a VSI.

Views

VSI view

Predefined user roles

network-admin

Parameters

priority: Sets the priority value in the range of 1 to 7. The smaller the value, the higher the priority.

Usage guidelines

The loop detection frames sent by an AC carry the loop detection priority of the VSI mapped to the AC. The loop detection priority of a frame contains the priority value, the bridge MAC address, and the AC's link ID. When an AC receives a loop detection frame, it compares its own loop detection priority with that in the frame to identify whether a loop exists. If the loop detection priority in the frame is higher, a loop exists and the loop protection action is triggered. If the loop detection priority of the AC is higher, the system only records the loop information.

An AC uses the following procedure to compare its loop detection priority with that in an incoming loop detection frame:

1. Compares the priority values. The smaller the value, the higher the priority.
2. Compares the bridge MAC addresses if the priority values are the same. A lower bridge MAC address has a higher priority.
3. Compares the link IDs if the bridge MAC addresses are the same, which indicates the loop detection frame is sent by another AC of the device. A smaller link ID has a higher priority.

Example

Set the priority value in the loop detection priority to 3 on VSI **vsi1**.

```
<Switch> system-view
[Switch] l2vpn enable
[Switch] vsi vsi1
[Switch-vsi-vsi1] loopback-detetion priority 3
```

Related commands

display loopback-detection

QX-S5600G Series Ethernet Switches

Command References

14. EVPN

This manual is including the following chapters.

01-EVPN commands

02- MVXLAN commands

Contents

A page of this section is **14-x-x**

1. EVPN commands 1-1
1.1. EVPN commands 1-1
1.1.1. address-family evpn (public instance view) 1-1
1.1.2. address-family evpn (VPN instance view) 1-1
1.1.3. address-family ipv4 (public instance view) 1-2
1.1.4. address-family ipv6 (public instance view) 1-2
1.1.5. address-family l2vpn evpn 1-3
1.1.6. advertise l2vpn evpn 1-3
1.1.7. arp mac-learning disable 1-4
1.1.8. arp-advertising disable 1-4
1.1.9. display bgp l2vpn evpn 1-5
1.1.10. display evpn auto-discovery 1-18
1.1.11. display evpn m-lag synchronized-mac 1-20
1.1.12. display evpn instance vxlan 1-21
1.1.13. display evpn route arp 1-22
1.1.14. display evpn route arp suppression 1-24
1.1.15. display evpn route arp-mobility 1-25
1.1.16. display evpn route smet 1-26
1.1.17. display evpn route mac 1-28
1.1.18. display evpn route mac-mobility 1-29
1.1.19. display evpn route nd 1-31
1.1.20. display evpn routing-table 1-32
1.1.21. evpn m-lag group 1-34
1.1.22. evpn m-lag local 1-34
1.1.23. evpn encapsulation 1-35
1.1.24. evpn global-mac 1-36
1.1.25. evpn route arp-mobility suppression 1-37
1.1.26. evpn route mac-mobility suppression 1-37
1.1.27. export route-policy 1-38
1.1.28. import evpn mac-ip 1-39
1.1.29. import route-policy 1-40
1.1.30. ip forwarding-conversational-learning 1-41
1.1.31. ip-prefix-route generate disable 1-42
1.1.32. l2vpn m-lag peer-link ac-match-rule vxlan-mapping 1-42
1.1.33. l2vpn statistics vsi l3-vni 1-43
1.1.34. l3-vni 1-44
1.1.35. mac-advertising disable 1-45
1.1.36. nd mac-learning disable 1-45
1.1.37. policy vpn-target 1-46
1.1.38. route-distinguisher (EVPN instance view) 1-46
1.1.39. route-distinguisher (public instance view) 1-47
1.1.40. route-distinguisher 1-48
1.1.41. vpn-target 1-49

1. EVPN commands

1.1. EVPN commands

1.1.1. address-family evpn (public instance view)

Use **address-family evpn** to enter EVPN view of the public instance.

Use **undo address-family evpn** to delete all settings in EVPN view of the public instance.

Syntax

address-family evpn

undo address-family evpn

Views

Public instance view

Predefined user roles

network-admin

Usage guidelines

You can configure EVPN settings such as route targets in EVPN view of the public instance.

Examples

Enter EVPN view of the public instance.

```
<Switch> system-view
[Switch] ip public-instance
[Switch-public-instance] address-family evpn
[Switch-public-instance-evpn]
```

1.1.2. address-family evpn (VPN instance view)

Use **address-family evpn** to enter EVPN view of a VPN instance.

Use **undo address-family evpn** to delete all settings in EVPN view of a VPN instance.

Syntax

address-family evpn

undo address-family evpn

Views

VPN instance view

Predefined user roles

network-admin

Usage guidelines

You can configure EVPN settings such as route targets and routing policies in EVPN view of a VPN instance.

Examples

Enter EVPN view of VPN instance **tenant**.

```
<Switch> system-view
[Switch] ip vpn-instance tenant
[Switch-vpn-instance-tenant] address-family evpn
[Switch-vpn-evpn-tenant]
```

1.1.3. address-family ipv4 (public instance view)

Use **address-family ipv4** to enter IPv4 VPN view of the public instance.

Use **undo address-family ipv4** to delete all settings in IPv4 VPN view of the public instance.

Syntax

address-family ipv4

undo address-family ipv4

Views

Public instance view

Predefined user roles

network-admin

Examples

Enter IPv4 VPN view of the public instance.

```
<Switch> system-view
[Switch] ip public-instance
[Switch-public-instance] address-family ipv4
[Switch-public-instance-ipv4]
```

1.1.4. address-family ipv6 (public instance view)

Use **address-family ipv6** to enter IPv6 VPN view of the public instance.

Use **undo address-family ipv6** to delete all settings in IPv6 VPN view of the public instance.

Syntax

address-family ipv6

undo address-family ipv6

Views

Public instance view

Predefined user roles

network-admin

Examples

Enter IPv6 VPN view of the public instance.

```
<Switch> system-view
[Switch] ip public-instance
[Switch-public-instance] address-family ipv6
[Switch-public-instance-ipv6]
```

1.1.5. address-family l2vpn evpn

Use **address-family l2vpn evpn** to create the BGP EVPN address family and enter its view, or enter the view of the existing BGP EVPN address family.

Use **undo address-family l2vpn evpn** to delete the BGP EVPN address family and all settings in BGP EVPN address family view.

Syntax

address-family l2vpn evpn

undo address-family l2vpn evpn

Default

The BGP EVPN address family does not exist.

Views

BGP instance view

Predefined user roles

network-admin

Usage guidelines

Configuration made in BGP EVPN address family view takes effect only on routes and peers of the BGP EVPN address family that are on the public network.

Examples

Create the BGP EVPN address family and enter its view.

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default] address-family l2vpn evpn
[Switch-bgp-default-evpn]
```

1.1.6. advertise l2vpn evpn

Use **advertise l2vpn evpn** to enable BGP EVPN route advertisement to the local site.

Use **undo advertise l2vpn evpn** to disable BGP EVPN route advertisement to the local site.

Syntax

advertise l2vpn evpn

undo advertise l2vpn evpn

Default

BGP EVPN route advertisement to the local site is enabled.

Views

BGP-VPN IPv4 unicast address family view

BGP-VPN IPv6 unicast address family view

Predefined user roles

network-admin

Usage guidelines

This command enables the device to advertise private BGP EVPN routes to the local site after the device adds the routes to the routing table of a VPN instance.

Examples

Enable BGP EVPN route advertisement to the local site for VPN instance **vpn1**.

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default] ip vpn-instance vpn1
[Switch-bgp-default-vpn1] address-family ipv4
[Switch-bgp-default-ipv4-vpn1] advertise l2vpn evpn
```

1.1.7. arp mac-learning disable

Use **arp mac-learning disable** to disable an EVPN instance from learning MAC addresses from ARP information.

Use **undo arp mac-learning disable** to restore the default.

Syntax

arp mac-learning disable

undo arp mac-learning disable

Default

An EVPN instance learns MAC addresses from ARP information.

Views

EVPN instance view

Predefined user roles

network-admin

Usage guidelines

The MAC information and ARP information advertised by a remote VTEP overlap. To avoid duplication, use this command to disable the learning of MAC addresses from ARP information. EVPN will learn remote MAC addresses only from the MAC information advertised from remote sites.

Examples

Disable an EVPN instance from learning MAC addresses from ARP information.

```
<Switch> system-view
[Switch] vsi aaa
[Switch-vsi-aaa] evpn encapsulation vxlan
[Switch-vsi-aaa-evpn-vxlan] arp mac-learning disable
```

1.1.8. arp-advertising disable

Use **arp-advertising disable** to disable ARP information advertisement for a VSI EVPN instance.

Use **undo arp-advertising disable** to restore the default.

Syntax

arp-advertising disable

undo arp-advertising disable

Default

ARP information advertisement is enabled for a VSI EVPN instance.

Views

VSI EVPN instance view

Predefined user roles

network-admin

Usage guidelines

In an EVPN network with distributed gateways, you can disable ARP information advertisement for a VXLAN to save resources if all its user terminals use the same EVPN gateway device. The EVPN instance of the VXLAN will stop advertising ARP information through MAC/IP advertisement routes and withdraw advertised ARP information. When ARP information advertisement is disabled, user terminals in other VXLANs still can communicate with that VXLAN through IP prefix advertisement routes.

Examples

Disable ARP information advertisement for a VSI EVPN instance.

```
<Switch> system-view
[Switch] vsi aaa
[Switch-vsi-aaa] evpn encapsulation vxlan
[Switch-vsi-aaa-evpn-vxlan] arp-advertising disable
```

1.1.9. display bgp l2vpn evpn

Use **display bgp l2vpn evpn** to display BGP EVPN routes.

Syntax

display bgp [**instance** *instance-name*] **l2vpn evpn** [**peer** { *ipv4-address* | *ipv6-address* } { **advertised-routes** | **received-routes** } [**statistics**] | [**route-distinguisher** *route-distinguisher* | **route-type** { **auto-discovery** | **es** | **igmp-ls** | **igmp-js** | **imet** | **ip-prefix** | **mac-ip** | **s-pmsi** | **smet** }] * [{ *evpn-route route-length* | *evpn-prefix* } [**advertise-info** | **ext-community**] | { *ipv4-address* | *ipv6-address* | *mac-address* } [**verbose**]] | **statistics**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

instance *instance-name*: Specifies a BGP instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the command displays BGP EVPN routes for the default BGP instance.

peer { *ipv4-address* | *ipv6-address* }: Specifies a peer by its IPv4 address or IPv6 address.

advertised-routes: Specifies the routes advertised to the specified peer.

received-routes: Specifies the routes received from the specified peer.

statistics: Displays BGP EVPN route statistics.

route-distinguisher *route-distinguisher*: Specifies a route distinguisher (RD), a string of 3 to 21 characters. The RD can use one of the following formats:

- *16-bit AS number:32-bit user-defined number*. For example, 101:3.
- *32-bit IP address:16-bit user-defined number*. For example, 192.168.122.15:1.
- *32-bit AS number:16-bit user-defined number*. For example, 65536:1. The AS number must be equal to or greater than 65536.

route-type: Specifies a route type.

auto-discovery: Specifies Ethernet auto-discovery routes.

es: Specifies Ethernet segment (ES) routes.

imet: Specifies inclusive multicast Ethernet tag (IMET) routes.

ip-prefix: Specifies IP prefix advertisement routes.

mac-ip: Specifies MAC/IP advertisement routes.

s-pmsi: Specifies Selective Provider Multicast Service Interface (S-PMSI) routes.*evpn-route*: Specifies a BGP EVPN route, a case-insensitive string of 1 to 512 characters.

smet: Specifies selective multicast Ethernet tag (SMET) routes.

route-length: Specifies the route length in bits, in the range of 0 to 65535.

advertise-info: Displays advertisement information for BGP EVPN routes.

ext-community: Specifies the extended community attribute.

verbose: Displays detailed BGP EVPN route information. If you do not specify this keyword, the command displays brief BGP EVPN route information.

Usage guidelines

If you do not specify any parameter, this command displays brief information about all BGP EVPN routes.

Examples

Display brief information about all BGP EVPN routes.

```
<Switch> display bgp l2vpn evpn

BGP local router ID is 8.8.8.8
 Status codes: * - valid, > - best, d - dampened, h - history,
               s - suppressed, S - stale, i - internal, e - external
               a - additional-path
               Origin: i - IGP, e - EGP, ? - incomplete

 Total number of routes from all PEs: 3

 Route distinguisher: 1:1
 Total number of routes: 2

* >e Network : [2][0][48][0011-0022-0033][32][11.22.33.55]/136
```

```
     NextHop : 1.1.1.2                                  LocPrf    : 100
     PrefVal : 0                                        OutLabel  : NULL
     MED     : 0
     Path/Ogn: 20i

Route distinguisher of public instance: 1:15
Total number of routes: 1

* >i Network : [2][0][48][7010-0000-0001][0][0.0.0.0]/104
     NextHop : 1.1.1.4                                  LocPrf    : 100
     PrefVal : 0                                        OutLabel  : NULL
     MED     : 0
     Path/Ogn: 20i
```

Display all BGP EVPN routes that carry extended community attributes.

```
<Sysname> display bgp l2vpn evpn ext-community

 BGP local router ID is 1.1.1.9
 Status codes: * - valid, > - best, d - dampened, h - history,
               s - suppressed, S - stale, i - internal, e - external
               a - additional-path
               Origin: i - IGP, e - EGP, ? - incomplete

 Total number of routes from all PEs: 6

 Route distinguisher: 100:1
 Total number of routes: 3

       Network       NextHop       MED     LocPrf    PrefVal   Path/Ogn    Ext-Community

* >  [2][0][48][00aa.00bb.00cc][4][0.0.0.0]/136
                    10.1.1.2        0        32768               ?          <RT 2:3>
*  e                10.1.1.1        0        0                   65410?     <RT 2:3>
* >  [3][300][16][::ffff:1.1.1.1]/176
                    127.0.0.1       0        32768               ?          <RT 3:4>
```

Table 1-1 Command output

Field	Description
Status codes	Route status codes: • *** - valid**—Valid route. • **> - best**—Optimal route. • **d - dampened**—Dampened route. • **h - history**—History route. • **i - internal**—Internal route. • **e - external**—External route. • **s - suppressed**—Suppressed route. • **S - Stale**—Stale route.

Field	Description
Origin	Origin of the route: • **i – IGP**—Originated in the AS. The origin of routes advertised by using the **network** command is **IGP**. • **e – EGP**—Learned through EGP. • **? – incomplete**—Unknown origin. The origin of routes redistributed from IGP protocols is **incomplete**.

Network	BGP EVPN route/route length. BGP EVPN routes are as follows:
	• [1][ESI][EthernetTagID]
	  ○ **1**—Ethernet auto-discovery route.
	  ○ **ESI**—Ethernet segment identifier (ESI).
	  ○ **EthernetTagID**—Ethernet tag ID.
	• [2][EthernetTagID][MACLength][MAC][IPAddressLength][IPAddress]
	  ○ **2**—MAC/IP advertisement route.
	  ○ **EthernetTagID**—Ethernet tag ID.
	  ○ **MACLength**—MAC address length.
	  ○ **MAC**—MAC address.
	  ○ **IPAddressLength**—IP address length.
	  ○ **IPAddress**—IP address.
	• [3][EthernetTagID][IPAddressLength][IPAddress]
	  ○ **3**—IMET route.
	  ○ **IPAddressLength**—IP address length.
	  ○ **IPAddress**—IP address of the originating router.
	• [4][ESI][IPAddressLength][IPAddress]
	  ○ **4**—ES route.
	  ○ **ESI**—ESI.
	  ○ **IPAddressLength**—IP address length.
	  ○ **IPAddress**—IP address of the originating router.
	• [5][EthernetTagID][IPAddressLength][IPAddress]
	  ○ **5**—IP prefix advertisement route.
	  ○ **EthernetTagID**—Ethernet tag ID.
	  ○ **IPAddressLength**—IP address length.
	  ○ **IPAddress**—IP address of the originating router.
	• [6][EthernetTagID][Source Len][Source IP][Group Len][Group IP][Originator Len][Originator IP]
	  ○ **6**—Selective multicast Ethernet tag route.
	  ○ **EthernetTagID**—Ethernet tag ID.
	  ○ **Source Len**—Length of the multicast source address. This field displays 0 if the multicast source is any (*, G).
	  ○ **Source IP**—Source IP address of IGMP membership reports. This field is not displayed if the multicast source is any (*, G).
	  ○ **Group Len**—Length of the multicast group address.
	  ○ **Group IP**—Multicast group address of IGMP membership reports.
	  ○ **Originator Len**—Length of the originating router's IP address.
	  ○ **Originator IP**—IP address of the originating router.

NextHop	Next hop IP address.

Field	Description
MED	Multi-Exit Discriminator (MED) attribute.
LocPrf	Local precedence.
OutLabel	Outgoing label.
PrefVal	Preferred value.
Path/Ogn	AS_PATH and ORIGIN attributes of the route.
Ext-Community	Extended community attribute.

Display detailed information about BGP EVPN route [1][00:00:00:00:00:00:00:00:00:00][5]/120 with RD 1.1.1.1:100.

```
<Switch> display bgp l2vpn evpn route-distinguisher 1.1.1.1:100
[1][00:00:00:00:00:00:00:00:00:00][5] 120

 BGP local router ID: 172.16.250.133
 Local AS number: 100



 Route distinguisher: 1.1.1.1:100
 Total number of routes: 1
 Paths:   1 available, 1 best

 BGP routing table information of [1][00:00:00:00:00:00:00:00:00:00][5]/120:
 From            : 10.1.1.2 (192.168.56.17)
 Rely nexthop    : 10.1.1.2
 Original nexthop: 10.1.1.2
 OutLabel        : NULL
 Ext-Community   : <RT: 1:2>, <Encapsulation Type: VXLAN >, <ESI Label: Flag 0,
                   Label 1>,
 RxPathID        : 0x0
 TxPathID        : 0x0
 AS-path         : 200
 Origin          : igp
 Attribute value : MED 0, pref-val 0
 State           : valid, external, best
 IP precedence   : N/A
 QoS local ID    : N/A
 Traffic index   : N/A
 EVPN route type : Ethernet auto-discovery route
 ESI             : 00:00:00:00:00:00:00:00:00:00
 Ethernet tag ID : 5
 MPLS label      : 10
```

Table 1-2 Command output

Field	Description
Paths	Number of routes: • **available**—Number of valid routes.

Field	Description
	• **best**—Number of optimal routes.
From	IP address of the BGP peer that advertised the route.
Rely Nexthop	Next hop after route recursion. If no next hop is found, this field displays **not resolved**.
Original nexthop	Original next hop of the route. If the route was obtained from a BGP update message, the original next hop is the next hop IP address in the message.
OutLabel	Outgoing label of the route.
Ext-Community	Extended community attributes: • **RT**. • **Encapsulation Type**. • **ESI Label**.
RxPathID	Add-Path ID value of the received route. This field is not supported by the BGP EVPN address family.
TxPathID	Add-Path ID value of the sent route. This field is not supported by the BGP EVPN address family.
AS-path	AS_PATH attribute of the route. This attribute records the ASs the route has passed and avoids routing loops.
Origin	Origin of the route: • **igp**—Originated in the AS. The origin of routes advertised by using the **network** command is **IGP**. • **egp**—Learned through EGP. • **incomplete**—Unknown origin. The origin of routes redistributed from IGP protocols is **incomplete**.
Attribute value	Attributes of the route: • **MED**—MED value for the destination network. • **localpref**—Local preference value. • **pref-val**—Preferred value. • **pre**—Route preference value.
State	Current state of the route: • **valid**. • **internal**. • **external**. • **local**. • **synchronize**. • **best**. • **bgp-rib-only**—The route will not be flushed to the routing table. This field is displayed only in the detailed command output.
IP precedence	IP precedence in the range of 0 to 7. **N/A** indicates that the IP precedence is invalid.
QoS local ID	The current software version does not support this field. QoS local ID in the range of 1 to 4095. **N/A** indicates that the QoS local ID is invalid.
Traffic index	Traffic index in the range of 1 to 64. **N/A** indicates that the traffic index is invalid.

Field	Description
MPLS label	MPLS label. The current software version does not support this field.

Display detailed information about BGP EVPN route [2][5][48][0001-0203-0405][32][4.5.5.5]/136 with RD 1.1.1.1:100.

```
<Switch> display bgp l2vpn evpn route-distinguisher 1.1.1.1:100 [2][5][48][0001-0203-
0405][32][5.5.5.5] 136

 BGP local router ID: 172.16.250.133
 Local AS number: 100


 Route distinguisher: 1.1.1.1:100
 Total number of routes: 1
 Paths:   1 available, 1 best

 BGP routing table information of [2][5][48][0001-0203-0405][32][5.5.5.5]/136:
 From            : 10.1.1.2 (192.168.56.17)
 Rely nexthop    : 10.1.1.2
 Original nexthop: 10.1.1.2
 OutLabel        : NULL
 Ext-Community   : <RT: 1:2>, <RT: 1:3>, <RT: 1:4>, <RT: 1:5>, <RT: 1:6>, <RT: 1:7
                   >, <Encapsulation Type: VXLAN>, <Router's Mac: 0006-0708-0910
                   >, <MAC Mobility: Flag 0, SeqNum 2>, <Default GateWay>
 RxPathID        : 0x0
 TxPathID        : 0x0
 AS-path         : 200
 Origin          : igp
 Attribute value : MED 0, pref-val 0
 State           : valid, external, best
 IP precedence   : N/A
 QoS local ID    : N/A
 Traffic index   : N/A
 EVPN route type : MAC/IP advertisement route
 ESI             : 00:00:00:00:00:00:00:00:00:00
 Ethernet tag ID : 5
 MAC address     : 0001-0203-0405
 IP address      : 5.5.5.5/32
 MPLS label1     : 10
 MPLS label2     : 100
 Re-origination  : Enable

 Route distinguisher: 2.2.2.2:100
 Total number of routes: 1
 Paths:   1 available, 1 best
```

```
BGP routing table information of [2][5][48][0001-0203-0405][32][5.5.5.5]/136:
From            : 10.1.1.2 (192.168.56.17)
Rely nexthop    : 10.1.1.2
Original nexthop: 10.1.1.2
OutLabel        : 0
Ext-Community   : <RT: 1:2>, <RT: 1:3>, <RT: 1:4>, <RT: 1:5>, <RT: 1:6>, <RT: 1:7
                  >, <Encapsulation Type: VXLAN>, <Router's Mac: 0006-0708-0910
                  >, <MAC Mobility: Flag 0, SeqNum 2>, <Default GateWay>
RxPathID        : 0x0
TxPathID        : 0x0
AS-path         : 200
Origin          : igp
Attribute value : MED 0, pref-val 0
State           : valid, external, best, reoriginated, remoteredist
IP precedence   : N/A
QoS local ID    : N/A
Traffic index   : N/A
EVPN route type : MAC/IP advertisement route
ESI             : 0001.0203.0405.0607.0809
Ethernet tag ID : 5
MAC address     : 0001-0203-0405
IP address      : 5.5.5.5/32
MPLS label1     : 200
MPLS label2     : 300
```

Table 1-3 Command output

Field	Description

Ext-Community	Extended community attributes:
	• **RT**.
	• **Encapsulation Type**.
	• **Router's Mac**.
	• **MAC Mobility**—MAC mobility.
	  ○ **Flag**—Indicates whether the MAC address can move. A value of 1 indicates that the MAC address cannot move, and a value of 0 indicates that the MAC address can move.
	  ○ **SeqNum**—Identifies the most recent move of the MAC address.
	• **Default GateWay**—Route for the default gateway.

State	Current state of the route: • **valid**. • **internal**. • **external**. • **local**. • **synchronize**. • **best**. • **reoriginated**—Reoriginated route. • **remoteredist**—MAC/IP advertisement route generated

Field	Description
	based on a remote route.
MPLS label1	VXLAN ID used for Layer 2 forwarding.
MPLS label2	L3 VXLAN ID used for Layer 3 forwarding.
Re-origination	State of route reorigination: • **Enable**. • **Disable**.

Display detailed information about BGP EVPN route [3][0][32][5.5.5.5]/80 with RD 1.1.1.1:100.

```
<Switch> display bgp l2vpn evpn route-distinguisher 1.1.1.1:100 [3][0][32][4.5.5.5]
80

BGP local router ID: 172.16.250.133
 Local AS number: 100


 Route distinguisher: 1.1.1.1:100
 Total number of routes: 1
 Paths:   1 available, 1 best

 BGP routing table information of [3][0][32][4.5.5.5]/80:
 From            : 10.1.1.2 (192.168.56.17)
 Rely nexthop    : 10.1.1.2
 Original nexthop: 10.1.1.2
 OutLabel        : NULL
 Ext-Community   : <RT: 1:2>, <Encapsulation Type: VXLAN>
 RxPathID        : 0x0
 TxPathID        : 0x0
 PMSI tunnel     : Flag 0, TunnelType 6, Label 10, EndPointAddress 10.1.1.2
 AS-path         : 200
 Origin          : igp
 Attribute value : MED 0,pref-val 0
 State           : valid, external, best
 IP precedence   : N/A
 QoS local ID    : N/A
 Traffic index   : N/A
 EVPN route type : Inclusive multicast Ethernet tag route
 Ethernet tag ID : 0
 Origin address  : 5.5.5.5/32
 Re-origination  : Enable

 Route distinguisher: 2.2.2.2:100
 Total number of routes: 1
 Paths:   1 available, 1 best
 BGP routing table information of [3][0][32][4.5.5.5]/80:
 From            : 10.1.1.2 (192.168.56.17)
```

```
Rely nexthop    : 10.1.1.2
Original nexthop: 10.1.1.2
OutLabel        : NULL
Ext-Community   : <RT: 1:2>, <Encapsulation Type: VXLAN>
RxPathID        : 0x0
TxPathID        : 0x0
PMSI tunnel     : Flag 0, TunnelType 6, Label 10, EndPointAddress 10.1.1.2
AS-path         : 200
Origin          : igp
Attribute value : MED 0,pref-val 0
State           : valid, external, best, reoriginated, remoteredist
IP precedence   : N/A
QoS local ID    : N/A
Traffic index   : N/A
EVPN route type : Inclusive multicast Ethernet tag route
Ethernet tag ID : 0
Origin address  : 5.5.5.5/32
```

Table 1-4 Command output

Field	Description
Ext-Community	Extended community attributes: • **RT**. • **Encapsulation Type**.
State	Route state: • **valid**—Valid route. • **internal**—Internal route. • **external**—External route. • **local**—Locally originated route. • **synchronize**—Synchronized route. • **best**—Optimal route. • **reoriginated**—Reoriginated route. • **remoteredist**—IMET route originated based on a remote route.
PMSI tunnel	P-Multicast Service Interface (PMSI) tunnel information: • **Flag**—Flags. This field is fixed at 0 in the current software version. • **TunnelType**—Tunnel type. This field is fixed at 6 in the current software version, which represents a head-end replication tunnel. • **Label**—VXLAN ID. • **EndPointAddress**—Tunnel destination address.
Origin address	IP address of the originating router.
Re-origination	Status of route reorigination: • **Enable**. • **Disable**.

Display detailed information about BGP EVPN route [4][00:00:00:00:00:00:00:00:00:00][32][4.5.5.5]/128 with RD 1.1.1.1:100.

```
<Switch> display bgp l2vpn evpn route-distinguisher 1.1.1.1:100
[4][00:00:00:00:00:00:00:00:00:00][32][4.5.5.5] 128

 BGP local router ID: 172.16.250.133
 Local AS number: 100


 Route distinguisher: 1.1.1.1:100
 Total number of routes: 1
 Paths:   1 available, 1 best

 BGP routing table information of
[4][00:00:00:00:00:00:00:00:00:00][32][4.5.5.5]/128:
 From            : 10.1.1.2 (192.168.56.17)
 Rely nexthop    : 10.1.1.2
 Original nexthop: 10.1.1.2
 OutLabel        : NULL
 Ext-Community   : <RT: 1:2>, <Encapsulation Type: VXLAN>, <ES-Import RT: 1:1>
 RxPathID        : 0x0
 TxPathID        : 0x0
 AS-path         : 200
 Origin          : igp
 Attribute value : MED 0,pref-val 0
 State           : valid, external, best
 IP precedence   : N/A
 QoS local ID    : N/A
 Traffic index   : N/A
 EVPN route type : Ethernet segment route
 ESI             : 00:00:00:00:00:00:00:00:00:00
 Origin address  : 4.5.5.5/32
```

Table 1-5 Command output

Field	Description
Ext-Community	Extended community attributes: • **RT**. • **Encapsulation Type**. • **ES-Import RT**.
Origin address	IP address of the originating router.

Display detailed information about BGP EVPN route [5][10][32][4.5.5.5]/80 with RD 1.1.1.1:100.

```
<Switch> display bgp l2vpn evpn route-distinguisher 1.1.1.1:100 [5][10][32][4.5.5.5]
80

 BGP local router ID: 172.16.250.133
 Local AS number: 100
```

```
Route distinguisher: 1.1.1.1:100
Total number of routes: 1
Paths:   1 available, 1 best

BGP routing table information of [5][10][32][4.5.5.5]/80:
From            : 10.1.1.2 (192.168.56.17)
Rely nexthop    : 10.1.1.2
Original nexthop: 10.1.1.2
OutLabel        : NULL
Ext-Community   : <RT: 1:2>, <Encapsulation Type: VXLAN>, <Router's Mac:
                  0006-0708-0910>
RxPathID        : 0x0
TxPathID        : 0x0
AS-path         : 200
Origin          : igp
Attribute value : MED 0,pref-val 0
State           : valid, external, best
IP precedence   : N/A
QoS local ID    : N/A
Traffic index   : N/A
EVPN route type : IP prefix advertisement route
ESI             : 00:00:00:00:00:00:00:00:00:00
Ethernet tag ID : 10
IP address      : 4.5.5.5/32
Gateway address : 0.0.0.0
MPLS Label      : 1
Re-origination  : Enable

Route distinguisher: 2.2.2.2:100
Total number of routes: 1
Paths:   1 available, 1 best

BGP routing table information of [5][10][32][4.5.5.5]/80:
From            : 10.1.1.2 (192.168.56.17)
Rely nexthop    : 10.1.1.2
Original nexthop: 10.1.1.2
OutLabel        : 0
Ext-Community   : <RT: 1:2>, <Encapsulation Type: VXLAN>, <Router's Mac:
                  0006-0708-0910>
RxPathID        : 0x0
TxPathID        : 0x0
AS-path         : 200
Origin          : igp
Attribute value : MED 0,pref-val 0
State           : valid, external, best, reoriginated, remoteredist
IP precedence   : N/A
QoS local ID    : N/A
Traffic index   : N/A
```

```
EVPN route type : IP prefix advertisement route
ESI             : 0000.0000.0000.0000.000a
Ethernet tag ID : 10
IP address      : 4.5.5.5/32
Gateway address : 0.0.0.0
MPLS Label      : 20
```

Table 1-6 Command output

Field	Description
Ext-Community	Extended community attributes: • **RT**. • **Encapsulation Type**. • **Router's Mac**.
State	Current state of the route: • **valid**. • **internal**. • **external**. • **local**. • **synchronize**. • **best**. • **reoriginated**—Reoriginated route. • **localredist**—IP prefix advertisement route generated based on a local route. • **remoteredist**—IP prefix advertisement route generated based on a remote route.
IP address	IP address and prefix length.
MPLS Label	L3 VXLAN ID used for Layer 3 forwarding.
Re-origination	State of route reorigination: • **Enable**. • **Disable**.

Display detailed information about BGP EVPN route [6][0][32][10.1.1.1][32][224.224.224.224][32][192.168.3.1]/160 with RD 1.1.1.1:100.

```
<Sysname> display bgp l2vpn evpn route-distinguisher 1.1.1.1:100
[6][0][32][10.1.1.1][32][224.224.224.224][32][192.168.3.1] 160

 BGP local router ID: 172.16.250.133
 Local AS number: 100



 Route distinguisher: 1.1.1.1:100
 Total number of routes: 1
 Paths:   1 available, 1 best

 BGP routing table information of
[6][0][32][10.1.1.1][32][224.224.224.224][32][192.168.3.1]/160:
 From            : 10.1.1.2
```

```
Rely nexthop     : 10.1.1.2
Original nexthop: 10.1.1.2
OutLabel         : NULL
Ext-Community    : <RT: 1:2>, <Encapsulation Type: VXLAN>,
RxPathID         : 0x0
TxPathID         : 0x0
AS-path          : 200
Origin           : igp
Attribute value  : MED 0,pref-val 0
State            : valid, external, best
IP precedence    : N/A
QoS local ID     : N/A
Traffic index    : N/A
EVPN route type  : Selective multicast Ethernet tag route
Ethernet tag ID  : 0
Source length    : 32
Source address   : 10.1.1.1
Group length     : 32
Group address    : 224.224.224.224
Origin address   : 192.168.3.1
IGMP flags       : v3, include
```

Table 1-7 Command output

Field	Description
Ext-Community	Extended community attributes: • **RT**. • **Encapsulation Type**.
Source length	Length of the multicast source address.
Source address	Multicast source address.
Group length	Length of the multicast group address.
Group address	Multicast group address.
Origin address	IP address of the originating router.

1.1.10. display evpn auto-discovery

Use **display evpn auto-discovery** to display information about IPv4 peers that are automatically discovered through BGP.

Syntax

display evpn auto-discovery { { **imet** | mac-ip } [**peer** *ip-address*] [**vsi** *vsi-name*] | **macip-prefix** [**nexthop** *next-hop*] [**count**] }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

imet: Specifies IPv4 peers discovered through IMET routes.

mac-ip: Specifies IPv4 peers discovered through MAC/IP advertisement routes that do not carry L3 VXLAN IDs.

peer *ip-address*: Specifies a peer by its IPv4 address. If you do not specify this option, the command displays information about all automatically discovered IPv4 peers.

vsi *vsi-name*: Specifies a VSI by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the command displays IPv4 peer information for all VSIs.

macip-prefix: Specifies IPv4 peers discovered through MAC/IP advertisement routes and IP prefix advertisement routes.

nexthop *next-hop*: Specifies a next hop. If you do not specify this option, the command displays IPv4 peer information for all next hops.

count: Displays the number of IPv4 peers. If you do not specify this keyword, the command displays detailed IPv4 peer information.

Examples

Display information about IPv4 peers discovered through IMET routes.

```
<Switch> display evpn auto-discovery imet
Total number of automatically discovered peers: 2

VSI name: vpna
EVPN instance: -
RD                    PE_address      Tunnel_address  Tunnel mode VXLAN ID
1:10                  2.2.2.2         2.2.2.2         VXLAN       10
2:100                 3.3.3.3         3.3.3.3         VXLAN       10
VSI name: vpnb
RD                    PE_address      In/Out label    Tunnel Mode
1:10                  4.4.4.4         1420/1419       PW
```

Table 1-8 Command output

Field	Description
EVPN instance	EVPN instance name. If the EVPN instance is created on a VSI, this field displays a hyphen (-).
PE_address	Identifier of the remote VTEP on the VSI.
Tunnel_address	Tunnel destination IP address.
Tunnel mode	Tunnel mode, which can only be **VXLAN**.
In/Out label	Incoming and outgoing labels for the PW. If the labels are invalid, this field displays a hyphen (-). PWs are not supported in the current software version.

Display information about IPv4 peers discovered through MAC/IP advertisement routes and IP prefix advertisement routes.

```
<Switch> display evpn auto-discovery macip-prefix
Destination IP  Source IP       L3VNI           Tunnel mode OutInterface
1.1.1.1         3.3.3.3         200             VXLAN       Vsi-interface3
2.2.2.2         3.3.3.3         200             VXLAN       Vsi-interface3
```

Display the total number of IPv4 peers discovered through MAC/IP advertisement routes and IP prefix advertisement routes.

```
<Switch> display evpn auto-discovery macip-prefix count
Total number of entries: 2
```

Table 1-9 Command output

Field	Description
Destination IP	Tunnel destination IP address.
Source IP	Tunnel source IP address.
L3VNI	L3 VXLAN ID used for Layer 3 forwarding.
Tunnel mode	VXLAN tunnel mode, which can only be **VXLAN**.
Outinterface	VSI interface associated with the L3 VXLAN ID.

1.1.11. display evpn m-lag synchronized-mac

Use **display evpn m-lag synchronized-mac** to display M-LAG-synchronized MAC address entries.

Syntax

display evpn m-lag synchronized-mac [**vsi** *vsi-name*] [**count**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vsi *vsi-name*: Specifies a VSI name, a case-sensitive string of 1 to 31 characters. If you do not specify a VSI, this command displays MAC address entries for all VSIs.

count: Displays the number of MAC address entries that match the command. If you do not specify this keyword, the command displays detailed information about MAC address entries.

Usage guidelines

To ensure VM reachability information consistency in a M-LAG system, M-LAG member devices synchronize MAC address entries and ARP packets with each other through a peer-link. This command displays the synchronized MAC address entries from a M-LAG peer.

Examples

Display all M-LAG -synchronized MAC address entries.

```
<Sysname> display evpn m-lag synchronized-mac
VSI name: bbb
```

```
MAC address           Link ID      Interface
0000-0000-000a        1            BAGG10
0000-0000-0009        0            Tunnel1
```

Display the total number of M-LAG -synchronized MAC address entries.

```
<Sysname> display evpn m-lag synchronized-mac count
Total number of entries: 2
```

Table 1-10 Command output

Field	Description
Link ID	AC's or VXLAN tunnel's link ID on a VSI.
Interface	Outgoing interface name.

1.1.12. display evpn instance vxlan

Use **display evpn instance vxlan** to display EVPN instance information.

Syntax

display evpn instance [**name** *instance-name* | **vsi** *vsi-name*] **vxlan**

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

name *instance-name*: Specifies an EVPN instance by its name, a case-sensitive string of 1 to 31 characters.

vsi *vsi-name*: Specifies a VSI by its name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

If you do not specify any parameters, this command displays information about all EVPN instances.

Examples

Display information about all EVPN instances.

```
<Switch> display evpn instance vxlan
EVPN instance            : evpn1
  Route distinguisher    : 1:1
  Export VPN targets     : 1:1
  Import VPN targets     : 1:1
  ARP-based MAC learning : Disabled
  ND-based MAC learning  : Disabled
  ARP advertising        : Disabled
  MAC advertising        : Disabled
  VSI binding list:
    VSI name                                VSI tag ID
    vpna                                    3
```

```
    vpnb                                  5

EVPN instance            : - (created on VSI vpnc)
  Route distinguisher    : 1:1
  Export VPN targets     : 1:1
  Import VPN targets     : 1:1
  ARP-based MAC learning : Disabled
  ND-based MAC learning  : Disabled
  ARP advertising        : Disabled
  MAC advertising        : Disabled
```

Table 1-11 Command output

Field	Description
EVPN instance	EVPN instance name in one of the following formats: • *instance-name*—Name of an EVPN instance created in system view. • - (**created on VSI** *vsi-name*)—Name of an EVPN instance created on a VSI.
ARP-based MAC learning	Whether EVPN is enabled to learn MAC addresses from ARP information: • - —**Enabled**. • **Disabled**.
ND-based MAC learning	Whether EVPN is enabled to learn MAC addresses from ND information: • - —**Enabled**. • **Disabled**.
ARP advertising	Whether ARP information advertisement is enabled: • - —**Enabled**. • **Disabled**.
MAC advertising	Whether MAC address advertisement is enabled: • - —**Enabled**. • **Disabled**.
VSI binding list	VSIs bound to the EVPN instance.

1.1.13. display evpn route arp

Use **display evpn route arp** to display EVPN ARP entries.

Syntax

display evpn route arp [**local** | **remote**] [**public-instance** | **vpn-instance** *vpn-instance-name*] [**count**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

local: Specifies local ARP entries.

remote: Specifies remote ARP entries.

public-instance: Specifies the public instance.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters.

count: Displays the number of ARP entries. If you do not specify this keyword, the command displays detailed information about ARP entries.

Usage guidelines

If you do not specify the **local** or **remote** keyword, this command displays both local and remote EVPN ARP entries.

If you do not specify the **public-instance** keyword or the **vpn-instance** *vpn-instance-name* option, this command displays EVPN ARP entries for the public instance and all VPN instances.

Examples

Display all EVPN ARP entries.

```
<Switch> display evpn route arp
Flags: D - Dynamic    B - BGP       L - Local active
       G - Gateway    S - Static    M - Mapping        I - Invalid

VPN instance: vpn1                              Interface: Vsi-interface1
IP address      MAC address     Router MAC      VSI index   Flags
10.1.1.1        0003-0003-0003  a0ce-7e40-0400  0           GL
10.1.1.11       0001-0001-0001  a0ce-7e40-0400  0           DL
10.1.1.12       0001-0001-0011  a0ce-7e41-0401  0           B
10.1.1.13       0001-0001-0021  a0ce-7e42-0402  0           B
10.1.1.101      0001-0011-0101  a0ce-7e40-0400  0           SL
10.1.1.102      0001-0011-0102  0011-9999-0000  0           BS

Public instance                                 Interface: Vsi-interface2
IP address      MAC address     Router MAC      VSI index   Flags
11.1.1.1        0033-0033-0033  a0ce-7e40-0400  0           GL
11.1.1.11       0011-0011-0011  a0ce-7e40-0400  0           DL
# Display the total number of EVPN ARP entries.
<Switch> display evpn route arp count
Total number of entries: 8
```

Table 1-12 Command output

Field	Description
Interface	VSI interface.
Flags	ARP entry type: • **D**—The entry is dynamically learned. • **B**—The entry is learned from BGP EVPN routes. • **L**—The local entry is active. If this flag is not set and the B flag is set, the entry learned from BGP EVPN routes is active.

Field	Description

	• **G**—The entry for the gateway is active.
	• **S**—The static entry is active. This entry type is not supported in the current software version.
	• **M**—The entry from a remote VXLAN mapped to a local VXLAN is active. This entry type is not supported in the current software version.
	• **I**—The entry is invalid.Possible reasons:
	  ○ The VSI has been administratively shut down by using the **shutdown** command.
	  ○ The outgoing tunnel interface does not exist.

1.1.14. display evpn route arp suppression

Use **display evpn route arp suppression** to display EVPN ARP flood suppression entries.

Syntax

display evpn route arp suppression [**local** | **remote**] [**vsi** *vsi-name*] [**count**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

local: Specifies local ARP flood suppression entries.

remote: Specifies remote ARP flood suppression entries.

vsi *vsi-name*: Specifies a VSI by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the command displays ARP flood suppression entries for all VSIs.

count: Displays the number of ARP flood suppression entries. If you do not specify this keyword, the command displays detailed information about ARP flood suppression entries.

Usage guidelines

If you do not specify the **local** or **remote** keyword, this command displays both local and remote EVPN ARP flood suppression entries.

Examples

Display all EVPN ARP flood suppression entries.

```
<Switch> display evpn route arp suppression
Flags: D - Dynamic   B - BGP      L - Local active
       G - Gateway   S - Static   M - Mapping

VSI name: vpna
EVPN instance: -
IP address      MAC address       Flags           Encap
10.1.1.12       0002-0002-0002    B               VXLAN
10.1.1.13       0002-0002-0002    BI              VXLAN
```

```
10.1.1.101      0001-0011-0101    BS              VXLAN
10.1.1.102      0001-0011-0102    DL              VXLAN
```

Display the total number of ARP flood suppression entries.

```
<Switch> display evpn route arp suppression count
Total number of entries: 4
```

Table 1-13 Command output

Field	Description
EVPN instance	EVPN instance name. If the EVPN instance is created on a VSI, this field displays a hyphen (**-**).
Flags	ARP flood suppression entry type: • **D**—The entry is dynamically learned. • **B**—The entry is learned from BGP EVPN routes. • **L**—The local entry is active. If this flag is not set and the B flag is set, the entry learned from BGP EVPN routes is active. • **G**—The entry for the gateway is active. • **S**—The static entry is active. This entry type is not supported in the current software version. • **M**—The entry from a remote VXLAN mapped to a local VXLAN is active. This entry type is not supported in the current software version.
Encap	Packet encapsulation type, which can only be **VXLAN**.

1.1.15. display evpn route arp-mobility

Use **display evpn route arp-mobility** to display EVPN ARP mobility information.

Syntax

display evpn route arp-mobility [**public-instance** | **vpn-instance** *vpn-instance-name*] [**ip** *ip-address*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

public-instance: Specifies the public instance.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters.

ip *ip-address*: Specifies an IPv4 address in dotted decimal notation. If you do not specify an IP address, this command displays ARP mobility information about all IP addresses of the public instance or MPLS L3VPN instance.

Usage guidelines

If you do not specify any parameters, this command displays ARP mobility information about the public instance and all VPN instances.

Examples

Display EVPN ARP mobility information about the public instance and all VPN instances.

```
<Switch> display evpn route arp-mobility
Flags: S - Suppressed, N - Not suppressed
  Suppression threshold: 5
  Detection cycle      : 180s

VPN instance : vpn1
Interface    : Vsi-interface1
  IP address      Seq number Moved from               Flags Suppressed at
  192.168.156.120 5          GE1/0/1                  S     17:24:33 2018/04/01
  192.168.56.20   -          -                        N     -

Public instance
Interface    : Vsi-interface2
  IP address      Seq number Moved from               Flags Suppressed at
  192.168.156.120 5          GE1/0/2                  S     17:24:33 2018/04/01
  192.168.56.20   5          2.2.2.2                  S     17:24:33 2018/04/01
```

Table 1-14 Command output

Field	Description
Suppression threshold	ARP mobility suppression threshold, which is the number of ARP moves from the local site to a remote site.
Detection cycle	ARP mobility detection cycle in seconds.
Seq number	ARP move sequence number.
Moved from	Source interface or source VTEP IP address for the ARP move.
Flags	Whether the ARP move was suppressed: • **S**—Suppressed. • **N**—Not suppressed.
Suppressed at	Time when the ARP move was suppressed.

Related commands

evpn route arp-mobility suppression

1.1.16. display evpn route smet

Use **display evpn route smet** to display EVPN multicast routes.

Syntax

display evpn route smet [**local** | **remote**] [**vsi** *vsi-name*] [**count**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

smet: Specifies SMET routes.

local: Specifies local multicast routes.

remote: Specifies remote multicast routes.

vsi *vsi-name*: Specifies a VSI by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the command displays multicast routes for all VSIs.

count: Displays the number of multicast routes. If you do not specify this keyword, the command displays detailed information about multicast routes.

Usage guidelines

If you do not specify the **local** or **remote** keyword, this command displays both local and remote multicast routes.

Examples

Display all SMET routes.

```
<Sysname> display evpn route smet
VSI name: bbb
  Source address  : 192.164.1.1
  Group address   : 226.1.1.1
  Local version   : v3(I)
  Peers :
    Nexthop          Tunnel name     Link ID    Remote version
    1.1.1.1          Tunnel0         0x5000000  v3(E)
  ACs   :
    AC                               Link ID    Flags
    GE1/0/1 srv1                     0          Sync
```

Table 1 Command output

Field	Description
Source address	Multicast source IP address.
Group address	Multicast group IP address.
Local version	Local IGMP version. IGMPv3 includes the v3(I) and v3(E) subversions.
Peers	Remote peers in SMET routes.
Nexthop	Remote VTEP IP address.
Tunnel name	Remote tunnel interface name.
Link ID	Link ID of the VXLAN tunnel.
Remote version	Remote IGMP version. IGMPv3 includes the v3(I) and v3(E) subversions.
ACs	Local ACs.
AC	AC name. This field displays a Layer 3 interface name or a Layer 2 interface name and an Ethernet service instance name.

Field	Description
Link ID	The AC's link ID.
Flags	Flags: • **Local**—Local AC. • **Sync**—AC synchronized from another VTEP.

1.1.17. display evpn route mac

Use **display evpn route mac** to display IPv4 EVPN MAC address entries.

Syntax

display evpn route mac [**local** | **remote**] [**vsi** *vsi-name*] [**count**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

local: Specifies local MAC address entries.

remote: Specifies remote MAC address entries.

vsi *vsi-name*: Specifies a VSI by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the command displays MAC address entries for all VSIs.

count: Displays the number of MAC address entries. If you do not specify this keyword, the command displays detailed information about MAC address entries.

Usage guidelines

If you do not specify the **local** or **remote** keyword, this command displays both local and remote IPv4 EVPN MAC address entries.

Examples

Display all IPv4 EVPN MAC address entries.

```
<Switch> display evpn route mac
Flags: D - Dynamic   B - BGP      L - Local active
       G - Gateway   S - Static   M - Mapping        I - Invalid

VSI name: bbb
EVPN instance: -
MAC address     Link ID/Name   Flags   Encap           Next hop
0000-0000-000a  1              DL      VXLAN           -
0000-0000-0009  Tunnel1        B       VXLAN           2.2.2.2
0001-2000-4000  -              BI      VXLAN           3.3.3.3
```

Display the total number of IPv4 EVPN MAC address entries.

```
<Switch> display evpn route mac count
Total number of entries: 3
```

Table 1-15 Command output

Field	Description
EVPN instance	EVPN instance name. If the EVPN instance is created on a VSI, this field displays a hyphen (**-**).
Link ID/Name	For a local MAC address, this field displays the AC's link ID on the VSI. For a remote MAC address, this field displays the tunnel interface name.

Flags	MAC address entry type:
	• **D**—The entry is dynamically learned.
	• **B**—The entry is learned from BGP EVPN routes.
	• **L**—The local entry is active. If this flag is not set and the B flag is set, the entry learned from BGP EVPN routes is active.
	• **G**—The entry for the gateway is active.
	• **S**—The static entry is active. This entry type is not supported in the current software version.
	• **M**—The entry from a remote VXLAN mapped to a local VXLAN is active. This entry type is not supported in the current software version.
	• **I**—The entry is invalid.Possible reasons:
	  ○ The VSI has been administratively shut down by using the **shutdown** command.
	  ○ The outgoing tunnel interface does not exist.

Encap	Packet encapsulation type, which can only be **VXLAN**.
Next hop	IP address of the remote VTEP. If the MAC address entry is a local entry, a hyphen (**-**) is displayed.

1.1.18. display evpn route mac-mobility

Use **display evpn route mac-mobility** to display EVPN MAC mobility information.

Syntax

display evpn [**ipv6**] **route mac-mobility** [**vsi** *vsi-name*] [**mac-address** *mac-address*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ipv6: Specifies IPv6 EVPN MAC mobility information. If you do not specify this keyword, the command displays IPv4 EVPN MAC mobility information.

vsi *vsi-name*: Specifies a VSI by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VSI, this command displays MAC mobility information about all VSIs.

mac-address *mac-address*: Specifies a MAC address in the format of H-H-H. You can omit the consecutive zeros at the beginning of each segment. For example, you can enter f-e2-1 for 000f-

00e2-0001. If you do not specify a MAC address, this command displays MAC mobility information about all MAC addresses in the specified VSI or all VSIs.

Usage guidelines

If you do not specify any parameters, this command displays IPv4 EVPN MAC mobility information about all VSIs.

Examples

Display IPv4 EVPN MAC mobility information about all VSIs.

```
<Switch> display evpn route mac-mobility
Flags: S - Suppressed, N - Not suppressed
  Suppression threshold: 5
  Detection cycle      : 180s

VSI name      : vsia
EVPN instance : -
  MAC address     Seq number Moved from              Flags Suppressed at
  1000-0000-0000  10         GE1/0/1                 S     15:30:30 2018/03/30
  1000-0000-0001  -          -                       N     -

VSI name      : vsib
EVPN instance : -
  MAC address     Seq number Moved from              Flags Suppressed at
  1000-0000-0003  2          GE1/0/2                 N     -
  1000-0000-0005  10         5.5.5.5                 S     17:24:33 2018/04/01
```

Display IPv6 EVPN MAC mobility information about all VSIs.

```
<Switch> display evpn ipv6 route mac-mobility
Flags: S - Suppressed, N - Not suppressed
  Suppression threshold: 5
  Detection cycle      : 180s

VSI name      : vpna
EVPN instance : -
  MAC address          : 1000-1000-1000
  Sequence number      : 5
  Moved from           : GE1/0/1
  Flags                : S
  Suppressed at        : 15:30:30 2018/03/30

VSI name      : vpnb
EVPN instance : -
  MAC address          : 1000-1000-1001
  Sequence number      : 5
  Moved from           : 1::1
  Flags                : S
  Suppressed at        : 15:30:30 2018/03/30
```

Table 1-16 Command output

Field	Description
Suppression threshold	MAC mobility suppression threshold, which is the number of MAC moves from the local site to a remote site.
Detection cycle	MAC mobility detection cycle in seconds.
EVPN instance	EVPN instance name. If the EVPN instance is created on a VSI, this field displays a hyphen (-).
Seq number/Sequence number	MAC move sequence number.
Moved from	Source interface or source VTEP IP address for the MAC move.
Flags	Whether the MAC move was suppressed: • **S**—Suppressed. • **N**—Not suppressed.
Suppressed at	Time when the MAC move was suppressed.

Related commands

evpn route mac-mobility suppression

1.1.19. display evpn route nd

Use **display evpn route nd** to display EVPN ND entries.

Syntax

display evpn route nd [**local** | **remote**] [**public-instance** | **vpn-instance** *vpn-instance-name*] [**count**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

local: Specifies local ND entries.

remote: Specifies remote ND entries.

public-instance: Specifies the public instance.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters.

count: Displays the number of ND entries. If you do not specify this keyword, the command displays detailed information about ND entries.

Usage guidelines

If you do not specify the **local** or **remote** keyword, this command displays both local and remote EVPN ND entries.

If you do not specify the **public-instance** keyword or the **vpn-instance** *vpn-instance-name* option, this command displays EVPN ND entries for the public instance and all VPN instances.

Examples

Display all EVPN ND entries.

```
<Switch> display evpn route nd
Flags: D - Dynamic   B - BGP      L - Local active
       G - Gateway   S - Static   M - Mapping

VPN instance: vpn1                          Interface: Vsi-interface1
IPv6 address :   AD80:0300:1000:0050:0200:0300:0100:0012
MAC address  :   0001-0001-0001       Router MAC    :   a0ce-7e40-0400
VSI index    :   0                    Flags         :   GL

IPv6 address :   AD10:0300:1000:0020:0200:0300:0100:0022
MAC address  :   0001-0001-0002       Router MAC    :   a0ce-7e40-0411
VSI index    :   0                    Flags         :   GL

Public instance                             Interface: Vsi-interface1
IPv6 address :   BC80:0300:1000:0050:0200:0300:0100:0033
MAC address  :   0002-0002-0001       Router MAC    :   a0ce-7e40-0422
VSI index    :   0                    Flags         :   GL

IPv6 address :   BC10:0300:1000:0020:0200:0300:0100:0034
MAC address  :   0002-0002-0002       Router MAC    :   a0ce-7e40-0433
VSI index    :   0                    Flags         :   GL
```

Display the total number of EVPN ND entries.

```
<Switch>display evpn route nd count
Total number of entries: 2
```

Table 1-17 Command output

Field	Description
Interface	VSI interface.
Flags	ND entry type: • **D**—The entry is dynamically learned. • **B**—The entry is learned from BGP EVPN routes. • **L**—The local entry is active. If this flag is not set and the B flag is set, the entry learned from BGP EVPN routes is active. • **G**—The entry for the gateway is active. • **S**—The static entry is active. This type is not supported in the current software version. • **M**—The entry from a remote VXLAN mapped to a local VXLAN is active. This type is not supported in the current software version.

1.1.20. display evpn routing-table

Use **display evpn routing-table** to display the EVPN routing table for a VPN instance.

Syntax

display evpn routing-table [**ipv6**] { **public-instance** | **vpn-instance** *vpn-instance-name* } [**count**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ipv6: Specifies IPv6 information. If you do not specify this keyword, the command displays IPv4 information.

public-instance: Specifies the public instance.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters.

count: Displays the number of entries in the routing table. If you do not specify this keyword, the command displays detailed information about the routing table.

Examples

Display the EVPN IPv4 routing table for VPN instance **vpn1**.

```
<Switch> display evpn routing-table vpn-instance vpn1

VPN instance name: vpn1                              Local L3VNI: 7
IP address          Nexthop            Outgoing interface       NibID
10.1.1.11           1.1.1.1            Vsi-interface3           0x18000000
10.1.1.12           2.2.2.2            Vsi-interface3           0x18000001
```

Display the EVPN IPv4 routing table for the public instance.

```
<Switch> display evpn routing-table public-instance

Public instance                                      Local L3VNI: 3900
IP address          Nexthop            Outgoing interface       NibID
10.1.1.11           1.1.1.1            Vsi-interface3           0x18000000
10.1.1.12           2.2.2.2            Vsi-interface3           0x18000001
```

Display the number of EVPN route entries in the IPv4 routing table for VPN instance **vpn1**.

```
<Switch> display evpn routing-table vpn-instance vpn1 count
Total number of entries: 2
```

Display the EVPN IPv6 routing table for VPN instance **vpna**.

```
<Switch> display evpn routing-table ipv6 vpn-instance vpna

VPN instance: vpna                                   Local L3VNI: 7
IPv6 address        :      BC10:0300:1000:0020:0200:0300:0100:0034
Next hop            :      1.1.1.1
Outgoing interface  :      Vsi-interface3
NibID               :      0x18000000

IPv6 address        :      BC10:0300:1000:0020:0200:0300:0100:0035
```

```
Next hop            :       2.2.2.2
Outgoing interface  :       Vsi-interface3
NibID               :       0x18000001
```

Table 1-18 Command output

Field	Description
Local L3VNI	L3 VXLAN ID associated with the VPN instance or the public instance.
NibID	Next hop ID.

1.1.21. evpn m-lag group

Use **evpn m-lag group** to enable EVPN M-LAG and specify the virtual VTEP address.

Use **undo evpn m-lag group** to restore the default.

Syntax

evpn m-lag group *virtual-vtep-ip*

undo evpn m-lag group

Default

EVPN M-LAG is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

virtual-vtep-ip: Specifies the virtual VTEP address.

Usage guidelines

EVPN M-LAG virtualizes two VTEPs or EVPN gateways into one M-LAG system to avoid single points of failure. The VTEPs or EVPN gateways use a virtual VTEP address to establish VXLAN tunnels to remote devices.

For the device to re-establish VXLAN tunnels, you must execute the **address-family l2vpn evpn** command in BGP instance view after you enable or disable EVPN M-LAG.

To modify the virtual VTEP address, you must first delete the original virtual VTEP address.

Examples

Enable EVPN M-LAG and specify the virtual VTEP address as 1.1.1.1.

```
<Sysname> system-view
[Sysname] evpn m-lag group 1.1.1.1
```

1.1.22. evpn m-lag local

Use **evpn m-lag local** to specify the IP addresses of the VTEPs in a M-LAG system.

Use **undo evpn m-lag local** to restore the default.

Syntax

evpn m-lag local *local-ip* **remote** *remote-ip*

undo evpn m-lag local

Default

The IP addresses of the VTEPs in a M-LAG system are not specified.

Views

System view

Predefined user roles

network-admin

Parameters

local *local-ip*: Specifies the IP address of the local VTEP.

remote *remote-ip*: Specifies the IP address of the peer VTEP.

Usage guidelines

An AC that is attached to only one of the VTEPs in a M-LAG system is called a single-armed AC. After you configure this command, each VTEP in a M-LAG system changes the next hop of the routes for single-armed ACs to its local VTEP IP address when advertising the routes. This ensures that the traffic of a single-armed AC is forwarded to its attached VTEP. When a VTEP receives BGP EVPN routes from the peer VTEP IP address specified by using this command, it does not set up a VXLAN tunnel to the peer VTEP.

You must execute this command if single-armed ACs are attached to a M-LAG system that uses an Ethernet aggregate link as the peer-link. You do not need to execute this command on a M-LAG system that uses a VXLAN tunnel as the peer-link. In such a M-LAG system, a VTEP uses the source IP address of the peer-link as the next hop of routes for single-armed ACs to ensure correct traffic forwarding.

When you execute this command, make sure the IP address of the local VTEP belongs to a local interface. Make sure the local VTEP IP address and peer VTEP IP address are reversed on the VTEPs in a M-LAG system.

Examples

Specify the IP addresses of the local and peer VTEPs in the M-LAG system as 2.2.2.2 and 3.3.3.3, respectively.

```
<Sysname> system-view
[Sysname] evpn m-lag local 2.2.2.2 remote 3.3.3.3
```

1.1.23. evpn encapsulation

Use **evpn encapsulation** to create an EVPN instance on a VSI and enter its view, or enter the view of the existing EVPN instance on a VSI.

Use **undo evpn encapsulation** to restore the default.

Syntax

evpn encapsulation vxlan

undo evpn encapsulation

Default

No EVPN instance exists.

Views

VSI view

Predefined user roles

network-admin

Parameters

vxlan: Specifies VXLAN encapsulation.

Usage guidelines

Before you can configure EVPN settings, you must create an EVPN instance.

Examples

Create an EVPN instance on VSI **aaa** and enter its view.

```
<Switch> system-view
[Switch] vsi aaa
[Switch-vsi-aaa] evpn encapsulation vxlan
[Switch-vsi-aaa-evpn-vxlan]
```

1.1.24. evpn global-mac

Use **evpn global-mac** to configure the EVPN global MAC address.

Use **undo evpn global-mac** to restore the default.

Syntax

evpn global-mac *mac-address*

undo evpn global-mac

Default

No EVPN global MAC address is configured.

Views

System view

Predefined user roles

network-admin

Parameters

mac-address: Specifies a MAC address in H-H-H format. Do not specify a multicast MAC address, broadcast MAC address, or all-zeros MAC address.

Usage guidelines

The EVPN global MAC address is used only by VSI interfaces associated with an L3 VXLAN ID.

For a VSI interface associated with an L3 VXLAN ID, the MAC address assigned to it by using the **mac-address** command takes precedence over the EVPN global MAC address.

Examples

Configure the EVPN global MAC address as **0001-0001-0001**.

```
<Sysname> system-view
[Sysname] evpn global-mac 1-1-1
```

1.1.25. evpn route arp-mobility suppression

Use **evpn route arp-mobility suppression** to enable ARP mobility event suppression.

Use **undo evpn route arp-mobility suppression** to disable ARP mobility event suppression.

Syntax

evpn route arp-mobility suppression

undo evpn route arp-mobility suppression

Default

ARP mobility event suppression is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

On an EVPN VXLAN network, misconfiguration of IP addresses might cause two sites to contain the same IP address. In this condition, VTEPs at the two sites constantly synchronize and update EVPN ARP entries and determine that ARP mobility events occur. As a result, an inter-site loop might occur, and the bandwidth is occupied by ARP entry synchronization traffic. To eliminate loops and suppress those ARP mobility events, enable ARP mobility event suppression on the VTEPs. This feature allows an IP address to move at most four times from a site within 180 seconds. If an IP address moves more than four times within 180 seconds, the VTEP at the site will suppress the excess ARP mobility events and will not advertise ARP information for the IP address.

After you execute the **undo evpn route arp-mobility suppression** command, a VTEP acts as follows:

- Advertises ARP information immediately for the suppressed ARP entries that have not aged out.
- Relearns ARP information for the suppressed ARP entries that have aged out and advertises the ARP information.

ARP mobility event suppression takes effect only on the following networks:

- EVPN VXLAN network enabled with ARP flood suppression.
- EVPN VXLAN network configured with distributed VXLAN IP gateways.

Examples

Enable ARP mobility event suppression.

```
<Switch> system-view
[Switch] evpn route arp-mobility suppression
```

Related commands

display evpn route arp-mobility

1.1.26. evpn route mac-mobility suppression

Use **evpn route mac-mobility suppression** to enable MAC mobility event suppression.

Use **undo evpn route mac-mobility suppression** to disable MAC mobility event suppression.

Syntax

evpn route mac-mobility suppression

undo evpn route mac-mobility suppression

Default

MAC mobility event suppression is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

On an EVPN VXLAN network, misconfiguration of MAC addresses might cause two sites to contain the same MAC address. In this condition, VTEPs at the two sites constantly synchronize and update EVPN MAC entries and determine that MAC mobility events occur. As a result, an inter-site loop might occur, and the bandwidth is occupied by MAC entry synchronization traffic. To eliminate loops and suppress those MAC mobility events, enable MAC mobility event suppression on the VTEPs. This feature allows an IP address to move at most four times from a site within 180 seconds. If an IP address moves more than four times within 180 seconds, the VTEP at the site will suppress the excess MAC mobility events and will not advertise information about the MAC address.

After you execute the **undo evpn route mac-mobility suppression** command, a VTEP acts as follows:

- Advertises MAC address entries immediately for the suppressed MAC address entries that have not aged out.
- Relearns the MAC addresses for the suppressed MAC address entries that have aged out and advertises the MAC address entries.

Examples

Enable MAC mobility event suppression.

```
<Switch> system-view
[Switch] evpn route mac-mobility suppression
```

Related commands

display evpn route mac-mobility

1.1.27. export route-policy

Use **export route-policy** to apply an export routing policy to EVPN on a VPN instance.

Use **undo export route-policy** to restore the default.

Syntax

export route-policy *route-policy*

undo export route-policy

Default

No export routing policy is applied to EVPN on a VPN instance.

Views

VPN instance EVPN view

Predefined user roles

network-admin

Parameters

route-policy: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters.

Usage guidelines

You can specify an export routing policy to filter advertised routes or modify their route attributes for EVPN.

If you execute this command multiple times, the most recent configuration takes effect.

EVPN can use an export routing policy specified in VPN instance view or in VPN instance EVPN view. Export routing policy configuration in VPN instance EVPN view takes precedence over that in VPN instance view.

Examples

Apply export routing policy **poly-1** to EVPN on VPN instance **vpn1**.

```
<Switch> system-view
[Switch] ip vpn-instance vpn1
[Switch-vpn-instance-vpn1] address-family evpn
[Switch-vpn-evpn-vpn1] export route-policy poly-1
```

Related commands

route-policy (*Layer 3—IP Routing Command Reference*)

1.1.28. import evpn mac-ip

Use **import evpn mac-ip** to enable the device to redistribute received MAC/IP advertisement routes that contain ARP or ND information into a BGP unicast routing table.

Use **undo import evpn mac-ip** to disable the device from redistributing received MAC/IP advertisement routes that contain ARP or ND information into a BGP unicast routing table.

Syntax

import evpn mac-ip

undo import evpn mac-ip

Default

MAC/IP advertisement routes that contain ARP or ND information are not redistributed into any BGP unicast routing table.

Views

BGP IPv4 unicast address family view

BGP IPv6 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP-VPN IPv6 unicast address family view

Predefined user roles

network-admin

Usage guidelines

This command enables the device to redistribute received MAC/IP advertisement routes that contain ARP or ND information into a BGP unicast routing table.

- If you use this command in BGP IPv4 or IPv6 unicast address family view, the device will redistribute the routes into the BGP IPv4 or IPv6 unicast routing table. In addition, the device will advertise the routes to the local site.
- If you use this command in BGP-VPN IPv4 or IPv6 unicast address family view, the device will redistribute the routes into the BGP-VPN IPv4 or IPv6 unicast routing table of the corresponding VPN instance. To advertise the routes to the local site, you must configure the **advertise l2vpn evpn** command.

Examples

Redistribute received MAC/IP advertisement routes into the BGP-VPN IPv4 unicast routing table of VPN instance **vpna**.

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default] ip vpn-instance vpna
[Switch-bgp-default-vpna] address-family ipv4
[Switch-bgp-default-ipv4-vpna] import evpn mac-ip
```

Related commands

advertise l2vpn evpn

1.1.29. import route-policy

Use **import route-policy** to apply an import routing policy to EVPN on a VPN instance.

Use **undo import route-policy** to restore the default.

Syntax

import route-policy *route-policy*

undo import route-policy

Default

No import routing policy is applied to EVPN on a VPN instance. The VPN instance accepts a route when the export route targets of the route match local import route targets.

Views

VPN instance EVPN view

Predefined user roles

network-admin

Parameters

route-policy: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters.

Usage guidelines

You can specify an import routing policy to filter received routes or modify their route attributes for EVPN.

If you execute this command multiple times, the most recent configuration takes effect.

EVPN can use an import routing policy specified in VPN instance view or in VPN instance EVPN view. Import routing policy configuration in VPN instance EVPN view takes precedence over that in VPN instance view.

Examples

Apply import routing policy **poly-1** to EVPN on VPN instance **vpn1**.

```
<Switch> system-view
[Switch] ip vpn-instance vpn1
[Switch-vpn-instance-vpn1] address-family evpn
[Switch-vpn-evpn-vpn1] import route-policy poly-1
```

Related commands

route-policy (*Layer 3—IP Routing Command Reference*)

1.1.30. ip forwarding-conversational-learning

Use **ip forwarding-conversational-learning** to enable conversational learning for host route FIB entries.

Use **undo ip forwarding-conversational-learning** to disable conversational learning for host route FIB entries.

Syntax

ip forwarding-conversational-learning [**aging** *aging-time*]

undo ip forwarding-conversational-learning

Default

Conversational learning is disabled for host route FIB entries.

Views

System view

Predefined user roles

network-admin

Parameters

aging *aging-time*: Specifies an aging timer in minutes for host route FIB entries, in the range of 60 to 1440. The default value is 60.

Usage guidelines

Use this command only on an EVPN network.

By default, the device issues a host route FIB entry to the hardware after the entry is generated. This feature enables the device to issue a host route FIB entry to the hardware only when the entry is required for packet forwarding. This feature saves hardware resources on the device.

Set an appropriate aging timer for host route FIB entries according to your network. A much longer or shorter aging timer will degrade the device performance.

- If the aging timer is too long, the device will save many outdated host route FIB entries and fail to accommodate the most recent network changes. These entries cannot be used for correct packet forwarding and exhaust FIB resources.
- If the aging timer is too short, the device will delete the valid host route FIB entries that can still be effective for packet forwarding. As a result, FIB entry flapping will occur, and the device performance will be affected.

1.1.31. ip-prefix-route generate disable

Use **ip-prefix-route generate disable** to disable generation of IP prefix advertisement routes for the subnets of a VSI interface.

Use **undo ip-prefix-route generate disable** to enable generation of IP prefix advertisement routes for the subnets of a VSI interface.

Syntax

ip-prefix-route generate disable

undo ip-prefix-route generate disable

Default

The device only generates MAC/IP advertisement routes for a VSI interface that provides centralized VXLAN IP gateway service. The device generates IP prefix advertisement routes for the subnets of a VSI interface that provides distributed VXLAN IP gateway service.

Views

VSI interface view

Predefined user roles

network-admin

Usage guidelines

This command takes effect only on a VSI interface that provides distributed VXLAN IP gateway service (configured by using the **distributed-gateway local** command). It does not take effect on VSI interfaces that provide centralized VXLAN IP gateway service.

Examples

Disable generation of IP prefix advertisement routes for the subnets of VSI-interface 1.

```
<Switch> system-view
[Switch] interface vsi-interface 1
[Switch-Vsi-interface1] ip-prefix-route generate disable
```

1.1.32. l2vpn m-lag peer-link ac-match-rule vxlan-mapping

Use **l2vpn m-lag peer-link ac-match-rule vxlan-mapping** to enable the device to create frame match criteria based on VXLAN IDs for the dynamic ACs on the Ethernet aggregate link peer-link.

Use **undo l2vpn m-lag peer-link ac-match-rule vxlan-mapping** to restore the default.

Syntax

l2vpn m-lag peer-link ac-match-rule vxlan-mapping

undo l2vpn m-lag peer-link ac-match-rule vxlan-mapping

Default

On a M-LAG system that uses an Ethernet aggregate link as the peer-link, dynamic ACs on the peer-link use frame match criteria that are identical to those of site-facing ACs.

Views

System view

Predefined user roles

network-admin

Usage guidelines

By default, if a M-LAG system uses an Ethernet aggregate link as the peer-link, each M-LAG member device creates a dynamic AC on the peer-link when an AC is configured on a site-facing interface. The dynamic AC and the site-facing AC have the same frame match criteria and VSI mapping. If two site-facing ACs on different interfaces have the same frame match criteria but different VSI mappings, the dynamic ACs created for the site-facing ACs will conflict with each other. To prevent this issue, enable the M-LAG member devices to create frame match criteria based on VXLAN IDs for the dynamic ACs on the peer-link.

With this command configured, a M-LAG member device creates dynamic ACs on the peer-link and maps them to the VSIs of VXLANs after the VXLANs are created. The matching VLAN IDs in frame match criteria are calculated for the dynamic ACs according to the following rules:

- Outer VLAN ID = VXLAN ID / 4094 + 1.
- Inner VLAN ID = VXLAN ID % 4094 + 1.
- If the calculated outer VLAN ID of a dynamic AC is the PVID of the peer-link interface, the device uses the calculated inner VLAN ID as the outer VLAN ID. The device does not add a matching inner VLAN ID to the frame match criterion of the dynamic AC.

After you execute this command, do not create VXLANs with IDs larger than 16000000.

This command deletes existing dynamic ACs from peer-link interface and takes effect on all VXLANs.

Examples

Enable the device to create frame match criteria based on VXLAN IDs for the dynamic ACs on the Ethernet aggregate link peer-link.

```
<Sysname> system-view
[Sysname] l2vpn m-lag peer-link ac-match-rule vxlan-mapping
```

1.1.33. l2vpn statistics vsi l3-vni

Use **l2vpn statistics vsi l3-vni** to enable traffic statistics for the VSIs that are automatically created for L3 VXLAN IDs.

Use **undo l2vpn l3-vni vsi statistics** to disable traffic statistics for the VSIs that are automatically created for L3 VXLAN IDs.

Syntax

l2vpn statistics vsi l3-vni

undo l2vpn statistics vsi l3-vni

Default

The traffic statistics feature is disabled for the VSIs that are automatically created for L3 VXLAN IDs.

Views

System view

Predefined user roles

network-admin

Usage guidelines

If you configure an L3 VXLAN ID on a distributed EVPN gateway, the gateway automatically creates a VSI for the L3 VXLAN ID. You cannot enter the view of such a VSI to configure settings on it.

This command enables the device to collect incoming and outgoing traffic statistics for the automatically created VSIs. You can use the **display l2vpn vsi verbose** command to view the traffic statistics and use the **reset l2vpn statistics vsi** command to clear the traffic statistics.

Examples

Enable traffic statistics for the VSIs that are automatically created for L3 VXLAN IDs.

```
<Sysname> system-view
[Sysname] l2vpn statistics vsi l3-vni
```

Related commands

display l2vpn vsi verbose (*VXLAN Command Reference*)

reset l2vpn statistics vsi (*VXLAN Command Reference*)

1.1.34. l3-vni

Use **l3-vni** to configure an L3 VXLAN ID for a VSI interface or for the public instance.

Use **undo l3-vni** to remove the L3 VXLAN ID for a VSI interface or for the public instance.

Syntax

l3-vni *vxlan-id*

undo l3-vni

Default

No L3 VXLAN ID is configured for a VSI interface or for the public instance.

Views

VSI interface view

Public instance view

Predefined user roles

network-admin

Parameters

vxlan-id: Specifies a VXLAN ID. The value range for this argument is 0 to 16777215.

Usage guidelines

On distributed EVPN gateways, you must configure L3 VXLAN IDs for the gateways to differentiate traffic of different VPN instances.

To forward Layer 3 traffic of a VPN instance, you must assign an L3 VXLAN ID to the VSI interface of the VPN instance. To forward Layer 3 traffic of the public network, you must assign the same L3 VXLAN ID to the public instance and the VSI interface of the public instance.

To modify the L3 VXLAN ID for the public instance, you must first delete the original L3 VXLAN ID.

The L3 VXLAN ID specified by using this command cannot be the same as any VXLAN ID specified by using the **mapping vni** command.

Examples

Configure the L3 VXLAN ID as 1000 for VSI-interface 100.

```
<Switch> system-view
[Switch] interface vsi-interface 100
[Switch-Vsi-interface100] l3-vni 1000
```

1.1.35. mac-advertising disable

Use **mac-advertising disable** to disable MAC address advertisement and withdraw advertised MAC addresses.

Use **undo mac-advertising disable** to restore the default.

Syntax

mac-advertising disable

undo mac-advertising disable

Default

MAC address advertisement is enabled.

Views

VSI EVPN instance view

Predefined user roles

network-admin

Usage guidelines

The MAC information and ARP information advertised by the VTEP overlap. To avoid duplication, use this command to disable MAC address advertisement and withdraw the MAC addresses advertised to remote VTEPs.

Examples

Disable MAC address advertisement and withdraw advertised MAC addresses for a VSI EVPN instance.

```
<Switch> system-view
[Switch] vsi aaa
[Switch-vsi-aaa] evpn encapsulation vxlan
[Switch-vsi-aaa-evpn-vxlan] mac-advertising disable
```

1.1.36. nd mac-learning disable

Use **nd mac-learning disable** to disable an EVPN instance from learning MAC addresses from ND information.

Use **undo nd mac-learning disable** to restore the default.

Syntax

nd mac-learning disable

undo nd mac-learning disable

Default

An EVPN instance learns MAC addresses from ND information.

Views

EVPN instance view

Predefined user roles

network-admin

Usage guidelines

The MAC information and ND information advertised by a remote VTEP overlap. To avoid duplication, use this command to disable the learning of MAC addresses from ND information. EVPN will learn remote MAC addresses only from the MAC information advertised from remote sites.

Examples

Disable an EVPN instance from learning MAC addresses from ND information.

```
<Switch> system-view
[Switch] vsi aaa
[Switch-vsi-aaa] evpn encapsulation vxlan
[Switch-vsi-aaa-evpn-vxlan] nd mac-learning disable
```

1.1.37. policy vpn-target

Use **policy vpn-target** to enable route target filtering for BGP EVPN routes.

Use **undo policy vpn-target** to disable route target filtering for BGP EVPN routes.

Syntax

policy vpn-target

undo policy vpn-target

Default

Route target filtering is enabled for BGP EVPN routes.

Views

BGP EVPN address family view

Predefined user roles

network-admin

Usage guidelines

When route target filtering is enabled for BGP EVPN routes, the EVPN routing table accepts only BGP EVPN routes of which the export route targets match the local import route targets. If the device must save all BGP EVPN routes, use the **undo policy vpn-target** command to disable route target filtering for BGP EVPN routes.

Examples

Disable route target filtering for BGP EVPN routes.

```
<Switch> system-view
[Switch] bgp 100
[Switch-bgp-default] address-family l2vpn evpn
[Switch-bgp-default-evpn] undo policy vpn-target
```

1.1.38. route-distinguisher (EVPN instance view)

Use **route-distinguisher** to configure an RD for an EVPN instance.

Use **undo route-distinguisher** to restore the default.

Syntax

route-distinguisher { *route-distinguisher* | **auto** }

undo route-distinguisher

Default

No RD is configured for an EVPN instance.

Views

EVPN instance view

Predefined user roles

network-admin

Parameters

route-distinguisher: Specifies an RD, a string of 3 to 21 characters. The RD cannot be all zeros and can use one of the following formats:

- *16-bit AS number:32-bit user-defined number*. For example, 101:3.
- *32-bit IP address:16-bit user-defined number*. For example, 192.168.122.15:1.
- *32-bit AS number:16-bit user-defined number*. For example, 65536:1. The AS number must be equal to or greater than 65536.

auto: Automatically generates an RD in the *N:VXLAN ID* format. The initial value of *N* is 1. If *N:VXLAN ID* is already in use, the system increases the value of *N* by 1 until the RD is available.

Usage guidelines

EVPN uses MP-BGP to advertise BGP EVPN routes for automatic VTEP discovery, MAC reachability information advertisement, and host route advertisement. MP-BGP uses the RD to differentiate BGP EVPN routes of different EVPN instances.

Examples

Configure 22:1 as the RD of an EVPN instance.

```
<Switch> system-view
[Switch] vsi aaa
[Switch-vsi-aaa] evpn encapsulation vxlan
[Switch-vsi-aaa-evpn-vxlan] route-distinguisher 22:1
```

1.1.39. route-distinguisher (public instance view)

Use **route-distinguisher** to configure an RD for the public instance.

Use **undo route-distinguisher** to restore the default.

Syntax

route-distinguisher *route-distinguisher*

undo route-distinguisher

Default

No RD is configured for the public instance.

Views

Public instance view

Predefined user roles

network-admin

Parameters

route-distinguisher: Specifies an RD, a string of 3 to 21 characters. The RD can use one of the following formats:

- *16-bit AS number:32-bit user-defined number*. For example, 101:3.
- *32-bit IP address:16-bit user-defined number*. For example, 192.168.122.15:1.
- *32-bit AS number:16-bit user-defined number*. For example, 65536:1. The AS number must be equal to or greater than 65536.

Usage guidelines

To modify the RD of the public instance, first execute the **undo route-distinguisher** command to remove the original RD.

Examples

Configure 22:1 as the RD of the public instance.

```
<Switch> system-view
[Switch] ip public-instance
[Switch-public-instance] route-distinguisher 22:1
```

1.1.40. route-distinguisher

Use **route-distinguisher** to configure an RD for an EVPN instance or the public instance.

Use **undo route-distinguisher** to restore the default.

Syntax

In public instance view:

route-distinguisher *route-distinguisher*

undo route-distinguisher

In VSI EVPN instance view:

route-distinguisher { *route-distinguisher* | **auto** [**router-id**] }

undo route-distinguisher

Default

No RD is configured for an EVPN instance or the public instance.

Views

Public instance view

VSI EVPN instance view

Predefined user roles

network-admin

Parameters

route-distinguisher: Specifies an RD, a string of 3 to 21 characters. The RD cannot be all zeros and can use one of the following formats:

- *16-bit AS number:32-bit user-defined number*. For example, 101:3.
- *32-bit IP address:16-bit user-defined number*. For example, 192.168.122.15:1.

- *32-bit AS number:16-bit user-defined number*. For example, 65536:1. The AS number must be equal to or greater than 65536.

auto: Automatically generates an RD in the *N:VXLAN ID* format. The initial value of *N* is 1. If *N:VXLAN ID* is already in use, the system increases the value of *N* by 1 until the RD is available.

router-id: Automatically generates an RD based on the router ID in the *Router ID*:*N* format. The initial value of *N* is 1. If *Router ID*:*N* is already in use, the system increases the value of *N* by 1 until the RD is available. If you do not specify this keyword with the **auto** keyword, the system automatically generates an RD based on the VXLAN ID in the *N*:*VXLAN ID* format.

Usage guidelines

EVPN uses MP-BGP to advertise BGP EVPN routes for automatic VTEP discovery, MAC reachability information advertisement, and host route advertisement. MP-BGP uses the RD to differentiate BGP EVPN routes of different EVPN instances.

To modify the RD of an EVPN instance or the public instance, first execute the **undo route-distinguisher** command to remove the original RD.

Examples

Configure 22:1 as the RD of the EVPN instance on VSI **aaa**.

```
<Switch> system-view
[Switch] vsi aaa
[Switch-vsi-aaa] evpn encapsulation vxlan
[Switch-vsi-aaa-evpn-vxlan] route-distinguisher 22:1
```

1.1.41. vpn-target

Use **vpn-target** to configure route targets for EVPN.

Use **undo vpn-target** to delete route targets for EVPN.

Syntax

In VSI EVPN instance view:

vpn-target { *vpn-target&<1-8>* | **auto** } * [**both** | **export-extcommunity** | **import-extcommunity**]

undo vpn-target { *vpn-target&<1-8>* | **auto** | **all** } [**both** | **export-extcommunity** | **import-extcommunity**]

In EVPN view of a VPN instance, public instance view, IPv4 VPN view of the public instance, IPv6 VPN view of the public instance, or EVPN view of the public instance:

vpn-target *vpn-target&<1-8>* [**both** | **export-extcommunity** | **import-extcommunity**]

undo vpn-target { **all** | *vpn-target&<1-8>* [**both** | **export-extcommunity** | **import-extcommunity**] }

Default

EVPN does not have route targets.

Views

VSI EVPN instance view

EVPN view of a VPN instance

Public instance view

EVPN view of the public instance

IPv4 VPN view of the public instance

IPv6 VPN view of the public instance

Predefined user roles

network-admin

Parameters

vpn-target&<1-8>: Specifies a space-separated list of up to eight route targets. Each route target is a string of 3 to 21 characters in one of the following formats:

- *16-bit AS number:32-bit user-defined number*. For example, 101:3.
- *32-bit IP address:16-bit user-defined number*. For example, 192.168.122.15:1.
- *32-bit AS number:16-bit user-defined number*. For example, 65536:1. The AS number must be equal to or greater than 65536.

auto: Automatically generates a route target in the format of *BGP AS number:VXLAN ID*.

both: Uses the specified route targets as both import and export targets. If you do not specify the **both**, **export-extcommunity**, or **import-extcommunity** keyword, the **both** keyword applies.

export-extcommunity: Uses the specified route targets as export targets.

import-extcommunity: Uses the specified route targets as import targets.

all: Specifies all route targets.

Usage guidelines

EVPN uses MP-BGP to advertise BGP EVPN routes for automatic VTEP discovery, MAC reachability information advertisement, and host route advertisement. MP-BGP uses route targets to control the advertisement and acceptance of BGP EVPN routes.

A VTEP sets the export targets for BGP EVPN routes before advertising the routes to remote VTEPs. The VTEP checks the export targets of BGP EVPN routes from remote VTEPs and imports only BGP EVPN routes of which the export targets match the local import targets.

Examples

Configure import route targets 10:1, 100:1, and 1000:1 for the EVPN instance on VSI **aaa**.

```
<Switch> system-view
[Switch] vsi aaa
[Switch-vsi-aaa] evpn encapsulation vxlan
[Switch-vsi-aaa-evpn-vxlan] vpn-target 10:1 100:1 1000:1 import-extcommunity
```

Contents

A page of this section is **14-x-x**

2. MVXLAN commands ····· 2-1
2.1. MVXLAN commands ····· 2-1
2.1.1. address-family ipv4 ····· 2-1
2.1.2. data-delay ····· 2-1
2.1.3. data-group ····· 2-2
2.1.4. default-group ····· 2-3
2.1.5. display multicast-vpn vxlan data-group receive ····· 2-4
2.1.6. display multicast-vpn vxlan data-group send ····· 2-6
2.1.7. display multicast-vpn vxlan default-group ····· 2-7
2.1.8. multicast extranet select-rpf ····· 2-8
2.1.9. multicast-vpn vxlan edge remote ····· 2-10
2.1.10. multicast-vpn vxlan public-instance ····· 2-10
2.1.11. multicast-vpn vxlan vpn-instance ····· 2-11
2.1.12. pim distributed-dr ····· 2-12
2.1.13. s-pmsi advertise source-active ····· 2-12
2.1.14. source ····· 2-13

2. MVXLAN commands

NOTE:

MVXLAN commands are being supported with after Ver7.4.27.

The MVXLAN commands are only supported when used in combination with UNIVERGE Network Operation Engine Overlay Network Extension.

2.1. MVXLAN commands

2.1.1. address-family ipv4

Use **address-family ipv4** to create an MVXLAN IPv4 address family and enter its view, or enter the view of the existing MVXLAN IPv4 address family.

Use **undo address-family ipv4** to delete the MVXLAN IPv4 address family and all settings in MVXLAN IPv4 address family view.

Syntax

address-family ipv4

undo address-family ipv4

Default

No MVXLAN IPv4 address family exists.

Views

MVXLAN view

Predefined user roles

network-admin

Examples

In MVXLAN view of VPN instance vpna, create an MVXLAN IPv4 address family and enter its view.

```
<Switch> system-view
[Switch] multicast-vpn vxlan vpn-instance vpna mode mdt
[Switch-mvxlan-vpna] address-family ipv4
[Switch-mvxlan-vpna-ipv4]
```

2.1.2. data-delay

Use **data-delay** to set the data-delay period (delay period before the device switches over from the default MDT to the data MDT).

Use **undo data-delay** to restore the default.

Syntax

data-delay *delay*

undo data-delay

Default

The data-delay period is 3 seconds.

Views

MVXLAN IPv4 address family view

Predefined user roles

network-admin

Parameters

delay: Specifies a data-delay period in the range of 1 to 60 seconds.

Examples

In MVXLAN IPv4 address family view of VPN instance vpna, set the data-delay period to 10 seconds.

```
<Switch> system-view
[Switch] multicast-vpn vxlan vpn-instance vpna mode mdt
[Switch-mvxlan-vpna] address-family ipv4
[Switch-mvxlan-vpna-ipv4] data-delay 10
```

2.1.3. data-group

Use **data-group** to specify a data group range and optionally configure the criteria for the device to initiate a switchover of the default MDT to a data MDT.

Use **undo data-group** to restore the default.

Syntax

data-group *group-address* { *mask-length* | *mask* } [**acl** *acl-number* | **name** *acl-name*]

undo data-group

Default

No data group range exists, and the device never initiates a switchover of the default MDT to a data MDT.

Views

MVXLAN IPv4 address family view

Predefined user roles

network-admin

Parameters

group-address: Specifies a multicast group address in the range of 224.0.1.0 to 239.255.255.255.

mask-length: Specifies a mask length for the multicast group address. The value range for this argument is 27 to 32.

mask: Specifies a subnet mask for the multicast group address. The value range for this argument is 255.255.255.224 to 255.255.255.255.

acl *acl-number*: Specifies an advanced ACL by its number in the range of 3000 to 3999.

name *acl-name*: Specifies a basic or advanced ACL by its name, a case-insensitive string of 1 to 63 characters. The name must start with a letter and cannot be **all**.

Usage guidelines

This command enables the device to initiate a switchover of the default MDT to a data MDT if the multicast data permitted by the specified ACL keeps arriving for a data-delay period.

The specified ACL matches traffic according to the following rules:

- A basic ACL uses the **source** keyword in an ACL rule to match multicast traffic by the multicast source address. All optional parameters are ignored, except **source**, **fragment**, and **time-range**.
- An advanced ACL uses the **source** and **destination** keywords in an ACL rule to match multicast traffic by the multicast source address and the multicast group address. All optional parameters are ignored, except **source**, **destination**, **fragment**, and **time-range**.

On a VTEP, the data group range for an MVXLAN cannot include the default group or data groups of any other MVXLAN.

If you specify an ACL, the multicast data permitted by the ACL can trigger the switchover. If you do not specify an ACL, any multicast data can trigger the switchover.

If you execute this command multiple times in the same MVXLAN IPv4 address family view, the most recent configuration takes effect.

Examples

In MVXLAN IPv4 address family view of VPN instance vpna, specify 239.1.0.0 through 239.1.0.255 as the data group range.

```
<Switch> system-view
[Switch] multicast-vpn vxlan vpn-instance vpna mode mdt
[Switch-mvxlan-vpna] address-family ipv4
[Switch-mvxlan-vpna-ipv4] data-group 239.1.0.0 32
```

2.1.4. default-group

Use **default-group** to specify a default group.

Use **undo default-group** to restore the default.

Syntax

default-group *group-address*

undo default-group

Default

No default group exists.

Views

MVXLAN IPv4 address family view

Predefined user roles

network-admin

Parameters

group-address: Specifies a default group in the range of 224.0.1.0 to 239.255.255.255.

Usage guidelines

The default group for an MVXLAN must be different from the default group and the data group used by any other MVXLAN.

Examples

In MVXLAN IPv4 address family view of VPN instance vpna, specify 236.0.0.1 as the default group.

```
<Switch> system-view
[Switch] multicast-vpn vxlan vpn-instance vpna mode mdt
[Switch-mvxlan-vpna] address-family ipv4
[Switch-mvxlan-vpna-ipv4] default-group 236.0.0.1
```

2.1.5. display multicast-vpn vxlan data-group receive

Use **display multicast-vpn vxlan data-group receive** to display received data group information in an MVXLAN.

Syntax

display multicast-vpn vxlan { **vpn-instance** *instance-name* | **public-instance** } **data-group receive** [**brief** | [**active** | **group** *group-address* | **sender** *source-address* | *vpn-source-address* [**mask** { *mask-length* | *mask* }] | *vpn-group-address* [**mask** { *mask-length* | *mask* }]] *]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vpn-instance *instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters.

public-instance: Specifies the public instance.

brief: Displays brief information. If you do not specify this keyword, the command displays detailed information.

active: Specifies data groups that have joined the data MDT.

group *group-address*: Specifies a data group by its IP address in the range of 224.0.1.0 to 239.255.255.255.

sender *source-address*: Specifies an MVXLAN source interface by its IP address.

vpn-source-address: Specifies a multicast source address of the specified VPN instance.

vpn-group-address: Specifies a multicast group address of the specified VPN instance. The value range for this argument is 224.0.1.0 to 239.255.255.255.

mask-length: Specifies a mask length of the specified multicast source address or multicast group address. The value range for this argument is 0 to 32, and the default is 32.

mask: Specifies a subnet mask of the specified multicast source address or multicast group address. The default is 255.255.255.255.

Usage guidelines

If you do not specify any parameters, this command displays detailed information about all received data groups in the MVXLAN of the specified VPN instance or the public instance.

Examples

Display detailed information about received data groups in the MVXLAN of VPN instance vpna.

```
<Switch> display multicast-vpn vxlan vpn-instance vpna data-group receive
VPN instance: vpna
Total 2 data-groups for 8 entries
Total 2 data-groups and 8 entries matched

Data-group: 226.1.1.0  Reference count: 4   Active count: 2
  Sender: 1.1.1.1   Active count: 1
    (192.6.1.5, 239.1.1.1)       Remaining lifetime: 00:03:10 active
    (192.6.1.5, 239.1.1.158)     Remaining lifetime: 00:03:10
  Sender: 181.100.1.1   Active count: 1
    (195.6.1.2, 239.1.2.12)      Remaining lifetime: 00:03:10 active
    (195.6.1.2, 239.1.2.197)     Remaining lifetime: 00:03:10

Data-group: 229.1.1.0   Reference count: 4   Active count: 2
  Sender: 185.100.1.1   Active count: 1
    (198.6.1.5, 239.1.3.62)      Remaining lifetime: 00:03:10 active
    (198.6.1.5, 225.1.1.109)     Remaining lifetime: 00:03:10
  Sender: 190.100.1.1   Active count: 1
    (200.6.1.2, 225.1.4.80)      Remaining lifetime: 00:03:10 active
    (200.6.1.2, 225.1.4.173)     Remaining lifetime: 00:03:10
```

Display brief information about received data groups in the MVXLAN of VPN instance vpna.

```
<Switch> display multicast-vpn vxlan vpn-instance vpna data-group receive brief
VPN instance: vpna
Total 2 data-groups for 8 entries
Total 2 data-groups and 8 entries matched

Data-group: 226.1.1.0   Reference count: 4   Active count: 2
Data-group: 229.1.1.0   Reference count: 4   Active count: 2
```

Table 1 Command output

Field	Description
Total 2 data-groups for 8 entries	A total of 2 data groups, associated with 8 (S, G) entries.
Total 2 data-groups and 8 entries matched	A total of 2 matching data groups, associated with 8 (S, G) entries.
Data-group	IP address of the received data group.
Reference count	Number of (S, G) entries that use the data group in the VPN instance.
Active count	Number of active (S, G) entries (entries with active receivers) that use the data group in the VPN instance.
Sender	Address of the VTEP that sent the data group.
Remaining lifetime	Remaining lifetime for the (S, G) entry that uses the data group in the VPN instance.
active	Indicates that the (S, G) entry is active.

2.1.6. display multicast-vpn vxlan data-group send

Use **display multicast-vpn vxlan data-group send** to display sent data group information in an MVXLAN.

Syntax

display multicast-vpn vxlan { **vpn-instance** *instance-name* | **public-instance** } **data-group send** [**group** *group-address* | *vpn-source-address* [**mask** { *mask-length* | *mask* }] | *vpn-group-address* [**mask** { *mask-length* | *mask* }]] *

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vpn-instance *instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters.

public-instance: Specifies the public instance.

group *group-address*: Specifies a data group by its IP address in the range of 224.0.1.0 to 239.255.255.255.

vpn-source-address: Specifies a multicast source address of the specified VPN instance. The value range for this argument is 224.0.1.0 to 239.255.255.255.

vpn-group-address: Specifies a multicast group address of the specified VPN instance. The value range for this argument is 224.0.1.0 to 239.255.255.255.

mask-length: Specifies a mask length of the specified multicast source address or multicast group address. The value range for this argument is 0 to 32, and the default is 32.

mask: Specifies a subnet mask of the specified multicast source address or multicast group address. The default is 255.255.255.255.

Usage guidelines

If you do not specify any parameters, this command displays information about all sent data groups in the MVXLAN of the specified VPN instance or the public instance.

Examples

Display information about all sent data groups in the MVXLAN of VPN instance vpna.

```
<Switch> display multicast-vpn vxlan vpn-instance vpna data-group send
VPN instance: vpna
Total 2 data-groups for 6 entries
Total 2 data-groups and 6 entries matched

Data-group: 226.1.1.0   Reference count: 3
  (192.6.1.5, 239.1.1.1)                Switchover time: 00:00:21
  (192.6.1.5, 239.1.1.158)              Switchover time: 00:00:21
  (192.6.1.5, 239.1.2.50)               Switchover time: 00:00:05
Data-group: 226.1.1.1   Reference count: 3
```

```
(192.6.1.2, 225.1.1.1)                Switchover time: 00:00:21
(192.6.1.2, 225.1.2.50)               Switchover time: 00:00:05
(192.6.1.5, 239.1.1.159)              Switchover time: 00:00:21
```

Table 2 Command output

Field	Description
Total 2 data-groups for 6 entries	A total of 2 data groups, associated with 6 (S, G) entries.
Total 2 data-groups and 6 entries matched	A total of 2 matching data groups, associated with 6 (S, G) entries.
Data-group	Data group address.
Reference count	Number of (S, G) entries that use the data group in the VPN instance.
Switchover time	Switchover time of the (S, G) entry that uses the data group in the VPN instance.

2.1.7. display multicast-vpn vxlan default-group

Use **display multicast-vpn vxlan default-group** to display information about default groups.

Syntax

display multicast-vpn vxlan [**vpn-instance** *instance-name* | **public-instance**] **default-group** { **local** | **remote** }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vpn-instance *instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters.

public-instance: Specifies the public instance.

local: Specifies local default groups.

remote: Specifies remote default groups.

Usage guidelines

If you do not specify the **vpn-instance** *instance-name* option or the **public-instance** keyword, this command displays default group information for all VPN instances and the public instance.

Examples

Display information about local default groups in all VPN instances and the public instance.

```
<Switch> display multicast-vpn vxlan default-group local
MVXLAN local default-group information of VPN instance 50:
 Group address    Source address   Interface
 237.1.0.0        1.1.1.1          MTunnel0
```

Display information about remote default groups in all VPN instances and the public instance.

```
<Switch> display multicast-vpn vxlan default-group remote
MVXLAN remote default-group information:
 Group address   Source address  Next hop         VPN instance
 239.1.1.1       1.2.0.1         1.2.0.1          a
 239.1.1.1       1.2.0.2         1.2.0.2          a
 239.1.1.1       1.2.0.3         1.2.0.3          a
 239.1.1.2       1.2.0.1         1.2.0.1          b
 239.1.1.2       1.2.0.2         1.2.0.2          b
 239.1.1.3       1.2.0.1         1.2.0.1          c
```

Table 3 Command output

Field	Description
Group address	IP address of the default group.
Source address	IP address of the MVXLAN source interface. This field displays two hyphens (--) if no source interface IP address is configured for the MVXLAN.
Interface	MVXLAN tunnel outgoing interface.
Next hop	Next hop address.
VPN instance	VPN instance to which the default group belongs.

2.1.8. multicast extranet select-rpf

Use **multicast extranet select-rpf** to configure an IPv4 MVXLAN extranet RPF selection policy.

Use **undo multicast extranet select-rpf** to delete an IPv4 MVXLAN extranet RPF selection policy.

Syntax

multicast extranet select-rpf [**l3-vni** *vxlan-id* | **vpn-instance** *vpn-instance-name*] { **group** *group-address* { *mask* | *mask-length* } | **source** *source-address* { *mask* | *mask-length* } } *

undo multicast extranet select-rpf [**l3-vni** *vxlan-id* | **vpn-instance** *vpn-instance-name*] { **group** *group-address* { *mask* | *mask-length* } | **source** *source-address* { *mask* | *mask-length* } } *

Default

No IPv4 MVXLAN extranet RPF selection policies are configured.

Views

MRIB view

Predefined user roles

network-admin

Parameters

l3-vni *vxlan-id*: Specifies the L3 VXLAN ID of the VPN instance to which the multicast source belongs. The value range for the *vxlan-id* argument is 0 to 16777215. If the multicast source belongs to the public network, do not specify this option.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the multicast source belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. The PIM routing entry will select this VPN instance for the upstream RPF neighbor. If the multicast source belongs to the public network, do not specify this option.

group *group-address*: Specifies a multicast group address in the policy. The address range is 224.0.1.0 to 239.255.255.255. If you do not this option, all multicast traffic that matches the source address in the policy in the source VPN instance will be directed to the receiver VPN instance.

source *source-address*: Specifies a source address in the policy, which can a multicast source address or the address of the RP designated to multicast groups. If you do not specify this option, all multicast traffic that matches the multicast group in the policy in the source VPN instance will be directed to the receiver VPN instance.

mask-length: Specifies a mask length for the multicast source address or the multicast group address. For a multicast group address, the value range for this argument is 4 to 32. For a multicast source address, the value range for this argument is 0 to 32.

mask: Specifies a subnet mask for the multicast source address or the multicast group address.

Usage guidelines

MVXLAN extranet RPF routing policies are used for multicast transmission when multicast sources and receivers are located in different VPNs.

MVXLAN extranet RPF selection policies identify the multicast traffic to forward between VPN instances based on the L3 VXLAN ID or VPN instance of traffic.

You cannot specify both an L3 VXLAN ID and an MPLS L3VPN instance for a multicast source address and multicast group address pair.

If the multicast source resides on the public network, do not specify an L3 VXLAN ID or MPLS L3VPN instance.

The PIM mode in the source VPN instance and the receiver VPN instance must be the same. Only PIM-SM and PIM-SSM are supported.

If an MVXLAN extranet RPF selection policy with only the multicast group address specified is configured in the receiver VPN instance, the intra-VPN multicast traffic transmission will be interrupted.

Multicast source addresses in different MVXLAN extranet RPF routing policies cannot be the same, but they can overlap. The same restriction applies to the multicast group addresses in different MVXLAN extranet RPF routing policies. If multiple routing policies exist for an (S, G) entry, the device selects the policy in which the multicast group address has the longest mask. If multiple policies have the same mask length, the device selects the policy in which the multicast source address has the longest mask.

Examples

Configure an IPv4 MVXLAN extranet RPF selection policy to direct multicast traffic from VPN instance vpn-source to VPN instance vpn-receiver.

```
<Switch> system-view
[Switch] multicast routing vpn-instance vpn-receiver
[Switch-mrib-vpn-receiver] multicast extranet select-rpf vpn-instance vpn-source
source 192.168.10.0 24
[Switch-mrib-vpn-receiver] multicast extranet select-rpf vpn-instance  vpn-source
source 1.1.1.1 24
```

2.1.9. multicast-vpn vxlan edge remote

Use **multicast-vpn vxlan edge remote** to specify a peer ED for ED redundancy in the same data center for Layer 3 multicast in DCI multihoming scenarios.

Use **undo multicast-vpn vxlan edge remote** to remove the peer ED configuration for ED redundancy.

Syntax

multicast-vpn vxlan edge remote *remote-ipv4-address*

undo multicast-vpn vxlan edge remote [*remote-ipv4-address*]

Default

No peer ED is specified for ED redundancy in the same data center for Layer 3 multicast in DCI multihoming scenarios.

Views

System view

Predefined user roles

network-admin

Parameters

remote-ipv4-address: Specifies the IPv4 address of a peer ED.

Usage guidelines

To avoid single point of failure for Layer 3 multicast in DCI scenarios, you can deploy multiple EDs at the edge of a data center. On each ED, specify the IP addresses of the other EDs in the same data center in order to recognize the S-PMSI A-D routes from these EDs. This configuration avoids the local ED from joining the multicast tunnels of the other EDs in the same data center.

Repeat this command to specify the IP addresses of multiple EDs in the same data center.

If you do not specify the *remote-ipv4-address* argument when executing the **undo multicast-vpn vxlan edge remote** command, the command removes the IP addresses of all peer EDs from the local ED.

Examples

Specify the peer EDs at 3.3.3.3 and 4.4.4.4 for ED redundancy in the same data center for Layer 3 multicast in DCI multihoming scenarios.

```
<Sysname> system-view
[Sysname] multicast-vpn vxlan edge remote 3.3.3.3
[Sysname] multicast-vpn vxlan edge remote 4.4.4.4
```

2.1.10. multicast-vpn vxlan public-instance

Use **multicast-vpn vxlan public-instance** to create an MVXLAN for the public instance and enter its view, or enter the view of the existing public instance MVXLAN.

Use **undo multicast-vpn vxlan public-instance** to delete the public instance MVXLAN and all settings in public instance MVXLAN view.

Syntax

multicast-vpn vxlan public-instance mode mdt { **ingress-replication** | **mdt** }

undo multicast-vpn vxlan public-instance

Default

No MVXLAN exists in the public instance.

Views

System view

Predefined user roles

network-admin

Parameters

mode: Specifies the MVXLAN mode.

ingress-replication: Sets the mode to ingress replication.

mdt: Sets the mode to MDT.

Examples

Create an MDT-based MVXLAN for the public instance and enter public instance MVXLAN view.

```
<Switch> system-view
[Switch] multicast-vpn vxlan public-instance mode mdt
[Switch—mvxlan-public-instance]
```

2.1.11. multicast-vpn vxlan vpn-instance

Use **multicast-vpn vxlan vpn-instance** to create an MVXLAN for a VPN instance and enter its view, or enter the view of an existing VPN instance MVXLAN.

Use **undo multicast-vpn vxlan vpn-instance** to delete a VPN instance MVXLAN and all settings in its view.

Syntax

multicast-vpn vxlan vpn-instance *instance-name* **mode** { **ingress-replication** | **mdt** }

undo multicast-vpn vxlan vpn-instance *instance-name*

Default

No MVXLAN exists in a VPN instance.

Views

System view

Predefined user roles

network-admin

Parameters

instance-name: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters.

mode: Specifies the MVXLAN mode.

ingress-replication: Sets the mode to ingress replication.

mdt: Sets the mode to MDT.

Examples

Create an MDT-based MVXLAN for VPN instance vpna and enter VPN instance MVXLAN view.

```
<Switch> system-view
[Switch] multicast-vpn vxlan vpn-instance vpna mode mdt
[Switch—mvxlan-vpna]
```

2.1.12. pim distributed-dr

Use **pim distributed-dr** to configure a VSI interface as a distributed DR interface.

Use **undo pim distributed-dr** to restore the default.

Syntax

pim distributed-dr

undo pim distributed-dr

Default

A VSI instance is not a distributed DR interface.

Views

VSI interface view

Predefined user roles

network-admin

Usage guidelines

On the VTEPs configured with MVXLAN, you must specify the VSI interfaces that act as distributed EVPN gateways as distributed DR interfaces. This operation ensures that a distributed EVPN gateway can forward multicast traffic to the local site.

Examples

Configure VSI-interface 1 as a distributed DR interface.

```
<Switch> system-view
[Switch] interface vsi-interface 1
[Switch-Vsi-interface1] pim distributed-dr
```

2.1.13. s-pmsi advertise source-active

Use **s-pmsi advertise source-active** to enable advertising active multicast sources through S-PMSI routes.

Use **undo s-pmsi advertise source-active** to restore the default.

Syntax

s-pmsi advertise source-active

undo s-pmsi advertise source-active

Default

The device does not advertise active multicast sources through S-PMSI routes.

Views

MVXLAN IPv4 address family view

Predefined user roles

network-admin

Usage guidelines

This command enables the VTEP to advertise an S-PMSI route for a (S, G) entry after it receives multicast traffic for the entry. The S-PMSI routes carry information about active multicast sources and allow other VTEPs and EDs in the MVXLAN network to be aware of multicast source location changes.

Examples

Enable the device to advertise active multicast sources through S-PMSI routes in MVXLAN IPv4 address family view of VPN instance vpna.

```
<Switch> system-view
[Switch] multicast-vpn vxlan vpn-instance vpna mode mdt
[Switch-mvxlan-vpn-instance-vpna] address-family ipv4
[Switch-mvxlan-vpn-instance-vpna-ipv4] s-pmsi advertise source-active
```

2.1.14. source

Use **source** to specify an MVXLAN source interface.

Use **undo source** to restore the default.

Syntax

source *interface-type interface-number*

undo source

Default

No MVXLAN source interface is specified.

Views

MVXLAN IPv4 address family view

Predefined user roles

network-admin

Parameters

interface-type interface-number: Specify an interface by its type and number.

Usage guidelines

For the VTEP to obtain correct routing information, you must specify the interface used for establishing BGP peer relationship as the MVXLAN source interface.

Examples

In MVXLAN IPv4 address family view of VPN instance vpna, specify Loopback 0 as the MVXLAN source interface. (Loopback 0 is the source interface used for establishing BGP peer relationship.)

```
<Switch> system-view
[Switch] multicast-vpn vxlan vpn-instance vpna mode mdt
[Switch-mvxlan-vpna] address-family ipv4
[Switch-mvxlan-vpna-ipv4] source loopback 0
```