NEC

GVT-159430-001-00　1.8

QX-S5100G シリーズ

Ethernet スイッチ コマンドマニュアル

改版履歴

版数	日付	改版内容
1.0	2021/04	初版発行
1.1	2021/07	・01-はじめにの 9 章 装置管理に、locator blink コマンドを追加しました。 ・09-セキュリティの 14 章　ARP アタックプロテクションに arp scan コマンドを追加しました。
1.2	2022/03	・09-セキュリティの 2 章 802.1X に display dot1x unicast-trigger quiet-mac コマンドを追加しました。 ・09-セキュリティの 2 章 802.1X の dot1x time コマンドに unicast-trigger quiet-period オプションを追加しました。 ・09-セキュリティの 3 章 MAC 認証の mac-authentication timer コマンドに temporary-user-aging オプションを追加しました。 ・09-セキュリティの 5 章ポートセキュリティの port-security port-mode コマンドに mac-and-userlogin-secure-ext オプションを追加しました。 ・09-セキュリティの 5 章ポートセキュリティに port-security triple-auth-order mac-dot 1 x-web コマンドを追加しました。
1.3	2022/05	・09-セキュリティの 2 章 802.1X の dot1x timer コマンドの **reauth-period** *reauth-period-value* 設定最大値が変更になりました。 ・09-セキュリティの 3 章 MAC 認証の mac-authentication timer コマンドの **reauth-period** *reauth-period-value* 設定最大値が変更になりました。
1.4	2022/06	・11-システム管理の 13 章 NetMiester に、netmeister management ip コマンドを追加しました。

版数	日付	改版内容
1.5	2023/02	・01-はじめにの 9 章 装置管理の以下のコマンドを削除しました。 ・display transceiver diagnosis ・03-アクセスの 1 章 Ethernet インタフェースに下記コマンドを追加しました。 ・ifmonitor crc-error ・ifmonitor input-error ・ifmonitor output-error ・03-アクセスの 15 章 LLDP に cdp voice-vlan コマンドを追加しました。 ・04-IP サービスの 1 章 ARP の arp max-learning-number コマンドの説明に追記しました。 ・04-IP サービスの 7 章 DHCP サーバの設定に下記コマンドを追加しました。 ・class option group ・dhcp class ・dhcp option group ・if-match ・08-ACL と QoS の 2 章 QoS ポリシーの以下のコマンドを削除しました。 ・remark ip precedence ・09-セキュリティの 11 章 SSL に security-enhanced level コマンドを追加しました。 ・11-システム管理の 4 章 PoE について、誤記訂正しました。 ・11-システム管理の 11 章 sFlow の sflow counter interval コマンドに注意を追加しました。 ・11-システム管理の 13 章 NetMeister について、親機モードをサポートしました。

版数	日付	改版内容
1.6	2025/05	・表紙ロゴ色、配置の変更 ・「03-アクセス」の「8 章 STP」の bpdu-drop any コマンドの説明に、ドロップするパケットを追記しました。 ・「04 IP サービス」の「2 章 Gratuitous ARP」に gratuitous-arp mac-change retransmit を追加しました。 ・「04-IP サービス」の「 8 章 DHCP リレーエージェント」に dhcp relay source-address を追加しました。 ・「08 ACL and QoS」の「1 章 ACL」の rule (IPv6 advanced ACL view)コマンドの destination オプションについて説明を追加しました。 ・「09 セキュリティ」の「3 章 MAC アドレス認証」の mac-authentication timer (system view)コマンドの Quiet timer について説明を追記しました。 ・「09-セキュリティ」の「15 章 uRPF」の display ip urpf コマンドについて、以下の誤記を修正しました。 ・loose を指定したサンプルを削除 ・インタフェースを指定したサンプルを削除 ・「09-セキュリティ」の「15 章 uRPF」の ip urpf コマンドについて、以下の誤記を修正 ・loose パラメータの削除 ・strict パラメータのオプションを削除 ・「パラメータ」の「strict uRPF チェックを有効にできるのは、VLAN interface view だけです。」という記載を削除 ・「11-システム管理」の「4 章 PoE」に以下を追加しました。 ・poe high-inrush を追加しました。 ・poe track を追加しました。 ・「11-システム管理」の「13 章 Netmeister」に以下を追加しました。 ・netmeister alarm enable notice ・netmeister update
1.7	2025/07	・06-マルチキャスト の 1 章 IGMP スヌーピング のdisplay igmp-snooping コマンドにメモを追加しました。 ・06-マルチキャスト の 1 章 IGMP スヌーピング の igmp-snooping コマンドと igmp-snooping enable コマンドの説明を追記しました。
1.8	2026/11	・QX-S5100Gシリーズ Ethernet スイッチマニュアル訂正資料9.0版を反映しました。

Copyright © NEC Corporation 2021-2026

All Rights Reserved

事前に NEC の書面による許可なく、本マニュアルをいかなる形式または方法で複製または配布することを禁止します。

商標

本マニュアルに記載されているその他の商標は、各社が保有します。

注意

- 本装置は QX-S5100G シリーズ Ethernet スイッチ コマンドマニュアルに記載されているコマンドのみ使用することができます。QX-S5100G シリーズ Ethernet スイッチ コマンドマニュアルに記載されていないコマンドを使用した場合の動作については保証しません。
- 本マニュアルの内容は、予告なく変更されることがあります。本マニュアルのすべての記述、情報、および推奨事項は、明示的か暗黙的かにかかわらず、いかなる種類の保証の対象になりません。

本マニュアルについて

バージョン

本マニュアルに対応する製品バージョンは Version 7.1.X を含む以降のソフトウェアです。

関連マニュアル

次のマニュアルには、QX-S5100G シリーズ Ethernet スイッチに関する詳細な説明が記載されています。

マニュアル	内容
QX-S5100G シリーズ Ethernet スイッチ インスタレーションマニュアル	システムのインストールについて説明しています。
QX-S5100G シリーズ Ethernet スイッチ オペレーションマニュアル	機能の設定について説明しています。
QX-S5100G シリーズ Ethernet スイッチ コマンドマニュアル	機能に関するコマンドについて説明しています。
QX-S5100G シリーズ Ethernet スイッチ Web コンソール操作マニュアル	Web コンソールからの装置設定、状態確認等についての操作を記述しています。

マニュアルの構成

このコマンドマニュアルは以下のセクションで構成されます。

- **はじめに**

  Ethernet スイッチへのアクセス方法、ファイルシステム管理、設定ファイル管理、ソフトウェア管理、装置管理といった、Ethernet スイッチの管理の設定について説明します。

- **IRF スタック**

  IRF スタックの設定について説明します。

- **アクセス**

  Ethernet ポート、リンクアグリゲーション、VLAN、STP といった、レイヤ 2 機能の設定について説明します。

- **IP サービス**

  ARP、IP アドレス（IPv4＆IPv6）、DHCP 関連機能、IP パフォーマンスといった、ネットワークプロトコルの設定について説明します。

- **ルーティングプロトコル**

各種ルーティングプロトコル（IPv4＆IPv6）の設定について説明します。

- **マルチキャスト**

  各種マルチキャストプロトコル（IPv4＆IPv6）の設定について説明します。

- **MCE**

  MCE の設定について説明します。

- **ACL and QoS**

  QoS、ACL の設定について説明します。

- **セキュリティ**

  AAA、RADIUS、802.1X、MAC アドレス認証、SSH 等の設定について説明します。

- **高可用性**

  Ethernet OAM、CFD、DLDP、RRPP、BFD 等の設定について説明します。

- **システム管理**

  システム保守、ネットワーク管理の設定といった、Ethernet スイッチのシステム管理および保守について説明します。

表記規則

本マニュアルでは、次の表記規則を使用しています。

I. コマンド表記規則

表記規則	説明
太字体	コマンドラインを示すキーワードには**太字体**を使用します。
イタリック体	コマンドの引数は*イタリック体*を使用します。
[ ]	大カッコに囲まれた項目(キーワード、引数)はオプションです。
{ x | y | … }	選択する項目は、中カッコに入れて縦線で区切ってあります。1 つを選択します。
[x | y | …]	オプションの選択項目は、大カッコに入れて縦線で区切ってあります。1 つまたは複数を選択します。
{ x | y | … }*	選択する項目は、中カッコに入れて縦線で区切ってあります。少なくとも 1 つ選択できます。
[x | y | …]*	オプションの選択項目は、大カッコに入れて、縦線で区切ってあります。1 つあるいは複数選択することも、何も選択しないこともできます。
&<1-n>	&の前のキーワードと引数を組み合わせます。引数で指定した数までキーワードを繰り返し指定できます。
#	#で始まる行はコメントを示します。

II. GUI 表記規則

表記規則	説明
< >	ボタン名は三角カッコに入っています。例えば、<OK>ボタンをクリックします。
[ ]	ウィンドウ名、メニュー項目、データ表、およびフィールド名は大カッコに入っています。例えば、[New User]ウィンドウが表示されます。
/	複数レベルのメニューはスラッシュで区切ってあります。例えば、[File/Create/Folder]。

III. キーボード操作

表記規則	説明
<KEY>	KEY のキーを押します。例えば、 <Enter>は Enter キーを押します。
<KEY1 + KEY2>	複数のキーを同時に押します。例えば、 <Ctrl+Alt+A>は 3 つのキーを同時に押すことを表します。
<KEY1, KEY2>	複数のキーを順番に押します。例えば、 <Alt, A>は 2 つのキーを順に押すことを表します。

IV. マウス操作

表記規則	説明
クリック	マウスのボタンを素早く押します。特に指定がない場合は左ボタンを押します。
ダブルクリック	マウスの左ボタンを素早く 2 回押します。
ドラッグ	マウスの左ボタンを押したまま移動します。

V. 記号

表記規則	説明
⚠**警告**	表示を無視したり指示に従わない場合、利用者が怪我などをする恐れのある重要な情報を示します。
⚠**注意**	表示を無視したり指示に従わない場合、データの損失や破損、ハードウェアやソフトウェアの損傷などが発生する恐れのある重要な情報を示します。
⚠**重要**	注意を払う必要がある情報を示します。
🕮**メモ**	追加または補足となる情報を示します。
🕮**ポイント**	参考となる情報を示します。

VI. ネットワークアイコン

表記規則	説明
	ルータ、スイッチ、またはファイアウォールなどの一般的なネットワークデバイスを表しています。
	ルータまたはレイヤ 3 スイッチなどのルーティング対応のデバイスを表しています。
	レイヤ 2、レイヤ 3 スイッチまたはレイヤ 2 転送機能に対応したルータなどの一般的なスイッチデバイスを表しています。

VII. 設定例

本マニュアルの設定例は各機能での代表的な設定例を示します。インタフェース番号、システム名の表記、display コマンドで表示される情報は、ご使用の装置と異なることがあります。

VIII. セキュリティ強化

セキュリティ強化のため、simple で設定されたパスワードも cipher や hash で登録されます。

本マニュアルは以下に示す 11 個のセクションで構成されています。

01 - はじめに

02 - IRF スタック

03 - アクセス

04 - IP サービス

05 - ルーティングプロトコル

06 - マルチキャスト

07 - MCE

08 - ACL and QoS

09 - セキュリティ

10 - 高可用性

11 - システム管理

QX-S5100G シリーズ Ethernet スイッチ

コマンドマニュアル

1. はじめに

本マニュアルは以下に示す章で構成されています。

01-CLI

02-RBAC

03-ログイン

04-FTP

05-TFTP

06-ファイルシステム管理

07-コンフィグレーションファイル管理

08-ソフトウェア管理

09-装置管理

10-Python

目次

このセクションのページは **1-x-x** です。

1 章 CLI 1-1
1.1 CLI 設定コマンド 1-1
1.1.1 alias 1-1
1.1.2 display | { begin | exclude | include } 1-3
1.1.3 display | by-linenum 1-4
1.1.4 display > 1-5
1.1.5 display >> 1-6
1.1.6 display alias 1-7
1.1.7 display history-command 1-8
1.1.8 display history-command all 1-9
1.1.9 display hotkey 1-11
1.1.10 hotkey 1-12
1.1.11 quit 1-13
1.1.12 return 1-14
1.1.13 screen-length disable 1-14
1.1.14 system-view 1-15

1章 CLI

1.1 CLI設定コマンド

1.1.1 alias

Syntax

alias *alias command*

undo alias *alias*

デフォルト

表 1-1 にシステム定義のエイリアスを示します。

表 1-1 システム定義のコマンドエイリアス

エイリアス	コマンド
access-list	acl
end	return
erase	delete
exit	quit
hostname	sysname
logging	info-center
no	undo
show	display
write	save

View

System view

定義済みユーザロール

network-admin

パラメータ

alias: エイリアスを指定します。設定範囲は 1～20 文字です。大文字、小文字を区別します。エイリアスは alias あるいはスペースを使用することができません。

command: コマンドの文字列を指定します。コマンドの文字列は Syntax の要件に一致している必要があります。

説明

alias コマンドはコマンドのエイリアスを設定します。

undo alias コマンドはコマンドのエイリアスを削除します。

システムで定義したエイリアスは削除することができません。

コマンドあるいはコマンドのパラメータで開始するエイリアスを設定することができます。コマンドを実行するため、エイリアスを使用することができます。**undo** で始まるコマンドがある場合についても、エイリアスを使用することができます。

コマンドのエイリアスを設定した後、コマンドのエイリアスを入力することができます。たとえば、**display ip routing-table** コマンドを行うため、**alias shiprt** コマンド設定します。**display ip** コマンドの **alias ship** コマンドを設定する場合、**display ip** で始まるすべてのコマンドを実行するため、**ship** を使用することができます。

- **display ip routing-table** コマンドを実行するため **ship routing-table** コマンドを入力します。
- **display ip interface** コマンドを実行するため **ship interface** コマンドを入力します。

エイリアスによって説明できる文字列は 9 つのパラメータまで設定することができます。各パラメータはドル記号（$）と 1～9 までのシーケンス番号で開始します。

たとえば、**display ip $1 | include $2** を行うために **alias shinc** コマンドを設定することができます。**display ip routing-table | include Static** を行う場合、**shinc routing-table Static** を入力することで実行することができます。**display ip interface | include GigabitEthernet1/0/1** コマンドを実行する場合、**shinc interface GigabitEthernet1/0/1** を入力することで実行することができます。

例

display ip routing-table コマンドを行うために **alias shiprt** コマンドを設定します。

<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
```

display $1 | include $2 コマンドを行うために **alias shinc** コマンドを設定します。

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

すべてのスタティックルート情報を表示するため **alias shinc** コマンドを使用します。

[Switch] shinc routing-table Static

```
3.3.3.3/32         Static  60  0          192.168.1.62    Vlan1
```

関連コマンド

display alias

1.1.2 display | { begin | exclude | include }

Syntax

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

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

command: **display** コマンドのキーワードと引数を指定します。有効なキーワードと引数を表示する場合、**display ?**と入力します。

begin: 指定した正規表現の文字列を含む行を含む以降の行を表示します。

exclude: 指定した正規表現の文字列を含まない行を表示します。

include: 指定した正規表現の文字列を含む行を表示します。

regular-expression: 1～256 字の大文字と小文字を区別した正規表現を指定します。

説明

display | { **begin** | **exclude** | **include** }コマンドは正規表現を使用して **display** コマンドから出力をフィルタします。

正規表現の詳細は、オペレーションマニュアルのセクション 1 *はじめに*”*CLI*”を参照してください。

例

カレントコンフィグレーションで vlan を含む行を表示します。

<Switch> display current-configuration | include vlan

```
vlan 1
vlan 999
 port access vlan 999
```

1.1.3 display | by-linenum

Syntax

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

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

command: **display** コマンドのキーワードと引数を指定します。有効なキーワードと引数を表示する場合、**display ?**と入力します。

説明

display | by-linenum コマンドは **display** コマンドに行番号をつけて表示します。

行番号を使用することで、わかりやすく表示することができます。

行番号は 5 桁で表示され、コロン（:）あるいはハイフン（-）が続きます。**display | by-linenum** コマンドと **display | begin regular-expression** コマンドを同時に使用した場合、正規表現に一致しないすべての行はハイフン（-）で表示されます。

例

VLAN999 の設定を表示するため、行番号をつけて出力を表示します。

<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
```

カレントコンフィグレーションで user-group で始まる行から以降の行を表示します。

<Switch> display current-configuration | by-linenum begin user-group

```
114: user-group system
115- #
116- return
```

1.1.4 display >

Syntax

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

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

command: **display** コマンドのキーワードと引数を指定します。有効なキーワードと引数を表示する場合、**display ?**と入力します。

filename: 出力を保存するファイル名を 1～63 文字で指定します。

説明

display >コマンドは、**display** コマンドの出力を別のファイルに保存します。

display コマンドは、設定、統計情報、装置の状態を表示します。**display >**コマンドはファイルに **display** コマンドの出力を保存します。

指定したファイルが存在しない場合、ファイルを新規に作成し、ファイルに **display** コマンドの出力を保存します。指定したファイルが存在する場合、ファイルに上書きします。

例

vlan.txt というファイルに VLAN 1 の設定を保存します。

<Switch> display vlan 1 > vlan.txt

vlan.txt ファイルの内容を確認します。

<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 >>

Syntax

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

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

command: **display** コマンドのキーワードと引数を指定します。有効なキーワードと引数を表示する場合、**display ?**と入力します。

filename: 出力を保存するファイル名を 1～63 文字で指定します。

説明

display >>コマンドは、**display** コマンドの出力をファイルの最後に追記します。

display コマンドは、設定、統計情報、装置の状態を表示します。**display >>**コマンドはファイルに **display** コマンドの出力を保存します。

指定したファイルが存在しない場合、ファイルを新規に作成し、ファイルに **display** コマンドの出力を保存します。指定したファイルが存在する場合、ファイルの最後に追記します。

例

vlan.txt というファイルの最後に VLAN 999 を追記します。

<Switch> display vlan 999 >> vlan.txt

```
<Switch>
```

vlan.txt ファイルの内容を確認します。

<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

Syntax

display alias [*alias*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

alias: コマンドエイリアスを指定します。指定しない場合、すべてのコマンドのエイリアスを表示します。

説明

display alias コマンドはコマンドエイリアスを表示します。

例

すべてのコマンドのエイリアスを表示します。

<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
```

コマンドエイリアス shinc を表示します。

<Switch> display alias shinc

```
Alias             Command key
shinc             display ip $1 | include $2
```

関連コマンド

alias

1.1.7 display history-command

Syntax

display history-command

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display history-command コマンドは、履歴バッファに保存されているすべてのコマンドを表示します。このコマンドは現在の CLI セッションで実行された有効なコマンドです。

システムは現在の CLI セッションで実行された有効なコマンドを自動的に保存します。

履歴バッファに保存されているコマンドを表示し、再度実行することができます。

デフォルトで、最大 10 個まで履歴コマンドを保存できます。履歴バッファのサイズを設定するには、**history-command max-size** コマンドを使用します。

バッファサイズが最大のときに新しいコマンドをバッファする場合、システムはバッファのもっとも古いコマンドを削除します。

現在の CLI セッションの履歴コマンドのすべてのコマンドはログアウトしたときに削除されます。

例

現在の CLI セッションで履歴バッファにあるすべてのコマンドを表示します。

<Switch> display history-command

```
system-view
vlan 2
quit
```

関連コマンド

history-command max-size

1.1.8 display history-command all

Syntax

display history-command all

View

すべての view

定義済みユーザロール

network-admin

説明

display history-command all コマンドは、履歴バッファに保存されているすべてのコマンドを表示します。このコマンドはすべての CLI セッションで実行された有効なコマンドです。

システムはすべての CLI セッションで実行された有効なコマンドを自動的に保存します。

履歴バッファに保存されているコマンドを表示し、再度実行することができます。

デフォルトで、最大 1024 個まで履歴コマンドを保存できます。履歴バッファのサイズが最大になったとき、最初に保存されたコマンドを削除し、新しく実行されたコマンドを保存します。

ユーザがログアウトした場合、すべての CLI セッションの履歴バッファからコマンドを削除します。

例

すべての CLI セッションで履歴バッファにあるすべてのコマンドを表示します。

<Switch> display history-command all

```
Date      Time     Terminal   Ip            User
03/16/2012 20:03:33 vty0      192.168.1.26    **
Cmd:dis his all

03/16/2012 20:03:29 vty0      192.168.1.26    **
Cmd:sys
```

表 1-2 コマンド出力

フィールド	説明
Date	コマンドを実行した日付です。
Time	コマンドを実行した時間です。
Terminal	ユーザが使用しているlineです。
Ip	ユーザが使用している端末のIPアドレスです。
User	ユーザがログインする際、認証モードがschemeを使用する場合のユーザ名です。認証モードがnoneあるいはpasswordの場合、“**”と表示します。
Cmd	ユーザによって入力したコマンドです。

関連コマンド

display history-command

1.1.9 display hotkey

Syntax

display hotkey

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display hotkey コマンドは、ホットキー情報を表示します。

例

ホットキー情報を表示します。

<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
```

関連コマンド

hotkey

1.1.10 hotkey

Syntax

hotkey { **ctrl_g** | **ctrl_l** | **ctrl_o** | **ctrl_t** | **ctrl_u** } *command*

undo hotkey { **ctrl_g** | **ctrl_l** | **ctrl_o** | **ctrl_t** | **ctrl_u** }

デフォルト

ctrl_g: **display current-configuration**（カレントコンフィグレーションを表示します。）

ctrl_l: **display ip routing-table**（IPv4 ルーティングテーブル情報を表示します。）

ctrl_o: **undo debugging all**（すべてのデバッグ機能を無効にします。）

ctrl_t: ホットキーにコマンドが割り当てられていません。

ctrl_u: ホットキーにコマンドが割り当てられていません。

View

System view

定義済みユーザロール

network-admin

パラメータ

ctrl_g: ホットキー**Ctrl+G** にコマンドを割り当てます。

ctrl_l: ホットキー**Ctrl+L** にコマンドを割り当てます。

ctrl_o: ホットキー**Ctrl+O** にコマンドを割り当てます。

ctrl_t: ホットキー**Ctrl+T** にコマンドを割り当てます。

ctrl_u: ホットキー**Ctrl+U** にコマンドを割り当てます。

command: ホットキーに割り当てるコマンドを指定します。

説明

hotkey コマンドは設定可能なホットキーにコマンドを割り当てます。

undo hotkey コマンドはデフォルトに戻します。

システムはいくつかのホットキーを定義し、5 つの設定可能なコマンドホットキーを提供します。ホットキーを押下することでホットキーに割り当てられたコマンドを実行します。

システムで定義されたホットキーと設定可能なホットキーを表示するには **display hotkey** コマンドを使用します。

例

ホットキーCTRL+T に **display tcp status** コマンドを割り当てます。

<Switch> system-view

[Switch] hotkey ctrl_t display tcp statistics

関連コマンド

display hotkey

1.1.11 quit

Syntax

quit

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

quit コマンドは上位の view に戻ります。

user view で **quit** コマンドを実行すると装置から切断されログアウトします。

例

GigabitEthernet 1/0/1 の view から system view に戻り、次に user view に戻ります。

[Switch-GigabitEthernet1/0/1] quit

[Switch] quit

<Switch>

1.1.12 return

Syntax

return

View

user view を除いたすべての view

定義済みユーザロール

network-admin

network-operator

説明

return コマンドは、ほかの view から user view に戻ります。

Ctrl+Z ホットキーは **return** コマンドと同一です。

例

GigabitEthernet 1/0/1 の view から user view に戻ります。

[Switch-GigabitEthernet1/0/1] return

<Switch>

1.1.13 screen-length disable

Syntax

screen-length disable

undo screen-length disable

デフォルト

user line view の **screen-length** コマンドの設定によってデフォルトは変わります。

screen-length コマンドのデフォルトは以下です。

- 出力画面ごとにスクロールを停止します。
- 画面上で一度に 24 行まで表示します。

View

User view

定義済みユーザロール

network-admin

説明

screen-length disable コマンドは現在のセッションで出力画面のスクロールの停止を無効にします。

undo screen-length disable コマンドは現在のセッションで出力画面のスクロールの停止を有効にします。出力画面のスクロールの停止を無効にした場合、すべての出力が表示されます。最後の画面が表示されるまで連続して画面がリフレッシュします。

このコマンドは現在の画面のみ適用されます。ログアウトすると設定はデフォルトに戻ります。

例

現在のセッションで出力画面のスクロールの停止を無効にします。

<Switch> screen-length disable

関連コマンド

screen-length

1.1.14 system-view

Syntax

system-view

View

User view

定義済みユーザロール

network-admin

network-operator

説明

system-view コマンドは user view から system view に移行します。

例

user view から system view に移行します。

<Switch> system-view

```
System View: return to User View with Ctrl+Z.
```

[Switch]

目次

このセクションのページは **1-x-x** です。

2 章 RBAC 2-1
2.1 RBAC 設定コマンド 2-1
2.1.1 description 2-1
2.1.2 display role 2-2
2.1.3 display role feature 2-10
2.1.4 display role feature-group 2-13
2.1.5 feature 2-15
2.1.6 interface policy deny 2-16
2.1.7 permit interface 2-18
2.1.8 permit vlan 2-20
2.1.9 role 2-22
2.1.10 role default-role enable 2-23
2.1.11 role feature-group 2-24
2.1.12 rule 2-25
2.1.13 super 2-29
2.1.14 super authentication-mode 2-30
2.1.15 super default role 2-32
2.1.16 super password 2-33
2.1.17 vlan policy deny 2-34

2章 RBAC

2.1 RBAC設定コマンド

2.1.1 description

Syntax

description *text*

undo description

デフォルト

設定なし

View

User role view

定義済みユーザロール

network-admin

パラメータ

text: ユーザロールの説明を設定します。設定範囲は 1～128 です。大文字、小文字を区別します。

説明

description コマンドはユーザロールの説明を設定します。ユーザロールの識別、管理しやすさを向上させることができます。

undo description コマンドはユーザロールの説明を削除します。

例

ユーザロール role1 の説明を labVIP に設定します。

<Switch> system-view

[Switch] role name role1

[Switch-role-role1] description labVIP

関連コマンド

- **display role**
- **role**

2.1.2 display role

Syntax

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

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

name *role-name*: ユーザロール名を指定します。設定範囲は 1～63 です。大文字、小文字を区別します。ユーザロール名を指定しない場合、定義済みのユーザロールを含むすべてのユーザロールの情報を表示します。

説明

display role コマンドはユーザロールの情報を表示します。

例

ユーザロール 123 の情報を表示します。

<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
```

すべてのユーザロールの情報を表示します。

<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 *
  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
  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
```

表 2-1 コマンド出力

フィールド	説明
Role	ユーザロール名です。 定義済みのユーザロール名は以下です。 ● network-admin ● network-operator ● level-*n* （*n*は0～15の整数です） ● security-audit（未サポートです） ● guest-manager（現在のソフトウェアバージョンではサポートしていません。）
Description	設定内容を容易に識別できるようにするためのユーザロールの説明です。
VLAN policy	ユーザロールのVLANポリシーです。 ● **deny**—許可されたVLANを除くVLANへのアクセスを拒否します。 ● **permit (default)**—デフォルトVLANポリシーです。すべてのVLANにアクセスするユーザロールを有効にします。
Permitted VLANs	ユーザロールにアクセス可能なVLANです。

フィールド	説明
Interface policy	ユーザロールのインタフェースポリシーです。 ● **deny**—許可されたインタフェースを除くインタフェースへのアクセスを拒否します。 ● **permit (default)**—デフォルトインタフェースポリシーです。すべてのインタフェースにアクセスするユーザロールを有効にします。
Permitted interfaces	ユーザロールにアクセス可能なインタフェースです。
VPN instance policy	ユーザロールのVLANインスタンスポリシーです。 このフィールドは現在のソフトウェアバージョンで未サポートです。 ● **deny**–許可されたVPNを除くVPNへのアクセスを拒否します。 ● **permit (default)**–デフォルトVPNインスタンスポリシーです。すべてのVPNインスタンスにアクセスするユーザロールを有効にします。
Permitted VPN instances	ユーザロールにアクセス可能なVPNインスタンスです。 このフィールドは現在のソフトウェアバージョンで未サポートです。
Rule	ユーザロール番号です。 ユーザロールのルールはコマンド、指定されたコマンドを含むアイテムのアクセス許可を指定します。 定義済みのユーザロールのルールはsys-*n*で指定されます。ここで*n*は整数です。
Perm	アクセス制御タイプです。 ● **permit**—ユーザロールは**Entity**フィールドに指定されたアイテムにアクセスできます。 ● **deny**—ユーザロールは**Entity**フィールドに指定されたアイテムにアクセスできせん。
Type	制御タイプです。 ● **R**–Read-onlyです。 ● **W**–Writeです。 ● **X**–Executeです。

フィールド	説明
Scope	ルール制御範囲です。 ● **command–Entity**フィールドに指定されるコマンドへのアクセスを制御します。 ● **feature–Entity**フィールドに指定される機能コマンドへのアクセスを制御します。 ● **feature-group–Entity**フィールドに指定される機能グループの機能コマンドへのアクセスを制御します。 ● **web-menu**—Webメニューへのアクセスを制御します。（未サポートです） ● **xml-element**—XMLエレメントへのアクセスを制御します。（未サポートです） ● **oid**—MIBノードへのアクセスを制御します。（未サポートです）
Entity	ユーザグループルールで指定されたコマンド文字列、機能名、機能グループ、Webメニュー、XMLエレメント、MIBノードです。 ● エンダッシュ（-）はすべての機能を示します。 ● アスタリスク（*）は0以上の文字を示します。

関連コマンド

role

2.1.3 display role feature

Syntax

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

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

name *feature-name*: 機能のコマンドを表示します。*feature-name* は機能名を指定します。すべての文字は小文字にする必要があります。

verbose: 各機能のコマンドを表示します。

説明

display role feature コマンドはシステムで有効な機能を表示します。

name *feature-name* パラメータあるいは **verbose** パラメータのいずれのパラメータを指定しない場合、システムで有効な機能のリストのみを表示します。

例

機能のリストを表示します。

<Switch> display role feature

```
Feature: device         (Device configuration related commands)
Feature: interface      (Interface related commands)
Feature: syslog         (Syslog related commands)
...
```

各機能のコマンドを表示します。

<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)
...
```

aaa 機能のコマンドを表示します。

<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)
  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)
...
```

表 2-2 コマンド出力（**display role feature name aaa**）

フィールド	説明
Feature	機能の名前、概要の説明を表示します。
system-view ; domain *	system viewでの**domain**パラメータで始まるすべてのコマンドです。ISP domain viewでのすべてのコマンドです。
system-view ; header *	system viewでの**header**パラメータで始まるすべてのコマンドです。
system-view ; aaa *	system viewでの**aaa**で始まるすべてのコマンドです。
display domain *	user viewでの**display domain**パラメータで始まるすべてのコマンドです。
system-view ; user-group *	system viewでの**user-group**パラメータで始まるすべてのコマンドとuser group viewのすべてのコマンドです。
system-view ; local-user *	system viewでの**local-user**パラメータで始まるすべてのコマンドとlocal user viewのすべてのコマンドです。
display local-user *	user viewでの**display local-user**パラメータで始まるすべてのコマンドです。
display user-group *	user viewでの**display user-group**パラメータで始まるすべてのコマンドです。
display debugging local-server	user viewでの**display debugging local-server**パラメータで始まるすべてのコマンドです。
debugging local-server *	user viewでの**debugging local-server**パラメータで始まるすべてのコマンドです。
super *	user viewでの**super**パラメータで始まるすべてのコマンドです。
display password-control *	user viewでの**display password-control**パラメータで始まるすべてのコマンドです。
reset password-control *	user viewでの**reset password-control**パラメータで始まるすべてのコマンドです。
system-view ; password-control *	system viewでの**password-control**パラメータで始まるすべてのコマンドです。
(W)	コマンドタイプがwriteです。**write**コマンドはシステムを設定します。

フィールド	説明
(R)	コマンドタイプがreadです。**read**コマンドは設定を表示あるいは情報を維持します。
(X)	コマンドタイプがexecuteです。**execute**コマンドは指定した機能を実行します。

関連コマンド

feature

2.1.4 display role feature-group

Syntax

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

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

name *feature-group-name*: 機能グループを指定します。*feature-group-name* は機能グループ名を指定します。設定範囲は 1～31 です。大文字、小文字を区別します。機能グループを指定しない場合、すべての機能グループの情報を表示します。

verbose: 指定された機能グループの各機能のコマンドを表示します。機能グループを指定しない場合、各機能グループの各機能のコマンドを表示します。**verbose** パラメータを指定しない場合、機能グループの機能リストのみを表示します。

説明

display role feature-group コマンドは機能グループの情報を表示します。

機能グループ L2、L3 は機能グループで定義されています。

例

機能グループの機能リストを表示します。

<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: mvrp           (MVRP related commands )
Feature: rrpp           (RRPP 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: lisp           (LISP protocol related commands)
Feature: route-policy    (Routing Policy related commands)
```

各機能グループのコマンドを表示します。コマンドのワイルドカードと記号についての詳細は、表 2-2 を参照してください。

<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 ; 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)
  reset igmp-snooping *    (W)
  reset pim-snooping *    (W)
  reset multicast-vlan *    (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 ; 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)
  reset mld-snooping *    (W)
  reset ipv6 pim-snooping *    (W)
  reset ipv6 multicast-vlan *    (W)
  debugging mld-snooping *    (W)
  display debugging mld-snooping *    (R)
  system-view ; probe ; debugging system internal mld-snooping *    (W)
…
```

機能グループ L3 の機能リストを表示します。

<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: lisp           (LISP protocol related commands)
Feature: route-policy    (Routing Policy related commands)
```

関連コマンド

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

2.1.5 feature

Syntax

feature *feature-name*

undo feature *feature-name*

デフォルト

設定なし

View

Feature group view

定義済みユーザロール

network-admin

パラメータ

feature-name: 機能名を指定します。大文字、小文字を区別します。機能名として表示される名前を省略しないで、小文字で入力する必要があります。

説明

feature コマンドは機能グループに機能を追加します。

undo feature コマンドは機能グループから機能を削除します。

機能グループに複数の機能を追加する場合、**feature** コマンドを繰り返してください。

例

セキュリティグループ security-features にセキュリティ機能 AAA、ACL を追加します。

<Switch> system-view

[Switch] role feature-group name security-features

[Switch-featuregrp-security-features] feature aaa

[Switch-featuregrp-security-features] feature acl

関連コマンド

- **display role feature**
- **display role feature-group**
- **role feature-group**

2.1.6 interface policy deny

Syntax

interface policy deny

undo interface policy deny

デフォルト

設定なし

View

User role view

定義済みユーザロール

network-admin

説明

interface policy deny コマンドはインタフェースへのアクセスを拒否し、ユーザロールの interface policy view に移行します。

undo interface policy deny コマンドはユーザロールインタフェースポリシーをデフォルトに戻します。

指定したインタフェースのみユーザロールのインタフェースへのアクセスを制限するために、以下の作業を行います。

1) **interface policy deny** コマンドでインタフェースへのアクセスを拒否します。
2) **permit interface** コマンドでアクセス可能なインタフェースを指定します。

🕮 **メモ：**

permit interface コマンドが設定されていない場合、**interface policy deny** コマンドはすべてのインタフェースへのアクセスを拒否します。

インタフェースを設定するため、ユーザロールのインタフェースポリシーで許可されているインタフェースが使用されているであることを確認してください。アクセス可能なインタフェースで以下の操作を実行することができます。

- インタフェースの作成、削除、設定を行います。
- interface view へ移行します。
- **feature** コマンドでインタフェースを指定します。

作成および削除は、論理インタフェースでのみ有効です。

ユーザロールのインタフェースポリシーの変更は、変更後にユーザロールにログインしたユーザのみ適用されます。

例

ユーザロール role1 ですべてのインタフェースへのアクセスを拒否します。

<Switch> system-view

[Switch] role name role1

[Switch-role-role1] interface policy deny

[Switch-role-role1-ifpolicy] quit

ユーザロール role1 の interface policy view に移行し、GigabitEthernet 1/0/1～GigabitEthernet 1/0/4 へのアクセスを許可します。GigabitEthernet 1/0/1～GigabitEthernet 1/0/4 を除くインタフェースへのアクセスを拒否します。

<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

関連コマンド

- **display role**
- **permit interface**
- **role**

2.1.7 permit interface

Syntax

permit interface *interface-list*

undo permit interface [*interface-list*]

デフォルト

設定なし

View

User role interface policy view

定義済みユーザロール

network-admin

パラメータ

interface-list: インタフェースを指定します。半角スペースで区切ることで 10 のインタフェースを指定することができます。各インタフェースは *interface-type interface-number* あるいは *interface-type interface-number* **to** *interface-type interface-number* の形式で指定します。インタフェースの範囲を指定する場合、終了インタフェースは以下の要件に一致する必要があります。

- 開始インタフェースと同一のタイプにしてください。
- 開始インタフェースよりもインタフェース番号を大きい値にしてください。

説明

permit interface コマンドはユーザロールにアクセス可能なインタフェースのリストを設定します。

undo permit interface コマンドは指定したインタフェースのアクセスを無効にします。

interface policy deny コマンドを設定した後、インタフェースにアクセスするユーザロールを許可するため、ポリシーの許可されたインタフェースリストにインタフェースを追加する必要があります。ユーザロールで許可されたインタフェースリストのインタフェースで以下の操作を実行することができます。

- インタフェースの作成、削除、設定を行います。
- interface view へ移行します。
- **feature** コマンドでインタフェースを指定します。

作成および削除は、論理インタフェースでのみ有効です。

ユーザロールのインタフェースポリシーに許可されたインタフェースを追加するため、**permit interface** コマンドを複数繰り返すことができます。

インタフェースを指定しない場合、**undo permit interface** コマンドは許可されたインタフェースのリスト全体を削除します。

ユーザロールのインタフェースポリシーの変更は、変更後にユーザロールにログインしたユーザのみ適用されます。

例

1) ユーザロール role1 を設定します。

interface view、VLAN view で有効なすべてのコマンドを実行するため、ユーザロールを許可します。

<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 *

GigabitEthernet 1/0/1、GigabitEthernet 1/0/3～GigabitEthernet 1/0/5 へアクセスするため、ユーザロールを許可します。

[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) GigabitEthernet 1/0/1、GigabitEthernet 1/0/3～GigabitEthernet 1/0/5 を除いたインタフェースで動作するユーザロールが使用できないことを確認します。

GigabitEthernet 1/0/1 interface view に移行できることを確認します。

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] quit

GigabitEthernet 1/0/5 に VLAN 10 の割り当てができることを確認します。この例では、ユーザロールのデフォルト VLAN ポリシーが使用されているため、ユーザロールはすべての VLAN にアクセスできます。

[Switch] vlan 10

[Switch-vlan10] port gigabitethernet 1/0/5

[Switch-vlan10] quit

GigabitEthernet 1/0/2 の interface view に移行できないことを確認します。

[Switch] interface gigabitethernet 1/0/2

```
Permission denied.
```

関連コマンド

- **display role**
- **interface policy deny**
- **role**

2.1.8 permit vlan

Syntax

permit vlan *vlan-id-list*

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

デフォルト

設定なし

View

User role VLAN policy view

定義済みユーザロール

network-admin

パラメータ

vlan-id-list: VLAN を指定します。半角スペースで区切ることで 10 の VLAN を指定することができます。各 VLAN は VLAN ID で VLAN を指定あるいは *vlan-id1* **to** *vlan-id2* の形式で指定します。VLAN ID の設定範囲は 1～4094 です。VLAN の範囲を指定する場合、*vlan-id2* は *vlan-id1* よりも大きい値にしてください。

説明

permit vlan コマンドはユーザロールにアクセスできる VLAN のリストを設定します。

undo permit vlan コマンドは指定した VLAN にアクセスするため、ユーザロールの許可を削除します。

vlan policy deny コマンドを設定したのち、VLAN にアクセスするユーザロールを許可するために、ポリシーの許可された VLAN リストに VLAN を追加する必要があります。ユーザロールで、許可された VLAN リストの VLAN で以下の操作を実行することができます。

- VLAN の作成、削除、設定を行います。
- VLAN view へ移行します。
- **feature** コマンドで VLAN を指定します。

ユーザロールの VLAN ポリシーに許可された VLAN を追加するため、**permit vlan** コマンドを複数繰り返すことができます。

VLAN を指定しない場合、**undo permit vlan** コマンドは許可された VLAN のリスト全体を削除します。

ユーザロールの VLAN ポリシーの変更は、変更後にユーザロールにログインしたユーザのみ適用されます。

例

1) ユーザロール role1 を設定します。

interface view、VLAN view で有効なすべてのコマンドを実行するため、ユーザロールを許可します。

<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 *

VLAN 2、VLAN 4、VLAN 50～VLAN 100 にアクセスするユーザロールを許可します。

[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) VLAN 2、VLAN 4、VLAN 50～VLAN 100 を除いた VLAN で動作するユーザロールが使用できないことを確認します。

VLAN 100 を作成し、VLAN view に移行できることを確認します。

[Switch] vlan 100

[Switch-vlan100] quit

アクセスポートとして VLAN 100 に GigabitEthernet 1/0/1 を追加できることを確認します。

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] port access vlan 100

[Switch-GigabitEthernet1/0/1] quit

VLAN 101 を作成し、VLAN view に移行できないことを確認します。

[Switch] vlan 101

```
Permission denied.
```

関連コマンド

- **display role**
- **role**
- **vlan policy deny**

2.1.9 role

Syntax

role name *role-name*

undo role name *role-name*

デフォルト

以下の定義済みユーザロールがあります。

- network-admin
- network-operator
- level-*n* （*n* は 0～15 の整数です）

View

System view

定義済みユーザロール

network-admin

パラメータ

name *role-name*: ユーザ名を指定します。設定範囲は 1～63 です。大文字、小文字を区別します。

説明

role コマンドはユーザロールを作成し、user role view に移行します。ユーザロールが作成されている場合、直接 user role view に移行します。

undo role コマンドはユーザロールを削除します。

定義済みのユーザロールに加えて 64 のユーザロールを作成することができます。

定義済みのユーザロールを削除することはできません。あるいは定義済みの network-admin、network-operator、level-15 に割り当てられた許可を変更することはできません。

Level-0～level-14 のユーザロールのルールとリソースアクセスポリシーを修正できます。しかし定義済みのアクセス権限を変更することはできません。たとえば、**display history-command all** コマンドのアクセス権限を変更することはできません。

例

ユーザロール role1 を作成し、user role view に移行します。

<Switch> system-view

[Switch] role name role1

[Switch-role-role1]

関連コマンド

- **display role**
- **interface policy deny**
- **rule**
- **vlan policy deny**

2.1.10 role default-role enable

Syntax

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

undo role default-role enable

デフォルト

デフォルトユーザロール機能は無効です。ユーザロールがない AAA ユーザは装置にログインすることができません。

View

System view

定義済みユーザロール

network-admin

パラメータ

role-name: ユーザロール名を指定します。設定範囲は 1～63 です。大文字、小文字を区別します。ユーザロールはすでに作成されている必要があります。

説明

role default-role enable コマンドはリモート AAAユーザのデフォルトユーザロールを有効にします。

undo role default-role enable コマンドはデフォルトに戻します。

認証（ローカルあるいはリモート）サーバがユーザにすべてのユーザロールを許可しない場合、デフォルトユーザロール機能は AAA 認証ユーザにデフォルトユーザロールを割り当てます。これらのユーザは、デフォルトユーザロールでシステムへのアクセスが許可されます。

AAA ユーザにユーザロールが割り当てられている場合、ユーザロールでログインします。

role-name パラメータの指定がない場合、デフォルトユーザロールとしてコマンドは network-operator を指定します。

例

デフォルトユーザロール機能を有効にします。

<Switch> system-view

[Switch] role default-role enable

関連コマンド

role

2.1.11 role feature-group

Syntax

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

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

デフォルト

ユーザロールグループ L2、L3 が作成されています。

View

System view

定義済みユーザロール

network-admin

パラメータ

name *feature-group-name*: 機能グループ名を指定します。設定範囲は 1～31 です。大文字、小文字を区別します。

説明

role feature-group コマンドはユーザロール機能グループを作成し、ユーザロールの group view に移行します。

undo role feature-group コマンドはユーザロール機能グループを削除します。

L2 機能グループはすべてのレイヤ 2 機能コマンドを含みます。L3 機能グループはすべてのレイヤ 3 機能コマンドを含みます。この定義済みの機能グループはユーザが設定できません。

定義済みの機能グループ L2、L3 に加えて、最大 64 のユーザ機能グループを作成することができます。

例

機能グループ security-features を作成し、ユーザロールの group view に移行します。

<Switch> system-view

[Switch] role feature-group name security-features

[Switch-featuregrp-security-features]

関連コマンド

- **display role feature**
- **display role feature-group**
- **feature**

2.1.12 rule

Syntax

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

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

デフォルト

ユーザが定義したユーザロールにルールがなく、すべてのコマンドへのアクセスができません。

View

User role view

定義済みユーザロール

network-admin

パラメータ

number: ルール番号を指定します。設定範囲は 1～256 です。

deny: 指定されたコマンドへのアクセスを拒否します。

permit: 指定されたコマンドへのアクセスを許可します。

command *command-string*: コマンドを指定します。*command-string* の設定範囲は 1～128 です。大文字、小文字を区別します。以下の記号を含むことができます。

- ワイルドカードアスタリスク（*）
- 半角スペースとタブキーの区切り記号
- 印刷可能な文字列

execute: 実行コマンドを指定します。**execute** コマンドは指定した機能あるいはプログラムを実行します。たとえば **ping** コマンドです。

read: 読み込みコマンドを指定します。**read** コマンドは設定を表示あるいは情報を維持します。たとえば、**display**、**dir**、**more**、**pwd** コマンドです。

write: 書き込みコマンドを指定します。**write** コマンドはシステムを設定します。たとえば、**ssh server enable** コマンドです。

feature [*feature-name*]: 1 つ以上の機能を指定します。*feature-name* は機能名を指定します。機能名を指定しない場合、システムのすべての機能を指定します。

feature-group *feature-group-name*: ユーザ定義あるいは定義済みの機能グループを指定します。*feature-group-name* は機能グループ名を示します。設定範囲は 1～31 です。大文字、小文字を区別します。機能グループが作成されていない場合、ルールはグループが作成されたのち適用されます。作成された機能グループを表示する場合、**display role feature-group** コマンドを使用します。

all: すべてのユーザロールのルールを削除します。

説明

rule コマンドは制御するコマンドのユーザロールのルールを作成あるいは変更します。

undo rule コマンドはユーザロールのルールを削除します。

細分化された異なるアクセス制御を行うため、以下のルールのタイプを定義することができます。

- **コマンドルール**－正規表現に一致するコマンドあるいはコマンドリストへのアクセス制御を行います。
- **機能ルール**－コマンドタイプによって機能のコマンドにアクセス制御を行います。
- **機能グループルール**－コマンドタイプによって機能グループのコマンドにアクセス制御を行います。

ユーザロールはユーザロールのルールで指定された許可されたコマンドリストにアクセスすることができます。ユーザロールは定義済み（sys-n で識別されます）、ユーザ定義のユーザロールのルールが含まれます。

ユーザロールに 256 のユーザ定義のルールを設定することができます。ユーザ定義のユーザロールのルールの合計は 1024 を超過することができません。

ユーザロールのルールの修正、追加、削除は変更されたのちにユーザロールにログインしたユーザにのみ適用されます。

ファイルシステムコマンドへのアクセスはファイルシステムコマンドのルールとファイルシステム機能のルールの両方で制御されます。

コマンドタイプ write がファイルシステム機能に割り当てられたとき、ファイルシステムへの出力のリダイレクトのコマンドのみが許可されます。

以下にルールを適用するガイドラインを示します。

- 同一タイプのユーザ定義のルールが混在した場合、高い IDのルールが適用されます。たとえば、もしユーザロールに以下のコマンドを使用したルールが含まれる場合、ユーザロールが **tracert** コマンドを使用することができますが、**ping** コマンドは使用できません。
  - □ **rule 1 permit command ping**
  - □ **rule 2 permit command tracert**
  - □ **rule 3 deny command ping**
- 定義済みのユーザロールのルールとユーザ定義のユーザロールが混在した場合、ユーザ定義したユーザロールが適用されます。

コマンド文字列を指定するとき、表 2-3 のガイドラインに従ってください。

表 2-3 コマンド文字列設定ルール

ルール	ガイドライン
区切り機能がセミコロン（;）です。	コマンドあるいはコマンドリストにアクセスする前に、各viewのコマンドを区切るためにセミコロンを使用してください。しかし**display**コマンドや**dir**コマンドなどuser viewや、すべてのviewで有効なコマンドを区切るためにセミコロンを使用しないでください。 セミコロンで区切られたセグメントは、最小限、印刷可能な1文字がある必要があります。 viewにあるが、サブviewにないコマンドを指定する場合、最後のセグメントの最後の印刷可能な文字にセミコロンを使用してください。viewとviewのサブviewにあるコマンドを指定する場合、最後のセグメントの最後の印刷可能な文字にセミコロンを使用しないでください。 たとえば、interface viewに移行する前にsystem viewに移行してください。すべてのinterface viewの**ip**パラメータで開始するすべてのコマンドを指定するため、**system ; interface * ; ip * ;**を使用してください。 **system ; radius scheme * ;**コマンドはsystem viewの**radius scheme**パラメータで始まるすべてのコマンドを示します。 **system ; radius scheme ***コマンドはsystem viewの**radius scheme**パラメータで始まるすべてのコマンドとRADIUS scheme viewのすべてのコマンドを示します。

ルール	ガイドライン
アスタリスク（*）がワイルドカードです。	アスタリスクは0あるいは複数の文字を示します。 最後のセグメントでない場合、セグメントの最後のみアスタリスクを使用することができます。 最後のセグメントである場合、セグメントのいずれの位置でもアスタリスクを使用することができます。アスタリスクから始まる場合、アスタリスクの後ろに印刷可能な文字を指定することができません。 たとえば、**system ; *コマンド**はsystem viewとsystem viewのサブviewで有効なすべてのコマンドを示します。**debugging * event**コマンドはuser viewで有効なすべてのイベントをデバッグするコマンドを示します。
パラメータの省略ができます。	パラメータの最初の数文字を入力することでパラメータを指定することができます。ルールに一致する文字列から始まるすべてのコマンドです。 たとえば、**rule 1 deny command dis arp source ***コマンドは**display arp source-mac interface**コマンドと**display arp source-suppression**コマンドのアクセスを拒否します。
コマンドへのアクセスを制御するため、コマンドがあるviewの直後にコマンドを指定する必要があります。	コマンドへのアクセスを制御するため、コマンドが割り当てられたviewの直後にコマンドを指定する必要があります。すべてのサブviewのコマンドを制御するルールはコマンドに適用されません。 たとえば、**rule 1 deny command system ; interface * ; ***コマンドはinterface viewに割り当てられたコマンドへのアクセスを無効にします。しかしこのコマンドはsystem viewよりもinterface viewで割り当てられるため、interface viewの**acl advanced**コマンドを実行することができます。 このコマンドへのアクセスを無効にする場合、**rule 1 deny command system ; acl *;**コマンドを使用します。
ユーザロールのコマンドルールの**display**コマンドを指定するとき、垂直バー（|）、大なり記号（>）、2重大なり記号（>>）を含みません。	システムはコマンドラインの一部として記号に従うリダイレクト記号とパラメータを含みません。 ユーザロールのコマンドルールで、コマンドラインの一部にリダイレクト記号とパラメータが存在します。その結果、これらの記号を含むルールは一致するコマンドはありません。 たとえば、**rule 1 permit command display debugging > log**コマンドは、**display debugging**コマンドではなく、**display debugging > log**コマンドに一致するコマンドはありません。

例

display acl コマンドを実行するユーザロール role1 を許可します。

<Switch> system-view

[Switch] role name role1

[Switch-role-role1] rule 1 permit command display acl

display パラメータで開始するすべてのコマンドを実行するユーザロール role1 を許可します。

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

system view の **radius scheme aaa** コマンドを実行するユーザロール role1 を許可し、RADIUS scheme view に割り当てられたすべてのコマンドを使用します。

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

すべての機能の read あるいは write コマンドへアクセスするユーザロール role1 を拒否します。

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

aaa 機能のすべての read コマンドへアクセスするユーザロール role1 を拒否します。

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

機能グループ security-features の read、write、execute コマンドへアクセスするユーザロール role1 を許可します。

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

関連コマンド

- **display role**
- **display role feature**
- **display role feature-group**
- **display web menu**
- **role**

2.1.13 super

Syntax

super [*role-name*]

View

User view

定義済みユーザロール

network-admin

パラメータ

role-name: ユーザロールを指定します。設定範囲は 1～63 です。大文字、小文字を区別します。システムにユーザロールが存在する必要があります。ユーザロールを指定しな

い場合、**super default role** コマンドで設定されたデフォルトターゲットのユーザロールを取得します。

説明

super コマンドは装置に再接続することなく、別のユーザロールを取得します。

このコマンドは現在のログインでのみ適用されるため、取得されたユーザロールは一時的なユーザロールです。次回ユーザアカウントでログインすると、元のユーザロールの設定が適用されます。

装置に再接続することなく、ユーザが別のユーザロールを取得するため、ユーザロールの認証を設定する必要があります。

- ローカルパスワードがローカルパスワード認証（local）で設定されていない場合、AUXユーザはいずれかの文字列を入力するか、なにも入力しないことでユーザロールの許可を取得できます。
- ローカルパスワードが local-then-remote 認証（local scheme）で設定されていない場合、以下のルールが適用されます。
  - VTY ユーザはリモート認証を実行します。
  - AUXユーザはいずれかの文字列を入力するか、なにも入力しないことでユーザロールの許可を取得できます。

例

ユーザロール network-operator を取得します。

<Switch> super network-operator

Password:

ユーザ権限は network-operator で、ロールに許可されたコマンドのみ使用することができます。

関連コマンド

- **authentication super**（コマンドマニュアルのセクション 9 *セキュリティ*）
- **super authentication-mode**
- **super password**

2.1.14 super authentication-mode

Syntax

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

undo super authentication-mode

デフォルト

local

View

System view

定義済みユーザロール

network-admin

パラメータ

local: ローカルパスワード認証を有効にします。

scheme: リモート AAA 認証を有効にします。

説明

super authentication-mode コマンドは一時的なユーザロールの許可を取得するため認証モードを設定します。

undo super authentication-mode コマンドはデフォルトに戻します。

ローカルパスワードでは、パスワードを設定するため、**super password** コマンドを使用します。

リモート AAA 認証では、RADIUS サーバのユーザ名とパスワードを設定します。

local パラメータと **scheme** パラメータの両方を指定した場合、最初に指定されたパラメータが適用されます。

- **scheme local**– remote-then-local 認証モードを有効にします。装置は一時的なユーザロールを取得するため、最初に AAA 認証を実行します。リモート RADIUS サーバが応答しないあるいは装置の AAA の設定が無効である場合、ローカル認証が実行されます。
- **local scheme**– local-then-remote 認証モードを有効にします。装置は最初にローカルパスワード認証を実行します。ユーザロールのパスワードが設定されていない場合、装置は VTY ユーザのリモート認証を実行します。AUXユーザはいずれかの文字列を入力するか、なにも入力しないことで別のユーザロールを取得できます。

AAA の詳細は、オペレーションマニュアルのセクション 9 *セキュリティ* “*AAA*”を参照してください。

例

一時的なユーザロールの許可を取得するため、local-only 認証を有効にします。

<Switch> system-view

[Switch] super authentication-mode local

一時的なユーザロールの許可を取得するため、remote-then-local 認証を有効にします。

<Switch> system-view

[Switch] super authentication-mode scheme local

関連コマンド

- **authentication super**（コマンドマニュアルのセクション 9 *セキュリティ*）
- **super password**

2.1.15 super default role

Syntax

super default role *role-name*

undo super default role

デフォルト

network-admin

View

System view

定義済みユーザロール

network-admin

パラメータ

role-name: デフォルトターゲットユーザロールの名前を指定します。設定範囲は 1～63 です。大文字、小文字を区別します。システムにユーザロールが存在する必要があります。

説明

super default role コマンドは一時的なユーザロールの許可を取得するためデフォルトターゲットのユーザロールを指定します。

undo super default role コマンドはデフォルトに戻します。

コマンドのユーザロールを指定しないとき、デフォルトターゲットのユーザロールが **super** コマンドあるいは **super password** コマンドに割り当てられます。

例

一時的なユーザロールの許可を取得するため、デフォルトターゲットのユーザロールを network-operator に指定します。

<Switch> system-view

[Switch] super default role network-operator

関連コマンド

- **super**
- **super password**

2.1.16 super password

Syntax

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

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

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

role *role-name*: ユーザロールを指定します。設定範囲は 1～63 です。大文字、小文字を区別します。システムにユーザロールが存在する必要があります。ユーザロールを指定しない場合、**super default role** コマンドで設定されたデフォルトターゲットのユーザロールのパスワードを設定します。

hash: ハッシュテキストのパスワードを設定します。

simple: プレーンテキストのパスワードを設定します。セキュリティのため、ハッシュテキストで保存され、暗号化されます。

string: パスワードを指定します。引数は大文字、小文字を区別します。

- **simple** キーワードが指定される場合、パスワードの設定範囲は 1～63 文字です。
- **hash** キーワードが指定される場合、パスワードの設定範囲は 1～110 文字です。

説明

super password コマンドはユーザロールのパスワードを設定します。

undo super password コマンドはデフォルトに戻します。

パラメータを指定しない場合、インタラクティブモードでプレーンテキストパスワードを指定します。

一時的なユーザロールの許可のローカルパスワード認証を設定する場合、パスワードを設定します。

異なるユーザロールに異なるパスワードを指定することを推奨します。

例

ユーザロール network-operator のパスワード 123456TESTplat&!を設定します。

<Switch> system-view

[Switch] super password role network-operator simple 123456TESTplat&!

ユーザロール network-operator のパスワード 123456TESTplat&!をインタラクティブモードで設定します。

<Switch> system-view

[Switch] super password role network-operator

```
Password:
Confirm :
Updating user information. Please wait... ...
```

関連コマンド

- **super authentication-mode**
- **super default role**

2.1.17 vlan policy deny

Syntax

vlan policy deny

undo vlan policy deny

デフォルト

設定なし

View

User role view

定義済みユーザロール

network-admin

説明

vlan policy deny コマンドは VLAN へのユーザロールのアクセスを拒否し、ユーザロールの VLAN policy view に移行します。

undo vlan policy deny コマンドはデフォルトに戻します。

指定した VLAN のみユーザロールの VLAN へのアクセスを制限するために、以下の作業を行います。

1) **vlan policy deny** コマンドで VLAN へのアクセスを拒否します。
2) **permit vlan** コマンドでアクセス可能な VLAN を指定します。

🕮 **メモ：**

interface policy deny コマンドは、**permit interface** コマンドが設定されていない場合、すべての VLAN へのユーザロールのアクセスを拒否します。

VLAN を設定するため、ユーザロールの VLAN ポリシーで許可されている VLAN が使用されていることを確認してください。アクセス可能な VLAN で以下の操作を実行することができます。

- VLAN の作成、削除、設定を行います。
- VLAN view へ移行します。
- **feature** コマンドで VLAN を指定します。

ユーザロールの VLAN ポリシーの変更は、変更後にユーザロールにログインしたユーザのみ適用されます。

例

role1 の VLAN policy view に移行し、VLAN へのユーザロール role1 のアクセスを拒否します。

<Switch> system-view

[Switch] role name role1

[Switch-role-role1] vlan policy deny

[Switch-role-role1-vlanpolicy] quit

role1 の VLAN policy view に移行し、VLAN 50～VLAN 100 を除く VLAN へのユーザロール role1 のアクセスを拒否します。

<Switch> system-view

[Switch] role name role1

[Switch-role-role1] vlan policy deny

[Switch-role-role1-vlanpolicy] permit vlan 50 to 100

関連コマンド

- **display role**
- **permit vlan**
- **role**

目次

このセクションのページは **1-x-x** です。

3章 ログイン 3-1
3.1 ログイン設定コマンド 3-1
3.1.1 authentication-mode 3-1
3.1.2 auto-execute command 3-3
3.1.3 databits 3-4
3.1.4 display ip http 3-5
3.1.5 display ip https 3-6
3.1.6 display line 3-7
3.1.7 display telnet client 3-9
3.1.8 display user-interface 3-10
3.1.9 display users 3-12
3.1.10 display web users 3-13
3.1.11 escape-key 3-14
3.1.12 free line 3-17
3.1.13 free user-interface 3-18
3.1.14 free web users 3-19
3.1.15 history-command max-size 3-19
3.1.16 idle-timeout 3-20
3.1.17 ip http acl 3-21
3.1.18 ip http enable 3-22
3.1.19 ip http port 3-23
3.1.20 ip https acl 3-24
3.1.21 ip https certificate access-control-policy 3-25
3.1.22 ip https enable 3-26
3.1.23 ip https port 3-27
3.1.24 ip https ssl-server-policy 3-27
3.1.25 line 3-28
3.1.26 line class 3-29
3.1.27 lock 3-30
3.1.28 lock reauthentication 3-31
3.1.29 lock-key 3-32
3.1.30 parity 3-34
3.1.31 protocol inbound 3-35
3.1.32 restful http enable 3-37
3.1.33 restful https enable 3-37
3.1.34 screen-length 3-38

3.1.35 send 3-39
3.1.36 set authentication password 3-40
3.1.37 shell 3-42
3.1.38 speed....3-43
3.1.39 stopbits 3-44
3.1.40 telnet....3-45
3.1.41 telnet client source....3-46
3.1.42 telnet ipv6 3-47
3.1.43 telnet server acl 3-48
3.1.44 telnet server acl-deny-log enable 3-49
3.1.45 telnet server dscp 3-50
3.1.46 telnet server enable 3-50
3.1.47 telnet server ipv6 acl 3-51
3.1.48 telnet server ipv6 dscp 3-52
3.1.49 terminal type....3-53
3.1.50 user-interface 3-54
3.1.51 user-interface class....3-55
3.1.52 user-role....3-57
3.1.53 web idle-timeout 3-58

3章 ログイン

3.1 ログイン設定コマンド

いくつかのログインコマンドは user line view と user line class view の両方で有効です。

- user line view の設定は、user line にのみ適用されます。user line class view はクラスのすべての user line に適用されます。
- user line view と user line class view のどちらかの view でデフォルトでない設定がある場合、デフォルトでない設定は、もう一方のデフォルト設定よりも優先されます。user line view のデフォルトでない設定は user line class view のデフォルトでない設定よりも優先されます。

3.1.1 authentication-mode

Syntax

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

undo authentication-mode

デフォルト

AUX line class の認証モードは password です。

AUX line の認証モードは none です。

VTY line/VTY line class の認証モードは password です。

View

User line view

User line class view

定義済みユーザロール

network-admin

パラメータ

none: 認証を無効にします。

password: ローカルパスワード認証を行います。

scheme: AAA 認証を行います。AAA の詳細はオペレーションマニュアルのセクション 9 *セキュリティ”AAA”*を参照してください。

説明

authentication-mode コマンドは user line の認証モードを設定します。

undo authentication-mode コマンドはデフォルトに戻します。

network-admin あるいはレベル 15 のユーザロールが割り当てられたユーザのみコマンドを実行することができます。実行権限があったとしてもほかのユーザはコマンドを実行できません。

認証モードが **none** である場合、すべてのユーザは認証なしでログインすることができます。装置のセキュリティを改善するため、認証モードを **password** あるいは **scheme** にしてください。

VTY line view で、**authentication-mode** コマンドは **protocol inbound** コマンドと関連します。

- VTY line view の 2 つのコマンドの設定がデフォルトでない場合、VTY line view のデフォルトでない認証モードを使用します。
- VTY line view で 2 つのコマンドのうち、1 つコマンドのみデフォルトでない認証モードである場合、もう一方のコマンドは VTY line class view の設定に関わらず、デフォルトの認証モードを使用します。

認証モードを変更した場合、現在のセッションに影響しません。次にログインしたときに適用されます。

例

user line VTY 0 で認証モードを none にします。

<Switch> system-view

[Switch] line vty 0

[Switch-line-vty0] authentication-mode none

user line VTY 0 で認証モードを password に設定し、パスワードを 321 に設定します。

<Switch> system-view

[Switch] line vty 0

[Switch-line-vty0] authentication-mode password

[Switch-line-vty0] set authentication password simple 321

user line VTY 0 で認証モードを scheme に設定します。ローカルユーザ 123 を設定し、パスワードを 321 に設定します。Telnet サービスを割り当て、ユーザのユーザロールを network-admin に割り当てます。

<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

関連コマンド

set authentication password

3.1.2 auto-execute command

⚠ **注意:**

user line にこのコマンドを実行すると、user line による CLI アクセスができなくなる可能性があります。このコマンドを設定する前に、異なる user line によって CLI にアクセスできることを確認してください。

Syntax

auto-execute command *command*

undo auto-execute command

デフォルト

無効

View

User line view

User line class view

定義済みユーザロール

network-admin

パラメータ

command: 自動で実行されるコマンドを指定します。

説明

auto-execute コマンドは、ユーザが現在の user line にログインしたとき、自動で実行されるコマンドを指定します。

undo auto-execute コマンドは設定を削除します。

ユーザが現在の user line にログインしたとき、装置は自動で指定されたコマンドを実行します。コマンドが実行されたのち、ユーザの接続を切断します。

このコマンドは AUX line view あるいは AUX line class view でサポートしていません。このコマンドは user line view および user line class view の両方でサポートしています。

- user line view の設定がデフォルトでないとき、user line view の設定が適用されます。
- user line view の設定がデフォルトで user line class view の設定がデフォルトでないとき、user line class view の設定が適用されます。

設定を変更した場合、現在のセッションに影響しません。次にログインしたときに適用されます。

例

ユーザが VTY line 0 にログインした後、自動的に Telnet192.168.1.41 を実行するように設定します。

<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]
```

設定を確認するため、192.168.1.40 に Telnet します。

装置は自動的に 192.168.1.41 に Telnet し、以下の出力が表示されます。

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>
```

この動作は、Telnet で 192.168.1.41 に直接ログインすることと同一です。192.168.1.41 への Telnet 接続を終了するとき、同時に 192.168.1.40 への Telnet 接続も終了されます。

3.1.3 databits

Syntax

databits { **5** | **6** | **7** | **8** }

undo databits

デフォルト

8

View

User line view

定義済みユーザロール

network-admin

パラメータ

5: データビット数 5 を指定します。

6: データビット数 6 を指定します。

7: データビット数 7 を指定します。

8: データビット数 8 を指定します。

説明

databits コマンドは各文字のデータビット数を指定します。

undo databits コマンドはデフォルトに戻します。

このコマンドは VTY line view でサポートしていません。

この設定は端末のデータビットと同一にしてください。

例

AUX 0 のデータビットを 7 に設定します。

<Switch> system-view

[Switch] line aux 0

[Switch-line-aux0] databits 7

3.1.4 display ip http

Syntax

display ip http

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display ip http コマンドは HTTP サービスの設定とステータス情報を表示します。

例

HTTP サービスの設定とステータス情報を表示します。

<Switch> display ip http

```
HTTP port: 80
Basic ACL: 2222
HTTP status: Enabled
```

表 3-1 コマンド出力

フィールド	説明
HTTP port	HTTPサービスのポート番号です。
Basic ACL	HTTPアクセスを制御するために使用されるACLです。HTTPサービスにACLが割り当てられていない場合、0と表示されます。
HTTP status	HTTPサービスが有効かどうかを示します。

関連コマンド

- **ip http acl**
- **ip http enable**
- **ip http port**

3.1.5 display ip https

Syntax

display ip https

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display ip https コマンドは HTTPS サービスの設定とステータス情報を表示します。

例

HTTPS サービスの設定とステータス情報を表示します。

<Switch> display ip https

```
HTTPS port: 443
SSL server policy: test
```

```
Certificate access control policy: Not configured
Basic ACL: 2222
HTTPS status: Enabled
```

表 3-2 コマンド出力

フィールド	説明
HTTPS port	HTTPSサービスのポート番号です。
SSL server policy	HTTPSサービスに割り当てられたSSLサービスポリシーです。HTTPSサービスにSSLサービスポリシーが割り当てられていない場合、**Not configured**と表示されます。
Certificate access-control-policy	クライアントアクセス権の制御に使用される証明書属性ベースのアクセスコントロールポリシーです。HTTPSサービスにアクセスコントロールポリシーが割り当てられていない場合、**Not configured**と表示されます。
Basic ACL	HTTPSアクセスを制御するために使用されるACLです。HTTPSサービスにACLが割り当てられていない場合、**0**と表示されます。
HTTPS status	HTTPSサービスが有効かどうかを示します。

関連コマンド

- **ip https acl**
- **ip https certificate access-control-policy**
- **ip https enable**
- **ip https port**
- **ip https ssl-server-policy**

3.1.6 display line

Syntax

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

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

number1: user line の通し番号を指定します。設定範囲は 0～73 です。

aux: AUX line を指定します。

vty: VTY line を指定します。

number2: user line のタイプごとの番号を指定します。AUX line の設定範囲は 0～9 で、VTY の設定範囲は 0～63 です。

summary: user line についての概要情報を表示します。このキーワードを指定しない場合、詳細な情報が表示されます。

説明

display line コマンドは user line の情報を表示します。

例

line 0 の情報を表示します。

<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.
```

表 3-3 コマンド出力

フィールド	説明
Modem	モデムのモードがin/outを示します。デフォルトでは設定されていません。ハイフン(－)が表示されます。
Int	lineの物理ポートです。lineに物理ポートがない、あるいはコンソールポートの場合、ハイフン(－)が表示されます。
Location	lineの物理的な位置です。スロット番号/CPU番号の形式です。

すべての user line の概要情報を表示します。

<Switch> display line summary

```
  Line type : [AUX]
```

```
          0:XXXX XXXX XX
  Line type : [VTY]
         10:UUXX XXXX XXXX XXXX
         26:XXXX XXXX XXXX XXXX
         42:XXXX XXXX XXXX XXXX
         58:XXXX XXXX XXXX XXXX


   2 lines used.     (U)
  72 lines not used.  (X)
```

表 3-4 コマンド出力

フィールド	説明
Line type	user lineのタイプです。 ● **AUX**—AUX lineです。 ● **VTY**—VTY lineです。
number:status	*number*はuser line classの最初のuser lineの通し番号を示します。0からの番号です。*status*はuser line classのuser lineが使用されているかどうかを示します。Xは未使用でUは使用されています。

3.1.7 display telnet client

Syntax

display telnet client

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display telnet client コマンドは、Telnet クライアント用のパケットの送信元の設定を表示します。

装置が Telnet クライアントとして動作するとき、**telnet client source** コマンドによって Telnet パケットを送信するときの送信元 IPv4 アドレスあるいは送信元インタフェースを表示します。

例

Telnet クライアント用のパケットの送信元の設定を表示します。

<Switch> display telnet client

```
The source IP address is 1.1.1.1.
```

関連コマンド

telnet client source

3.1.8 display user-interface

Syntax

display user-interface [*number1* | { **aux** | **vty** } *number2*] [**summary**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

number1: user line の絶対番号です。設定範囲は 0～73 です。

aux: AUX line を指定します。

vty: VTY line を指定します。

number2: user line の相対番号を指定します。AUX line の設定範囲は 0～9 です。VTY line の設定範囲は 0～63 です。

summary: user line の概要を表示します。指定しない場合、詳細な情報を表示します。

説明

display user-interface コマンドは user line の情報を表示します。

このコマンドは古いソフトウェアバージョンで使用していたユーザのためにサポートされているコマンドです。古いソフトウェアバージョンで動作するコマンドです。**display line** コマンドと同一機能です。通常は **display line** コマンドを使用してください。

例

line 0 の情報を表示します。

Switch> display user-interface 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.
```

表 3-5 コマンド出力

フィールド	説明
Modem	モデムのモードがin/outを示します。デフォルトでは設定されていません。ハイフン(−)が表示されます。
Int	lineの物理ポートです。lineに物理ポートがない、あるいはコンソールポートの場合、ハイフン(−)が表示されます。
Location	lineの物理的な位置です。スロット番号/CPU番号の形式です。

すべての user line の概要情報を表示します。

<Switch> display user-interface summary

```
Line type : [AUX]
        0:XXXX XXXX XX
Line type : [VTY]
       10:UXUX XXXX XXXX XXXX
       26:XXXX XXXX XXXX XXXX
       42:XXXX XXXX XXXX XXXX
       58:XXXX XXXX XXXX XXXX

 2 lines used.     (U)
72 lines not used.  (X)
```

表 3-6 コマンド出力

フィールド	説明
Line type	user lineのタイプです。 ● **AUX**—AUX lineです。 ● **VTY**—VTY lineです。

フィールド	説明
number:status	*number*はuser line classの最初のuser lineの通し番号を示します。0からの番号です。*status*はuser line classのuser lineが使用されているかどうかを示します。Xは未使用でUは使用されています。

3.1.9 display users

Syntax

display users [**all**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all: 装置でサポートされるすべての user line を表示します。

説明

display usersコマンドは、オンライン CLI ユーザの情報を表示します。

例

オンライン CLI ユーザの情報を表示します。

<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.
```

表 3-7 コマンド出力

フィールド	説明
Idx	user lineの通し番号です。
Line	user lineのタイプとタイプごとの番号です。
Idle	ユーザがログインしてからの経過時間です。hh:mm:ssで表示します。
Time	ユーザのログイン時間です。
Pid	ユーザセッションのプロセスIDです。
Type	ユーザタイプです。 ● **TEL**—Telnetユーザです。 ● **SSH**—SSHユーザです。 コンソールポートでログインしているユーザは、表示されません。
+	カレントユーザが使用しているuser lineを示します。
Location	カレントユーザのIPアドレスです。

3.1.10 display web users

Syntax

display web users

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display web users コマンドはオンライン Web ユーザを表示します。

例

オンライン Web ユーザを表示します。

<Switch> display web users

```
UserID        Name          Type   Language JobCount LoginTime LastOperation
```

```
AB2039483271293 Administrator   HTTP   Chinese    3    12:00:23  14:10:05
F09382BA2014AC8 user            HTTPS  English    1    13:05:00  14:11:00
```

表 3-8 コマンド出力

フィールド	説明
UserID	オンラインWebユーザを一意に識別するために使用されるIDです。
JobCount	ユーザによって接続が確立された数です。

3.1.11 escape-key

Syntax

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

undo escape-key

デフォルト

Ctrl+C

View

User line view

User line class view

定義済みユーザロール

network-admin

パラメータ

key-string: ショートカットキーを指定します。“d”、“D” を除く文字列あるいは ASCII コードで指定します。文字列は大文字、小文字を区別します。ASCII コードの設定範囲は 0～127 です。たとえば、**escape-key** 1 コマンドを設定した場合、ショートカットキーは Ctrl+A です。escape-key a コマンドを設定した場合、ショートカットキーは a です。文字列に“d”あるいは“D”を指定した場合、ショートカットキーは Ctrl+C となります。ショートカットキーとして“d”あるいは“D”を指定する場合、ASCII コードで指定する必要があります。Ctrl キーを使用する ASCII コードの詳細は表 3-9 を参照してください。

表 3-9 Ctrl キーを使用する ASCII コード

フィールド	説明
Ctrl+A	1

フィールド	説明
Ctrl+B	2
Ctrl+C	3
Ctrl+D	4
Ctrl+E	5
Ctrl+F	6
Ctrl+G	7
Ctrl+H	8
Ctrl+I	9
Ctrl+J	10
Ctrl+K	11
Ctrl+L	12
Ctrl+M	13
Ctrl+N	14
Ctrl+O	15
Ctrl+P	16
Ctrl+Q	17
Ctrl+R	18
Ctrl+S	19
Ctrl+T	20
Ctrl+U	21
Ctrl+V	22
Ctrl+W	23
Ctrl+X	24
Ctrl+Y	25

フィールド	説明
Ctrl+Z	26

default: エスケープキーを Ctrl+C に戻します。

説明

escape-key コマンドはエスケープキーを設定します。

undo escape-key コマンドはエスケープキーを無効にします。

実行したコマンドを中断する場合、エスケープキーを押下します。たとえば、ping コマンド、tracert コマンドを中断する場合に使用します。デフォルトで Ctrl+C が指定されているかどうかはコマンドの実装によって異なります。詳細はコマンドのガイドラインに従ってください。

エスケープキーとしてキーシーケンスを使用します。エスケープシーケンスとして 1 文字を指定する場合、実行したコマンドを中断するとき、キーを押下します。コマンドが実行されない場合、通常の文字列としてキーが入力されます。装置からリモート装置に Telnet を行う場合、エスケープキーを押下した場合、リモート装置の通常の文字列として入力されます。以下の状況に一致した場合のみ、リモート装置でエスケープキーを使用することができます。

- リモート装置でエスケープキーが同一の文字列で定義されています。
- リモート装置でコマンドを実行している間にキーを入力しました。

undo escape-key コマンドは現在のエスケープキーを無効にします。

コマンドは user line view と user line class view で有効です。user line view と user line class view のどちらかの view でデフォルトでない設定がある場合、デフォルトでない設定は、もう一方のデフォルト設定よりも優先されます。user line view のデフォルトでない設定は user line class view のデフォルトでない設定よりも優先されます。

user line view で設定した場合、現在のセッションにすぐに適用します。user line class view で設定を変更した場合、現在のセッションに影響しません。次にログインしたときに適用されます。

現在のエスケープキーを表示する場合、**display current-configuration | include escape-key** コマンドを使用します。

例

VTY line 0 でエスケープキーとして a を設定します。

<Switch> system-view

[Switch] line vty 0

[Switch-line-vty0] escape-key a

設定を確認します。

2) IP アドレス 192.168.1.49 に ping を実行します。-c パラメータを使用して ICMP エコーリクエストパケットの数を 20 に設定します。

<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
```

3) a を押下します。

システムはコマンドを中断し、user view に戻ります。

```
--- 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>
```

3.1.12 free line

Syntax

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

View

User view

定義済みユーザロール

network-admin

パラメータ

number1: user line の通し番号を指定します。設定範囲は 0～73 です。

aux: AUX line を指定します。

vty: VTY line を指定します。

number2: user line のタイプごとの番号を指定します。AUX line の設定範囲は 0～9 で、VTY の設定範囲は 0～63 です。

説明

free line コマンドは user line を切断します。

カレントユーザを切断することはできません。

例

VTY 1 を切断します。

<Switch> free line vty 1

```
Are you sure to free line vty1? [Y/N]:y
 [OK]
```

3.1.13 free user-interface

Syntax

free user-interface { *number1* | { **aux** | **vty** } *number2* }

View

User view

定義済みユーザロール

network-admin

パラメータ

number1: user line の通し番号を指定します。設定範囲は 0～73 です。

aux: AUX line を指定します。

vty: VTY line を指定します。

number2: user line のタイプごとの番号を指定します。AUX line の設定範囲は 0～9 で、VTY の設定範囲は 0～63 です。

説明

free user-interface コマンドは user line を切断します。

カレントユーザを切断することはできません。

このコマンドは古いソフトウェアバージョンで使用していたユーザのためにサポートされているコマンドです。古いソフトウェアバージョンで動作するコマンドです。**free line** コマンドと同一機能です。通常は **free line** コマンドを使用してください。

例

VTY 1 を切断します。

<Switch> free user-interface vty 1

```
Are you sure to free line vty1? [Y/N]:y
 [OK]
```

3.1.14 free web users

Syntax

free web users { **all** | **user-id** *user-id* | **user-name** *user-name* }

View

User view

定義済みユーザロール

network-admin

パラメータ

all: すべての Web ユーザを指定します。

user-id: Web ユーザの ID を指定します。15 桁の 16 進数表示です。ユーザを識別するため、各 Web ユーザに一意の ID を割り当てます。

user-name: Web ユーザのユーザ名を指定します。設定範囲は 1～255 文字です。大文字、小文字を区別します。

説明

free web users コマンドはオンライン Web ユーザをログオフします。

例

すべてのオンライン Web ユーザをログオフします。

<Switch> free web users all

関連コマンド

display web users

3.1.15 history-command max-size

Syntax

history-command max-size *size-value*

undo history-command max-size

デフォルト

10

View

User line view

User line class view

定義済みユーザロール

network-admin

パラメータ

size-value: 履歴コマンドをバッファに保存できる最大数を指定します。設定範囲は 0～256 です。

説明

history-command max-size コマンドは user line のコマンドの履歴をバッファに保存する最大数を設定します。

undo history-command max-size コマンドはデフォルトに戻します。

各 user line は、実行された有効なコマンドを別のバッファに保存します。バッファサイズはバッファにいくつの履歴コマンドを保存できるかを決定します。

カレント user line で保存された履歴コマンドを表示する場合、矢印キーの↑あるいは↓を押下するか、**display history-command** コマンドを実行します。詳細はオペレーションマニュアルのセクション 1 *はじめに* “*CLI*”を参照してください。

CLI セッションを終了すると、履歴コマンドのバッファはクリアされます。

user line view での設定は現在のセッションにすぐさま適用されます。user line class view での設定は、設定が行われた後、ログインセッションで適用されます。

例

VTY line 0 のコマンドの履歴をバッファに記録する最大数を 20 に設定します。

<Switch> system-view

[Switch] line vty 0

[Switch-line-vty0] history-command max-size 20

3.1.16 idle-timeout

Syntax

idle-timeout *minutes* [*seconds*]

undo idle-timeout

デフォルト

10 分

View

User line view

User line class view

定義済みユーザロール

network-admin

パラメータ

minutes: タイムアウト時間の分を指定します。設定範囲は 0～35791 です。デフォルトは 10 分です。

seconds: タイムアウト時間の秒を指定します。設定範囲は 0～59 です。デフォルトは 0 秒です。

説明

idle-timeout コマンドは CLI セッションがタイムアウトする時間を設定します。

undo idle-timeout コマンドはデフォルトに戻します。

ユーザ操作が実行されずにタイムアウト時間が経過すると、ユーザ接続を切断します。

タイムアウト時間を 0 にすると、**idle-timeout** コマンドを無効にし、セッションがタイムアウトしません。

このコマンドは user line view および user line class view の両方でサポートしています。

- user line view の設定がデフォルトでないとき、user line view の設定が適用されます。
- user line view の設定がデフォルトで user line class view の設定がデフォルトでないとき、user line class view の設定が適用されます。

user line view での設定は現在のセッションにすぐさま適用されます。user line class view での設定は、設定が行われた後、ログインセッションで適用されます。

例

VTY line 0 の CLI セッションのタイムアウト時間を 1 分 30 秒に設定します。

<Switch> system-view

[Switch] line vty 0

[Switch-line-vty0] idle-timeout 1 30

3.1.17 ip http acl

Syntax

ip http acl *acl-number*

undo ip http acl

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

acl-number: ACL の番号を指定します。設定範囲は 2000～2999 です。

説明

ip http acl コマンドは HTTP サービスに ACL を割り当てます。

undo ip http acl コマンドは ACL の割り当てを削除します。

ip http acl コマンドを複数実行した場合、最後に行った設定が適用されます。

HTTP サービスに ACL が割り当てられたのち、ACL で許可されたクライアントのみ HTTP を通して装置にアクセスすることができます。

例

10.10.0.0/16 のユーザのみが HTTP を通して装置にアクセスできるように HTTP サービスに ACL2001 を割り当てます。

<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] ip http acl 2001

関連コマンド

acl（コマンドマニュアルのセクション 8 ***ACL and QoS***）

3.1.18 ip http enable

Syntax

ip http enable

undo ip http enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

ip http enable コマンドは HTTP サービスを有効にします。

undo ip http enable コマンドは HTTP サービスを無効にします。

ユーザが HTTP を通して装置にアクセスする場合、HTTP サービスを有効にする必要があります。

例

HTTP サービスを有効にします。

<Switch> system-view

[Switch] ip http enable

関連コマンド

ip https enable

3.1.19 ip http port

Syntax

ip http port *port-number*

undo ip http port

デフォルト

80

View

System view

定義済みユーザロール

network-admin

パラメータ

port-number: HTTP サービスのポート番号を指定します。設定範囲は 1～65535 です。

説明

ip http port コマンドは HTTP サービスのポート番号を指定します。

undo ip http port コマンドはデフォルトに戻します。

HTTP サービスが有効であるとき、HTTP サービスのポート番号を変更した場合、HTTP サービスを再度有効にし、すべての HTTP 接続を切断します。再度ログインする場合、ユーザは Web ブラウザのアドレスバーで新しい URL を入力する必要があります。

例

HTTP サービスのポート番号を 80 に指定します。

<Switch> system-view

[Switch] ip http port 80

3.1.20 ip https acl

Syntax

ip https acl *acl-number*

undo ip https acl

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

acl-number: ACL の番号を指定します。設定範囲は 2000～2999 です。

説明

ip https acl コマンドは HTTPS サービスに ACL を割り当てます。

undo ip https acl コマンドは ACL の割り当てを削除します。

HTTPS サービスに ACL が割り当てられたのち、ACL で許可されたクライアントのみ HTTPS を通して装置にアクセスすることができます。

装置は Web ログイン要求を転送する場合、常に HTTPS を使用するため、HTTPS サービスに適用された ACL は HTTPS と HTTP ログインの両方を制御します。装置にアクセスするため、HTTP クライアントは以下の ACL によって許可する必要があります。

- HTTP サービスに適用する ACL
- HTTPS サービスに適用する ACL

ip https acl コマンドを複数実行した場合、最後に行った設定が適用されます。

例

10.10.0.0/16 のユーザのみが HTTP あるいは HTTPS を通して装置にアクセスできるように ACL2001 を割り当てます。

<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] ip https acl 2001

関連コマンド

acl（コマンドマニュアルのセクション 8 ***ACL and QoS***）

3.1.21 ip https certificate access-control-policy

Syntax

ip https certificate access-control-policy policy-name

undo ip https certificate access-control-policy

デフォルト

設定なし

Views

System view

定義済みユーザロール

network-admin

パラメータ

policy-name: アクセスコントロールポリシーの証明書の名前を指定します（範囲：1～16 文字）。

説明

ip https certificate access-control-policy コマンドは、アクセスコントロールポリシーの証明書を HTTPS サービスに関連付けます。

undo ip https certificate access-control-policy コマンドは、アクセスコントロールポリシーの証明書と HTTPS サービスとの関連付けを無効にします。

デフォルト：無効

HTTPS サービスをアクセスコントロールポリシーの証明書に関連付けした後、クライアントが正しいアクセスであるかどうか管理することができます。

例

アクセスコントロールポリシーの証明書 myacl を HTTPS サーバに関連付けします。

<QX> system-view

[QX] ip https certificate access-control-policy myacl

3.1.22 ip https enable

Syntax

ip https enable

undo ip https enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

ip https enable コマンドは HTTPS サービスを有効にします。

undo ip https enable コマンドは HTTPS サービスを無効にします。

ユーザが HTTPS を通して装置にアクセスする場合、HTTPS サービスを有効にする必要があります。

HTTPS サービスを有効にすると、SSH ハンドシェークのネゴシエーションプロセスが開始します。

- 装置がローカル証明書を持っている場合、SSH ハンドシェークのネゴシエーションは成功し、HTTPS サービスを開始します。
- 装置がローカル証明書を持っていない場合、証明書アプリケーションプロセスが開始します。証明書アプリケーションプロセスは長い時間がかかるため、SSH ハンドシェークは失敗し、HTTPS サービスが開始されない可能性があります。この問題を解決するため、HTTPS サービスが有効になるまで **ip https enable** コマンドを再度実行します。

例

HTTPS サービスを有効にします。

<Switch> system-view

[Switch] ip https enable

3.1.23 ip https port

Syntax

ip https port *port-number*

undo ip https port

デフォルト

443

View

System view

定義済みユーザロール

network-admin

パラメータ

port-number: HTTPS サービスのポート番号を指定します。設定範囲は 1～65535 です。

説明

ip https port コマンドは HTTPS サービスのポート番号を指定します。

undo ip https port コマンドはデフォルトに戻します。

HTTPS サービスが有効であるとき、HTTPS サービスのポート番号を変更した場合、HTTPS サービスを再度有効にし、すべての HTTPS 接続を切断します。再度ログインする場合、ユーザは Web ブラウザのアドレスバーで新しい URL を入力する必要があります。

例

HTTPS サービスのポート番号を 8080 に指定します。

<Switch> system-view

[Switch] ip https port 8080

3.1.24 ip https ssl-server-policy

Syntax

ip https ssl-server-policy *policy-name*

undo ip https ssl-server-policy

デフォルト

無効

Views

System view

定義済みユーザロール

network-admin

パラメータ

policy-name: SSL サーバーエンドポリシーの名前を指定します (範囲: 1～31 文字)。

説明

ip https ssl-server-policy コマンドは、SSL サーバーエンドポリシーを HTTPS サービスに関連付けます。

undo ip https ssl-server-policy コマンドは、関連付けを削除します。

HTTPS サービスは、このコマンドが正常に設定された後、有効になります。

HTTPS サービスが有効になった後、SSL サーバーエンドポリシーを修正し、HTTPS サービスと SSL サーバーエンドポリシー間の関連付けを削除することはできません。

例

SSL サーバーエンドポリシーmyssl を HTTPS サーバに関連付けます。

<QX> system-view

[QX] ip https ssl-server-policy myssl

3.1.25 line

Syntax

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

View

System view

定義済みユーザロール

network-admin

パラメータ

first-number1: 最初の user line の通し番号を指定します。設定範囲は 0～73 です。

last-number1: 最後の user line の通し番号を指定します。*first-number1* よりも小さくすることはできません。

aux: AUX line を指定します。

vty: VTY line を指定します。

first-number2: 最初の user line のタイプごとの番号を指定します。AUX line の設定範囲は 0～9 で、VTY line の設定範囲は 0～63 です。

last-number2: 最後の user line のタイプごとの番号を指定します。VTY line の設定範囲は 1～9 です。*first-number2* よりも小さくすることはできません。

説明

line コマンドは 1 つ以上の user line view に移行します。

例

VTY line 0 の view に移行します。

<Switch> system-view

[Switch] line vty 0

[Switch-line-vty0]

VTY 0～VTY 63 の view に移行します。

<Switch> system-view

[Switch] line vty 0 63

[Switch-line-vty0-63]

関連コマンド

line class

3.1.26 line class

Syntax

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

View

System view

定義済みユーザロール

network-admin

パラメータ

aux: AUX line class view を指定します。

vty: VTY line class view を指定します。

説明

line class コマンドは user line class view に移行します。

line class のすべての user line で設定を同一にするために、user line class view に移行します。

user line class view では以下のコマンドを実行することができます。

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

いくつかのログインコマンドは user line view および user line class view の両方でサポートしています。

- user line view の設定は user line で適用されます。user line class view の設定は class のすべての user line で適用されます。
- user line view と user line class view のどちらかの view でデフォルトでない設定がある場合、デフォルトでない設定は、もう一方のデフォルト設定よりも優先されます。user line view のデフォルトでない設定は user line class view のデフォルトでない設定よりも優先されます。
- user line view の設定はすぐに適用され、オンラインユーザに影響します。user line class view の設定は設定が完了したのちにログインしたユーザのみ適用されます。user line class view の設定はオンラインユーザに影響しません。

例

VTY line class view でユーザ接続タイムアウト時間を 15 分に設定します。

<Switch> system-view

[Switch] line class vty

[Switch-line-class-vty] idle-timeout 15

関連コマンド

line

3.1.27 lock

Syntax

lock

デフォルト

設定なし

View

User view

定義済みユーザロール

network-admin

説明

lock コマンドは現在の user line をロックします。

許可されていないユーザが user line で操作を使用しないように防止します。

lock コマンドを実行した後、ロックされていない user line のパスワードを入力し、再度パスワードを入力します。

user line を解除する場合、Enter キーを押下し、正しいパスワードを入力します。

例

現在の user line をロックします。その後ロックを解除します。

<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>
```

3.1.28 lock reauthentication

Syntax

lock reauthentication

デフォルト

設定なし

View

全ての view

定義済みユーザロール

network-admin

説明

lock reauthentication コマンドは現在の user line をロックしてロック解除認証を有効にします。

このコマンドは現在の user line をロックします。user line のロックを解除するには、**Enter** を押して再認証にパスするためのログインパスワードを入力する必要があります。ログイン後にログインパスワードを変更した場合は、新しいパスワードを入力する必要があります。ログインパスワードが設定されていない場合は、**Enter** キーを押した後にシステムが user line のロックを解除します。

例

現在の user line をロックして、ロック解除認証を有効にします。

<Switch> lock reauthentication

```
Please press Enter to unlock the screen.
```

// user line がロックされています。ロックを解除するには、**Enter** キーを押してログインパスワードを入力します。

```
Password:
```

<Switch>

関連コマンド

lock-key

3.1.29 lock-key

Syntax

lock-key *key-string*

undo lock-key

デフォルト

設定なし

View

User line view

User line class view

定義済みユーザロール

network-admin

パラメータ

key-string: ショートカットキーを指定します。大文字、小文字を区別します。あるいは 0 ～127 までの ASCII コード値を指定できます。たとえば、**lock-key 1** を設定する場合、ショートカットキーは **Ctrl+A** です。**lock-key a** を設定する場合、ショートカットキーは **a** です。個々の文字の ASCII コード値については、標準 ASCII コード表を参照してください。

説明

lock-key コマンドは user line ロックキーを設定します。このショートカットキーを押すと、現在の user line がロックされ、認証のロック解除が有効になります。

undo lock-key コマンドはデフォルトに戻します。

ベストプラクティスとして、結合されたキーを User line ロックキーとして指定します。キーとして単一の文字を指定した場合、その文字は User line ロックキーとしてのみ機能します。コマンド、キーワード、あるいは文字を入力することはできません。

User line ロックキーを押すのは、**lock reauthentication** コマンドを実行するのと同じことです。

このコマンドはすぐに有効になります。

display current-configuration|include lock-key コマンドは、現在の User line ロックキーを表示します。

例

VTY line 0 の user line ロックキーを **Ctrl + A** に設定します。

<Switch> system-view

[Switch] line vty 0

[Switch-line-vty0] lock-key 1

[Switch-line-vty0] quit

設定を確認するには:

1) **Ctrl+A** を押します。

[Switch]

```
Please press Enter to unlock the screen.
```

2) **Enter** キーを押してログインパスワードを入力します。

```
Password:
```

[Switch]

関連コマンド

lock reauthentication

3.1.30 parity

Syntax

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

undo parity

デフォルト

none

View

User line view

定義済みユーザロール

network-admin

パラメータ

even: 偶数パリティチェックを実行します。

mark: 記号パリティチェックを実行します。

none: パリティチェックを実行しません。

odd: 奇数パリティチェックを実行します。

space: 空白のパリティチェックを実行します。

説明

parity コマンドはパリティチェックモードを指定します。

undo parity コマンドはデフォルトに戻します。

このコマンドは VTY line view でサポートしていません。

この設定は端末のパリティチェックと同一にしてください。

例

AUX line 0 で偶数パリティチェックを実行するように設定します。

<Switch> system-view

[Switch] line aux 0

[Switch-line-aux0] parity odd

3.1.31 protocol inbound

Syntax

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

undo protocol inbound

デフォルト

all

View

VTY line view

VTY line class view

定義済みユーザロール

network-admin

パラメータ

all: SSH、Telnet のプロトコルをサポートします。

ssh: SSH のプロトコルをサポートします。

telnet: Telnet のプロトコルをサポートします。

説明

protocol inbound コマンドはサポートするプロトコルを設定します。

undo protocol inbound コマンドはデフォルトに戻します。

network-admin あるいはレベル 15 のユーザロールが割り当てられたユーザのみコマンドを実行することができます。実行権限があったとしてもほかのユーザはコマンドを実行できません。

user line view で設定を変更した場合、現在のセッションに影響しません。次にログインしたときに適用されます。

SSH をサポートするため user line を設定する前に、user line の認証モードを scheme に設定してください。

VTY line view で、**protocol inbound** コマンドは **authentication-mode** コマンドと関連します。VTY line view で 2 つのコマンドのうち、1 つコマンドのみデフォルトでない認証モードである場合、もう一方のコマンドは VTY line class view の設定に関わらず、デフォルトの認証モードを使用します。

- VTY line view の 2 つのコマンドの設定がデフォルトである場合、VTY line view の認証モードを使用します。
- VTY line view の 2 つのコマンドの設定がデフォルトでない場合、VTY line view のデフォルトでない認証モードを使用します。

- VTY line view で 2 つのコマンドのうち、1 つコマンドのみデフォルトでない認証モードである場合、もう一方のコマンドは VTY line class view の設定に関わらず、デフォルトの認証モードを使用します。

例

user line VTY 0～4 で SSH のみを有効にするように設定します。

<Switch> system-view

[Switch] line vty 0 4

[Switch-line-vty0-4] authentication-mode scheme

[Switch-line-vty0-4] protocol inbound ssh

SSH を有効にし、VTY line class view で認証モードを scheme に設定します。user line VTY 0～VTY 4 ですべてのプロトコルを有効にし、user line で認証を無効にします。

<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

設定を確認します。

1) 装置に Telnet します。

<Client> telnet 192.168.1.241

```
Trying 192.168.1.241 ...
Press CTRL+K to abort
Connected to 192.168.1.241 ...

<Server>
```

認証なしでログインしました。

2) オンライン CLI ユーザの情報を表示します。

<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.
```

出力は、ユーザは VTY 0 を使用していることを示します。user line view の設定は適用されています。

関連コマンド

authentication-mode

3.1.32 restful http enable

Syntax

restful http enable

undo restful http enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

restful http enable コマンドは HTTP を介した RESTful アクセスを有効にします。

undo restful http enable コマンドは HTTP を介した RESTful アクセスを無効にします。

このコマンドは FIPS モードではサポートされません。

ユーザが HTTP ベースの RESTful API を使用して装置にアクセスするには、HTTP を介した RESTful アクセスを有効にする必要があります。

例

HTTP を介した RESTful アクセスを有効にします。

<Switch> system-view

[Switch] restful http enable

3.1.33 restful https enable

Syntax

restful https enable

undo restful https enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

restful https enable コマンドは HTTPS を介した RESTful アクセスを有効にします。

undo restful https enable コマンドは HTTPS を介した RESTful アクセスを無効にします。

ユーザが HTTPS ベースの RESTful API を介して装置にアクセスするには、HTTPS を介した RESTful アクセスを有効にする必要があります。

例

HTTPS を介した RESTful アクセスを有効にします。

<Switch> system-view

[Switch] restful https enable

3.1.34 screen-length

Syntax

screen-length *screen-length*

undo screen-length

デフォルト

24 行

View

User line view

User line class view

定義済みユーザロール

network-admin

パラメータ

screen-length: 画面上で一度に表示される行の最大数を指定します。設定範囲は 0～512 です。0 に設定した場合、出力画面のスクロールは停止しません。

説明

screen-length コマンドは画面上で一度に表示される行の最大数を設定します。

undo screen-length コマンドはデフォルトに戻します。

出力画面に表示される実際の行数は端末のモニタの仕様によって制限されます。

たとえば、画面上で一度に表示される行の最大数を 40 に設定した場合、装置はすぐに端末に 40 行を送信します。もし端末のモニタの仕様が 24 である場合、出力画面には最後の 24 行のみが表示されます。前の 16 行を表示する場合、PgUp キーを押下します。

停止したのち、出力を継続する場合、スペースキーを押下します。出力画面のスクロールの停止機能はデフォルトで有効です。

このコマンドは user line view および user line class view の両方でサポートしています。

- user line view の設定がデフォルトでないとき、user line view の設定が適用されます。
- user line view の設定がデフォルトで user line class view の設定がデフォルトでないとき、user line class view の設定が適用されます。

設定を変更した場合、すぐに現在のセッションに適用します。user line class view での設定は、設定が行われた後、ログインセッションで適用されます。

例

VTY line 0 で一度に表示される行の最大数を 30 行に設定します。

<Switch> system-view

[Switch] line vty 0

[Switch-line-vty0] screen-length 30

関連コマンド

screen-length disable

3.1.35 send

Syntax

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

View

User view

定義済みユーザロール

network-admin

パラメータ

all: すべての user line を指定します。

number1: user line の通し番号を指定します。設定範囲は 0～73 です。

aux: AUX line を指定します。

vty: VTY line を指定します。

number2: user line のタイプごとの番号を指定します。AUX line の設定範囲は 0～9 で、VTY の設定範囲は 0～63 です。

説明

send コマンドはオンラインログインユーザにメッセージを送信します。

ほかのオンラインユーザに影響を及ぼす操作を実行する前に、オンラインユーザに通知するために使用することができます。たとえば装置を再起動する場合などに使用します。

メッセージを終了する場合、Enter キーを押下します。メッセージをキャンセルし、user view に戻る場合、Ctrl+C キーを押下します。

例

VTY 1 の user に通知するため、メッセージを送信します。

<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
```

メッセージは以下の例のようにユーザの設定端末の画面に表示されます。

```
[Switch]


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

3.1.36 set authentication password

Syntax

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

undo set authentication password

デフォルト

AUX line class は **qx-admin** です。

AUX line/VTY line/VTY line class は設定なしです。

View

User line view

User line class view

定義済みユーザロール

network-admin

パラメータ

hash: 暗号テキストのパスワードを設定します。

simple: プレーンテキストのパスワードを設定します。

string: 大文字、小文字が区別されたパスワードを指定します。**simple** が指定された場合、設定範囲は 1～16 文字です。**hash** が指定された場合、設定範囲は 1～110 文字です。

説明

set authentication password コマンドはパスワード認証のパスワードを設定します。

undo set authentication password コマンドはパスワードを削除します。

セキュリティのため、保存されたパスワードは設定に関わらず常に暗号テキストで表示されます。

network-admin あるいはレベル 15 のユーザロールが割り当てられたユーザのみコマンドを実行することができます。実行権限があったとしてもほかのユーザはコマンドを実行できません。

このコマンドは user line view および user line class view の両方でサポートしています。

- user line view の設定がデフォルトでないとき、user line view の設定が適用されます。
- user line view の設定がデフォルトで user line class view の設定がデフォルトでないとき、user line class view の設定が適用されます。

パスワードを変更した場合、現在のセッションに影響しません。次にログインしたときに適用されます。

例

VTY line 0 でパスワード認証のパスワード hello を設定します。

<Switch> system-view

[Switch] line vty 0

[Switch-line-vty0] authentication-mode password

[Switch-line-vty0] set authentication password simple hello

関連コマンド

authentication-mode

🕮 **メモ：**

AUX line class view のデフォルトのパスワード **qx_admin** は、工場出荷時の初期パスワードです。セキュリティが損なわれないようパスワードを変更してください。

3.1.37 shell

Syntax

shell

undo shell

デフォルト

有効

View

User line view

User line class view

定義済みユーザロール

network-admin

説明

shell コマンドは user line の端末サービスを有効にします。

undo shell コマンドは user line の端末サービスを無効にします。

AUX line view あるいは AUX line class view でコマンドは **undo shell** サポートしていません。

現在使用している user line の端末サービスを無効にすることはできません。

装置が Telnet あるいは SSH サーバとして動作するとき、**undo shell** コマンドを設定することはできません。

user line class view で **undo shell** コマンドが設定された場合、class の user line の view で **shell** コマンドを設定することはできません。

端末サービスが有効であるとき、user line は装置へのログインに使用されます。装置がリダイレクトサーバとして稼働している場合、user line はリダイレクトサービスに使用されます。user line は 1 回につき、1 つの処理のみ行うことができます。

例

user line からユーザが装置にログインできないようにするため、VTY line 0～VTY line 4 の端末サービスを無効にします。

<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]
```

3.1.38 speed

Syntax

speed *speed-value*

undo speed

デフォルト

9600 bps

View

User line view

定義済みユーザロール

network-admin

パラメータ

speed-value: 通信速度を bps で指定します。サポートされる通信速度は設定環境によって異なります。非同期シリアルインタフェースの通信速度を以下に示します。

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

説明

speed コマンドは user line の通信速度（ボーレートと呼ばれます）を設定します。

undo speed コマンドはデフォルトに戻します。

このコマンドは VTY line view でサポートしていません。

端末と装置で設定を同一にしてください。

例

#AUX line 0 で通信速度を 19200 bps に設定します。

<Switch> system-view

[Switch] line aux 0

[Switch-line-aux0] speed 19200

3.1.39 stopbits

Syntax

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

undo stopbits

デフォルト

1

View

User line view

定義済みユーザロール

network-admin

パラメータ

1: ストップビットを 1 に設定します。

1.5: ストップビットを 1.5 に設定します。装置はストップビット 1.5 をサポートしていません。1.5 が設定された場合、ストップビットは 2 が使用されます。

2: ストップビットを 2 に設定します。

説明

stopbits コマンドは文字列のストップビットを設定します。

undo stopbits コマンドはデフォルトに戻します。

このコマンドは VTY line view でサポートしていません。

端末と装置で設定を同一にしてください。

例

#AUX line 0 のストップビットを 1 に設定します。

<Switch> system-view

[Switch] line aux 0

[Switch-line-aux0] stopbits 1

3.1.40 telnet

Syntax

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

View

User view

定義済みユーザロール

network-admin

パラメータ

remote-host: リモートホストの IPv4 アドレスあるいはホスト名を指定します。ホスト名は大文字、小文字が区別されません。設定範囲は 1～253 文字です。ホスト名の変数は英字、数字、ハイフン(－)、アンダーライン(_)、ドット(.)が含まれます。

service-port: リモートホストの Telnet サービスの TCP ホスト番号を指定します。設定範囲は 0～65535 です。デフォルトは 23 です。

source: Telnet パケットを送信する送信元 IPv4 アドレスあるいは送信元インタフェースを指定します。指定しない場合、ルートの出力インタフェースのプライマリ IPv4 アドレスを使用します。

interface *interface-type interface-number*: 送信元インタフェースを指定します。インタフェースのプライマリ IPv4 アドレスは Telnet パケットを送信する送信元 IPv4 アドレスとして使用されます。

ip *ip-address*: Telnet パケットを送信する送信元 IPv4 アドレスを指定します。

dscp *dscp-value*: パケットの優先度を指定するため、Telnet パケットの DSCP 値を指定します。設定範囲は 0～63 です。デフォルトは 48 です。

説明

telnet コマンドは IPv4 ネットワークのホストに Telnet します。

現在の Telnet 接続を終了するには、Ctrl+K キーを押下するか **quit** コマンドを実行します。

このコマンドで指定された送信元 IPv4 アドレスあるいは送信元インタフェースは現在の Telnet 接続にのみ適用されます。

例

Telnet パケットを送信する送信元 IP アドレス 1.1.1.1 を使用し、ホスト 1.1.1.2 に Telnet します。

<Switch> telnet 1.1.1.2 source ip 1.1.1.1

関連コマンド

telnet client source

3.1.41 telnet client source

Syntax

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

undo telnet client source

デフォルト

Telnet パケットを送信するために指定された送信元 IPv4 アドレスあるいは送信元インタフェースはありません。送信元 IPv4 アドレスは出力インタフェースのプライマリ IPv4 アドレスです。

View

System view

定義済みユーザロール

network-admin

パラメータ

interface *interface-type interface-number*: 送信元インタフェースを指定します。インタフェースのプライマリ IPv4 アドレスは Telnet パケットを送信する送信元 IPv4 アドレスとして使用されます。

ip *ip-address*: 送信元 IPv4 アドレスを指定します。

説明

telnet client source コマンドは、装置が Telnet クライアントとして動作するとき、Telnet パケットを送信する送信元 IPv4 アドレスあるいは送信元インタフェースを指定します。

undo telnet client source コマンドは設定を削除します。

このコマンドで指定された送信元 IPv4 アドレスあるいは送信元インタフェースはすべての Telnet 接続に適用されます。ユーザが **telnet** コマンドを実行して送信元 IPv4 アドレスあるいは送信元インタフェースを指定した場合、ユーザが設定した送信元 IPv4 アドレスあるいは送信元インタフェースが適用されます。

例

装置が Telnet クライアントとして動作するとき、Telnet パケットを送信する送信元 IPv4 アドレスを 1.1.1.1 に設定します。

<Switch> system-view

[Switch] telnet client source ip 1.1.1.1

関連コマンド

display telnet client configuration

3.1.42 telnet ipv6

Syntax

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

View

User view

定義済みユーザロール

network-admin

パラメータ

remote-host: リモートホストの IP アドレスあるいはホスト名を指定します。ホスト名は大文字、小文字が区別されません。設定範囲は 1～253 文字です。ホスト名の変数は英字、数字、ハイフン(－)、アンダーライン(__)、ドット(.)が含まれます。

-i *interface-type interface-number*: Telnet パケットを送信する出力インタフェースを指定します。宛先アドレスがリンクローカルアドレスであるとき、このパラメータが必要となります。サーバアドレスがグローバルユニキャストアドレスである場合、パラメータを指定することはできません。

port-number: リモートホストの Telnet サービスの TCP ホスト番号を指定します。設定範囲は 0～65535 です。デフォルトは 23 です。

dscp *dscp-value*: パケットの優先度を指定するため、Telnet パケットを送信する IPv6 パケットの DSCP 値を指定します。設定範囲は 0～63 です。デフォルトは 48 です。

説明

telnet ipv6 コマンドは IPv6 ネットワークのホストに Telnet します。

現在の Telnet 接続を終了するには、Ctrl+K キーを押下するか **quit** コマンドを実行します。

例

ホスト 5000::1 に Telnet します。

<Switch> telnet ipv6 5000::1

3.1.43 telnet server acl

Syntax

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

undo telnet server acl

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

mac: L2 ACL を指定します。標準 ACL、拡張 ACL を指定する場合、**mac** パラメータを指定しないでください。

acl-number: 以下の番号の ACL を指定します。

- 2000～2999：標準 ACL です。
- 3000～3999：拡張 ACL です。
- 4000～4999：L2 ACL です。**mac** パラメータが必要です。

説明

telnet server acl コマンドは Telnet ログインにフィルタリングを行います。

undo telnet server acl コマンドはデフォルトに戻します。

ACL が作成されていなくても、このコマンドで ACL を指定することができますが、ACL が作成されたのち、フィルタリングが適用されます。ACL の詳細はオペレーションマニュアルのセクション 8 *ACL and QoS*”*ACL*”を参照してください。

コマンドを複数実行した場合、最後に行った設定が適用されます。

このコマンドは既存の Telnet 接続には適用されません。

例

IP アドレス 1.1.1.1 のユーザのみ装置に Telnet を行うことができるようにフィルタリングを行います。

<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

3.1.44 telnet server acl-deny-log enable

Syntax

telnet server acl-deny-log enable

undo telnet server acl-deny-log enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

telnet server acl-deny-log enable コマンドは Telnet ログイン制御 ACL によって拒否された Telnet ログイン試行のロギングを有効にします。

undo telnet server acl-deny-log enable コマンドは Telnet ログイン制御 ACL によって拒否された Telnet ログイン試行のロギングを無効にします。

Telnet ログイン制御 ACL によって許可されたクライアントだけが装置に Telnet 接続できます。このロギング機能は、Telnet ログイン制御 ACL によって拒否された Telnet ログイン試行のログメッセージを生成します。

ログメッセージの出力については、オペレーションマニュアルのセクション 11 *システム管理* "*Information Center*"を参照してください。Telnet ログイン制御 ACL の設定については、**telnet server acl** または **telnet server ipv6 acl** コマンドを参照してください。

例

Telnet ログイン制御 ACL によって拒否された Telnet ログイン試行のロギングを有効にします。

<Switch> system-view

[Switch] telnet server acl-deny-log enable

関連コマンド

- **telnet server acl**
- **telnet server ipv6 acl**

3.1.45 telnet server dscp

Syntax

telnet server dscp *dscp-value*

undo telnet server dscp

デフォルト

48

View

System view

定義済みユーザロール

network-admin

パラメータ

dscp-value: DSCP 値を指定します。設定範囲は 0～63 です。

説明

telnet server dscp コマンドは Telnet サーバで Telnet パケットを送信する IPv4 の DSCP 値を設定します。

undo telnet server dscp コマンドはデフォルトに戻します。

DSCP 値は IPv4 パケットの ToS フィールドで送信されます。パケットを転送する優先度を示します。

例

Telnet サーバで Telnet パケットを送信する IPv4 の DSCP 値を 30 に設定します。

<Switch> system-view

[Switch] telnet server dscp 30

3.1.46 telnet server enable

Syntax

telnet server enable

undo telnet server enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

telnet server enable コマンドは Telnet サーバ機能を有効にします。

undo telnet server enable コマンドは Telnet サーバ機能を無効にします。

管理者は Telnet サーバ機能が有効であるときのみ装置に Telnet を行うことができます。

例

Telnet サーバ機能を有効にします。

<Switch> system-view

[Switch] telnet server enable

3.1.47 telnet server ipv6 acl

Syntax

telnet server ipv6 acl [**ipv6** | **mac**] *acl-number*

undo telnet server ipv6 acl

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

ipv6: IPv6 ACL を指定します。

mac: L2 ACL を指定します。標準 IPv6 ACL、拡張 IPv6 ACL を指定する場合、**mac** パラメータを指定しないでください。

acl-number: 以下の番号の IPv6 ACL を指定します。

- 2000～2999：標準 IPv6 ACL です。**ipv6** パラメータが必要です。
- 3000～3999：拡張 IPv6 ACL です。**ipv6** パラメータが必要です。
- 4000～4999：L2 ACL です。**mac** パラメータが必要です。

説明

telnet server ipv6 acl コマンドは IPv6 Telnet ログインに IPv6 ACL フィルタリングを行います。

undo telnet server ipv6 acl コマンドはデフォルトに戻します。

ACL が作成されていなくても、このコマンドで ACL を指定することができますが、ACL が作成されたのち、フィルタリングが適用されます。ACL の詳細はオペレーションマニュアルのセクション 8 *ACL and QoS*”*ACL*”を参照してください。

コマンドを複数実行した場合、最後に行った設定が適用されます。

このコマンドは既存の Telnet 接続には適用されません。

例

IPv6 アドレス 2000::1 のユーザのみ装置に Telnet を行うことができるようにフィルタリングを行います。

<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

3.1.48 telnet server ipv6 dscp

Syntax

telnet server ipv6 dscp *dscp-value*

undo telnet server ipv6 dscp

デフォルト

48

View

System view

定義済みユーザロール

network-admin

パラメータ

dscp-value: DSCP 値を指定します。設定範囲は 0～63 です。

説明

telnet server ipv6 dscp コマンドは Telnet クライアントに Telnet パケットを送信する IPv6 の DSCP 値を設定します。

undo telnet server ipv6 dscp コマンドはデフォルトに戻します。

DSCP 値は IPv6 パケットの ToS フィールドで送信されます。パケットを転送する優先度を示します。

例

Telnet サーバで Telnet パケットを送信する IPv6 の DSCP 値を 30 に設定します。

<Switch> system-view

[Switch] telnet server ipv6 dscp 30

3.1.49 terminal type

Syntax

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

undo terminal type

デフォルト

ANSI

View

User line view

User line class view

定義済みユーザロール

network-admin

パラメータ

ansi: 端末の表示タイプを ANSI に指定します。

vt100: 端末の表示タイプを VT100 に指定します。

説明

terminal type コマンドは端末の表示タイプを指定します。

undo terminal type コマンドはデフォルトに戻します。

装置は端末の表示タイプ ANSI と VT100 をサポートします。NEC は装置と端末の両方で表示タイプを VT100 に設定することを推奨します。

装置あるいは端末のどちらかが ANSI を使用している場合、コマンドラインが 80 文字を越えたときにカーソル位置のエラーなどの表示に関する問題が発生する可能性があります。

このコマンドは user line view および user line class view の両方でサポートしています。user line view と user line class view のどちらかの view でデフォルトでない設定がある場合、デフォルトでない設定は、もう一方のデフォルト設定よりも優先されます。user line view のデフォルトでない設定は user line class view のデフォルトでない設定よりも優先されます。

端末の表示タイプを変更した場合、現在のセッションに影響しません。次にログインしたときに適用されます。

例

端末の表示タイプを VT100 に設定します。

<Switch> system-view

[Switch] line vty 0

[Switch-line-vty0] terminal type vt100

3.1.50 user-interface

Syntax

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

View

System view

定義済みユーザロール

network-admin

パラメータ

first-number1: 最初の user line の通し番号を指定します。設定範囲は 0～73 です。

last-number1: 最後の user line の通し番号を指定します。*first-number1* よりも小さくすることはできません。

aux: AUX line を指定します。

vty: VTY line を指定します。

first-number2: 最初の user line のタイプごとの番号を指定します。AUX line の設定範囲は 0～9 で、VTY line の設定範囲は 0～63 です。

last-number2: 最後の user line のタイプごとの番号を指定します。VTY line の設定範囲は 1～9 です。*first-number2* よりも小さくすることはできません。

説明

user-interface コマンドは 1 つ以上の user line view に移行します。

このコマンドは古いソフトウェアバージョンで使用していたユーザのためにサポートされているコマンドです。古いソフトウェアバージョンで動作するコマンドです。**line** コマンドと同一機能です。通常は **line** コマンドを使用してください。

1 つの user line を設定する場合、**user-interface** コマンドを使用して user line view に移行します。

複数の user line で同一の設定を行う場合、**user-interface** コマンドを使用して複数の user line view に移行します。

例

AUX line 0 の view に移行します。

<Switch> system-view

[Switch] user-interface aux 0

[Switch-line-aux0]

VTY 0～VTY 4 の view に移行します。

<Switch> system-view

[Switch] user-interface vty 0 4

[Switch-line-vty0-4]

関連コマンド

user-interface class

3.1.51 user-interface class

Syntax

user-interface class { **aux** | **vty** }

View

System view

定義済みユーザロール

network-admin

パラメータ

aux: AUX line class view を指定します。

vty: VTY line class view を指定します。

説明

user-interface class コマンドは user line class view に移行します。

このコマンドは古いソフトウェアバージョンで使用していたユーザのためにサポートされているコマンドです。古いソフトウェアバージョンで動作するコマンドです。**line class** コマンドと同一機能です。通常は **line class** コマンドを使用してください。

line class のすべての user line で設定を同一にするために、user line class view に移行します。

user line class view では以下のコマンドを実行することができます。

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

いくつかのログインコマンドは user line view および user line class view の両方でサポートしています。

- user line view の設定は user line で適用されます。user line class view の設定は class のすべての user line で適用されます。
- user line view と user line class view のどちらかの view でデフォルトでない設定がある場合、デフォルトでない設定は、もう一方のデフォルト設定よりも優先されます。user line view のデフォルトでない設定は user line class view のデフォルトでない設定よりも優先されます。
- user line view の設定はすぐに適用され、オンラインユーザに影響します。user line class view の設定は設定が完了したのちにログインしたユーザのみ適用されます。user line class view の設定はオンラインユーザに影響しません。

例

VTY line class view でユーザ接続タイムアウト時間を 15 分に設定します。

<Switch> system-view

[Switch] user-interface class vty

[Switch-line-class-vty] idle-timeout 15

関連コマンド

user-interface

3.1.52 user-role

Syntax

user-role *role-name*

undo user-role [*role-name*]

デフォルト

コンソールユーザのユーザロールは network-admin です。

ほかの user line のユーザロールは network-operator です。

View

User line view

User line class view

定義済みユーザロール

network-admin

パラメータ

role-name: ユーザロール名を指定します。大文字、小文字を区別します。範囲は 1～63 です。ユーザロールはユーザ定義あるいは定義済みのユーザロールがあります。定義済みは network-admin、network-operator、level-0～level-15 があります。**undo user-role** コマンドで *role-name* を指定しない場合、デフォルトのユーザロールに戻します。

説明

user-role コマンドは user line でログインしたユーザがユーザロールを取得できるように user line にユーザロールを割り当てます。

undo user-role コマンドはユーザロールを削除あるいはデフォルトに戻します。

network-admin あるいはレベル 15 のユーザロールが割り当てられたユーザのみコマンドを実行することができます。実行権限があったとしてもほかのユーザはコマンドを実行できません。

このコマンドは user line view および user line class view の両方でサポートしています。

- user line view の設定がデフォルトでないとき、user line view の設定が適用されます。
- user line view の設定がデフォルトで user line class view の設定がデフォルトでないとき、user line class view の設定が適用されます。

設定を変更した場合、現在のセッションに影響しません。次にログインしたときに適用されます。

user line に 64 のユーザロールを割り当てることができます。user line からログインしたユーザはすべてのユーザロールを取得します。

ユーザロールの詳細はオペレーションマニュアルのセクション 1 *はじめに*”*RBAC*”を参照してください。

例

AUX line 0 にユーザロール network-admin を割り当てます。

<Switch> system-view

[Switch] line aux 0

[Switch-line-aux0] user-role network-admin

3.1.53 web idle-timeout

Syntax

web idle-timeout *idle-time*

undo web idle-timeout

デフォルト

10 分

View

System view

定義済みユーザロール

network-admin

パラメータ

idle-time: タイムアウトタイマを指定します。設定範囲は 1～999 分です。

説明

web idle-timeout コマンドは Web ユーザの接続のタイムアウトタイマを設定します。

undo web idle-timeout コマンドはデフォルトに戻します。

許可されていないアクセスを防ぐため、アイドルタイムアウト時間内にマウスあるいはキーボードの動作がない場合、システムは自動でユーザの接続を切断します。

設定を変更した場合、現在の Web 接続に影響しません。次に Web 接続したときに適用されます。

例

Web ユーザの接続のタイムアウトタイマを 100 分に設定します。

<Switch> system-view

[Switch] web idle-timeout 100

目次

このセクションのページは **1-x-x** です。

4 章 FTP 4-1
4.1 FTP サーバ設定コマンド 4-1
4.1.1 display ftp-server 4-1
4.1.2 display ftp-user 4-2
4.1.3 free ftp user 4-3
4.1.4 free ftp user-ip 4-3
4.1.5 free ftp user-ip ipv6 4-4
4.1.6 ftp server acl 4-5
4.1.7 ftp server acl-deny-log enable 4-6
4.1.8 ftp server dscp 4-7
4.1.9 ftp server enable 4-7
4.1.10 ftp server ipv6 dscp 4-8
4.1.11 ftp timeout 4-9
4.2 FTP クライアント設定コマンド 4-10
4.2.1 ascii 4-10
4.2.2 binary 4-11
4.2.3 bye 4-11
4.2.4 cd 4-12
4.2.5 cdup 4-13
4.2.6 close 4-14
4.2.7 debug 4-15
4.2.8 delete 4-16
4.2.9 dir 4-16
4.2.10 disconnect 4-18
4.2.11 display ftp client source 4-18
4.2.12 ftp 4-19
4.2.13 ftp client ipv6 source 4-20
4.2.14 ftp client source 4-21
4.2.15 ftp ipv6 4-22
4.2.16 get 4-24
4.2.17 help 4-25
4.2.18 lcd 4-26
4.2.19 ls 4-27
4.2.20 mkdir 4-28
4.2.21 newer 4-29
4.2.22 open 4-30

4.2.23 passive 4-31
4.2.24 put 4-31
4.2.25 pwd 4-33
4.2.26 quit 4-33
4.2.27 rhelp 4-34
4.2.28 rmdir 4-36
4.2.29 user 4-37
4.2.30 verbose 4-38
4.2.31 ? 4-39

4章 FTP

4.1 FTPサーバ設定コマンド

4.1.1 display ftp-server

Syntax

display ftp-server

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display ftp-server コマンドは FTP サーバの設定と情報を表示します。

例

FTP サーバの設定と情報を表示します。

<Switch> display ftp-server

```
FTP server is running.
User count:                    1
Idle-timeout timer (in minutes):  30
```

表 4-1 コマンド出力

フィールド	説明
User count	現在ログインしているユーザ数です。
Idle-timeout timer (in minutes)	FTPサーバとクライアント間で一定期間、パケットの交換がない場合、FTP接続が切断されます。

関連コマンド

- **ftp server enable**
- **ftp timeout**

4.1.2 display ftp-user

Syntax

display ftp-user

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display ftp-user コマンドは FTP ログインユーザに関する詳細情報を表示します。

例

FTP ログインユーザに関する詳細情報を表示します。

<Switch> display ftp-user

```
UserName     HostIP           Port     HomeDir
root         192.168.20.184    46539    flash:
```

文字数が超過している場合、フィールドの値は次の行に表示されます。改行される場合のフィールドの値の制限を示します。

- **UserName**—10 文字
- **HostIP**—15 文字
- **HomeDir**—37 文字

<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
```

表 4-2 コマンド出力

フィールド	説明
UserName	ユーザ名です。
HostIP	ユーザのIPアドレスです。

フィールド	説明
Port	ユーザのポート番号です。
HomeDir	ユーザの許可ディレクトリです。

4.1.3 free ftp user

Syntax

free ftp user *username*

View

User view

定義済みユーザロール

network-admin

パラメータ

username: ユーザ名を指定します。FTP ユーザの情報を表示する場合、**display ftp-user** コマンドを使用します。

説明

free ftp user コマンドは指定したアカウントにより確立された FTP 接続を手動で切断します。

例

ユーザ ftpuser により確立された FTP 接続を手動で切断します。

<Switch> free ftp user ftpuser

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

4.1.4 free ftp user-ip

Syntax

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

View

User view

定義済みユーザロール

network-admin

パラメータ

ip-address: FTP 接続の送信元 IP アドレスです。FTP 接続の送信元 IP アドレスを表示する場合、**display ftp-user** コマンドを使用します。

port *port*: FTP 接続の送信元ポート番号を指定します。FTP 接続の送信元ポート番号を表示する場合、**display ftp-user** コマンドを使用します。

説明

free ftp user-ip コマンドは指定した IPv4 アドレスにより確立された FTP 接続を手動で切断します。

例

IPv4 アドレス 192.168.20.184 により確立された FTP 接続を手動で切断します。

<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

Syntax

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

View

User view

定義済みユーザロール

network-admin

パラメータ

ipv6-address: FTP 接続の送信元 IPv6 アドレスを指定します。FTP 接続の送信元 IPv6 アドレスを表示する場合、**display ftp-user** コマンドを使用します。

port *port*: FTP 接続の送信元ポート番号を指定します。FTP 接続の送信元ポート番号を表示する場合、**display ftp-user** コマンドを使用します。

説明

free ftp user-ip ipv6 コマンドは指定した IPv6 アドレスにより確立された FTP 接続を手動で切断します。

例

IPv6 アドレス 2000::154 により確立された FTP 接続を手動で切断します。

<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

Syntax

ftp server acl { *ipv4-acl-number* | **ipv6** *ipv6-acl-number* }

undo ftp server acl [**ipv6**]

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

ipv4-acl-number: IPv4 ACL 番号を指定します。設定範囲は 2000～3999 です。

ipv6 *ipv6-acl-number*: IPv6 ACL 番号を指定します。設定範囲は 2000～3999 です。

説明

ftp server acl コマンドは FTP サーバへの FTP クライアントのアクセスを制御します。

undo ftp server acl コマンドはデフォルトに戻します。

ACL により、FTP サーバは特定の FTP クライアントからの FTP リクエストのみを許可することができます。

この設定は FTP 接続が確立されたときのみ適用されます。既存の FTP 接続は影響がありません。

複数回コマンドを実行した場合、最後に指定した設定が適用されます。

例

FTP サーバへのアクセスが FTP クライアント 1.1.1.1 のみであるように ACL 2001 を指定します。

<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 acl-deny-log enable

Syntax

ftp server acl-deny-log enable

undo ftp server acl-deny-log enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

ftp server acl-deny-log enable コマンドは FTP ログイン制御 ACL によって拒否される FTP ログイン試行のロギングを有効にします。

undo ftp server acl-deny-log enable コマンドは FTP ログイン制御 ACL によって拒否された FTP ログイン試行のロギングを無効にします。

FTP ログイン制御 ACL によって許可されたクライアントだけが、FTP を使用して装置にアクセスできます。

このロギング機能は、FTP ログイン制御 ACL によって拒否された FTP ログイン試行のログメッセージを生成します。

ログメッセージの出力については、 セクション 11 *システム管理 オペレーションマニュアルの"Information Center"*を参照してください。

FTP ログイン制御 ACL の設定については、**ftp server acl** コマンドを参照してください

例

FTP ログイン制御 ACL によって拒否された、FTP ログイン試行のロギングを有効にします。

<Switch> system-view

[Switch] FTP server acl-deny-log enable

関連コマンド

ftp server acl

4.1.8 ftp server dscp

Syntax

ftp server dscp *dscp-value*

undo ftp server dscp

デフォルト

0

View

System view

定義済みユーザロール

network-admin

パラメータ

dscp-value: DSCP 値を指定します。設定範囲は 0～63 です。

説明

ftp server dscp コマンドは FTP クライアントに送信する IPv4 パケットの DSCP 値を指定します。

undo ftp server dscp コマンドはデフォルトに戻します。

DSCP 値は、IP パケットの ToS フィールドによって送信されます。パケットを転送する優先度を示します。

例

FTP サーバの送信 IPv4 パケットの DSCP 値を 30 に設定します。

<Switch> system-view

[Switch] ftp server dscp 30

4.1.9 ftp server enable

Syntax

ftp server enable

undo ftp server enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

ftp server enable コマンドは FTP サーバを有効にします。

undo ftp server enable コマンドは FTP サーバを無効にします。

例

FTP サーバを有効にします。

<Switch> system-view

[Switch] ftp server enable

4.1.10 ftp server ipv6 dscp

Syntax

ftp server ipv6 dscp *dscp-value*

undo ftp server ipv6 dscp

デフォルト

0

View

System view

定義済みユーザロール

network-admin

パラメータ

dscp-value: DSCP 値を指定します。設定範囲は 0～63 です。

説明

ftp server ipv6 dscp コマンドは FTP クライアントに送信する IPv6 パケットの DSCP 値を指定します。

undo ftp server ipv6 dscp コマンドはデフォルトに戻します。

DSCP 値は、IPv6 パケットの ToS フィールドによって送信されます。パケットを転送する優先度を示します。

例

FTP サーバの送信 IPv6 パケットの DSCP 値を 30 に設定します。

<Switch> system-view

[Switch] ftp server ipv6 dscp 30

4.1.11 ftp timeout

Syntax

ftp timeout *minute*

undo ftp timeout

デフォルト

30 分

View

System view

定義済みユーザロール

network-admin

パラメータ

minute: アイドルタイムアウトの時間です。設定範囲は 1～35791 分です。

説明

ftp timeout コマンドは FTP 接続のアイドルタイムアウトを設定します。

undo ftp timeout コマンドはデフォルトに戻します。

FTP 接続のアイドルタイムアウト内にパケットの送信が行われていない場合、FTP サーバはリソースを確保するために接続を切断します。

例

アイドルタイムアウトを 36 分に設定します。

<Switch> system-view

[Switch] ftp timeout 36

4.2 FTPクライアント設定コマンド

FTP クライアント設定コマンドを実行する前、FTP サーバでのユーザの許可設定が適用されていることを確認してください。許可設定は、作業ディレクトリ下のファイルの参照、ファイルの読み込み、ダウンロード、アップロード、ファイルのリネーム、ファイルの削除、ディレクトリの作成があります。

この章の FTP クライアントのコマンドは、装置によってサポートされていますが、正常に動作するかどうかは FTP サーバに依存します。

このセクションの例の出力例は FTP サーバの種類によって異なる場合があります。

4.2.1 ascii

Syntax

ascii

デフォルト

バイナリモード

View

FTP client view

定義済みユーザロール

network-admin

説明

ascii コマンドはファイルの転送モードを ASCII モードに設定します。

- **バイナリモード**－非テキストファイル（プログラムファイルや絵）を転送します。
- **ASCII モード**－テキストファイルを転送します。

FTP サーバにログイン後のみコマンドを設定することができます。

装置が FTP サーバとして動作するとき、転送モードは FTP クライアントによって決定します。装置が FTP クライアントとして動作するとき、転送モードを設定することができます。

例

転送モードを ASCII モードに設定します。

ftp> ascii

```
200 TYPE is now ASCII
```

関連コマンド

binary

4.2.2 binary

Syntax

binary

デフォルト

バイナリモード

View

FTP client view

定義済みユーザロール

network-admin

説明

binary コマンドはファイルの転送モードをバイナリモードに設定します。このモードはフローモードと呼ばれます。

ascii コマンドはファイルの転送モードを ASCII モードに設定します。

- **バイナリモード**－非テキストファイル（プログラムファイルや絵）を転送します。
- **ASCII モード**－テキストファイルを転送します。

FTP サーバにログイン後のみコマンドを設定することができます。

装置が FTP サーバとして動作するとき、転送モードは FTP クライアントによって決定します。装置が FTP クライアントとして動作するとき、転送モードを設定することができます。

例

転送モードをバイナリモードに設定します。

ftp> binary

```
200 TYPE is now 8-bit binary
```

関連コマンド

ascii

4.2.3 bye

Syntax

bye

View

FTP client view

定義済みユーザロール

network-admin

説明

bye コマンドは FTP サーバの接続を終了し、user view に戻ります。

装置とリモート FTP サーバ間で接続が確立していない場合、user view に戻ります。

例

FTP サーバの接続を終了し、user view に戻ります。

ftp> bye

```
221-Goodbye. You uploaded 2 and downloaded 2 kbytes.
221 Logout.
<Switch>
```

関連コマンド

quit

4.2.4 cd

Syntax

cd { *directory* | **..** | */* }

View

FTP client view

定義済みユーザロール

network-admin

パラメータ

directory: [*drive*:][*/*]*path* の形式のターゲットディレクトリ名を指定します。ここでは記憶媒体の名前を示します。通常はフラッシュあるいは CF です。ターゲットディレクトリが存在しない場合、**cd** コマンドは現在の作業ディレクトリを変更しません。ドライブ情報がない場合、現在のディレクトリのフォルダあるいはサブフォルダを示します。*drive* と *path* の引数についての詳細は、オペレーションマニュアルのセクション 1 *はじめに* “*FTP*” を参照してください。

..: 上位のディレクトリに戻ります。**cd ..**コマンドは **cdup** コマンドを実行するのと同一です。現在の作業ディレクトリが FTP ルートディレクトリである場合、**cd ..**はルートディレクトリに戻ります。

/: FTP ルートディレクトリに戻ります。

説明

cd コマンドは FTP サーバの現在の作業ディレクトリを別のディレクトリに変更します。

FTP サーバにログインした後のみ実行できます。

アクセスできるディレクトリは FTP サーバによって許可されている必要があります。

例

作業ディレクトリを現在のディレクトリのサブディレクトリ logfile に変更します。

ftp> cd logfile

```
250 OK. Current directory is /logfile
```

作業ディレクトリを FTP ルートディレクトリのサブディレクトリフォルダに変更します。

ftp> cd /folder

```
250 OK. Current directory is /folder
```

作業ディレクトリを現在のディレクトリの上位ディレクトリに変更します。

ftp> cd ..

```
250 OK. Current directory is /
```

作業ディレクトリを FTP ルートディレクトリに変更します。

ftp> cd /

```
250 OK. Current directory is /
```

関連コマンド

- **cdup**
- **pwd**

4.2.5 cdup

Syntax

cdup

View

FTP client view

定義済みユーザロール

network-admin

説明

cdup コマンドは FTP サーバの上位ディレクトリに移行します。

FTP サーバにログインした後のみ実行できます。

現在のディレクトリが FTP ルートディレクトリである場合、このコマンドは作業ディレクトリを変更しません。

例

作業ディレクトリを上位ディレクトリに移行します。

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
```

関連コマンド

- **cd**
- **pwd**

4.2.6 close

Syntax

close

View

FTP client view

定義済みユーザロール

network-admin

説明

close コマンドは FTP client view から移動することなく、FTP サーバの接続を終了します。

FTP サーバにログインした後のみ実行できます。

例

FTP client view から移動することなく、FTP サーバの接続を終了します。

ftp> close

```
221-Goodbye. You uploaded 0 and downloaded 0 kbytes.
221 Logout.
ftp>
```

関連コマンド

disconnect

4.2.7 debug

Syntax

debug

デフォルト

無効

View

FTP client view

定義済みユーザロール

network-admin

説明

debug コマンドは FTP クライアントのデバッグを無効あるいは有効に設定します。

FTP クライアントのデバッグが有効であるとき、このコマンドを使用して FTP クライアントのデバッグを無効にします。

FTP クライアントのデバッグが無効であるとき、このコマンドを使用して FTP クライアントのデバッグを有効にします。

例

FTP クライアントのデバッグを有効にし、その後、無効にします。

ftp> debug

```
Debugging on (debug=1).
```

ftp> debug

```
Debugging off (debug=0).
```

4.2.8 delete

Syntax

delete *remotefile*

View

FTP client view

定義済みユーザロール

network-admin

パラメータ

remotefile: FTP サーバのファイル名を指定します。

説明

delete コマンドは FTP サーバのファイルを完全に削除します。

FTP サーバにログインした後のみ実行できます。

この動作を実行するため、FTP サーバの削除権限が必要です。

例

ファイル b.txt を削除します。

ftp> delete b.txt

```
250 Deleted b.txt
```

4.2.9 dir

Syntax

dir [*remotefile* [*localfile*]]

View

FTP client view

定義済みユーザロール

network-admin

パラメータ

remotefile: FTP サーバのファイルあるいはディレクトリを指定します。

localfile: 表示された情報が保存されるローカルファイルの名前を指定します。

説明

dir コマンドは FTP サーバ上の、現在のディレクトリにあるファイルおよびサブディレクトリに関する詳細情報を表示します。

dir *remotefile* コマンドは FTP サーバのファイルあるいはディレクトリに関する詳細情報を表示します。

dir *remotefile localfile* コマンドはリモート FTP サーバ上の指定したファイルまたはディレクトリに関する詳細情報を表示し、表示された情報を引数 *localfile* で指定したローカルファイルに保存します。

FTP サーバにログインした後のみ実行できます。

FTP client view において、**dir** コマンドは **ls** コマンドと同一です。

例

FTP サーバの現在のディレクトリのファイル、サブディレクトリの詳細情報を表示します。

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
```

ファイル a.txt の詳細情報を s.txt に保存します。

ftp> dir a.txt s.txt

```
output to local-file: s.txt ? [Y/N]y
150 Connecting to port 50203
226-Glob: a.txt
```

ファイル s.txt の内容を表示します。

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
```

関連コマンド

ls

4.2.10 disconnect

Syntax

disconnect

View

FTP client view

定義済みユーザロール

network-admin

説明

disconnect コマンドは FTP client view から移動することなく、FTP サーバへの接続を終了します。

FTP サーバにログインした後のみ実行できます。

例

FTP client view から移動することなく、FTP サーバへの接続を終了します。

ftp> disconnect

```
221-Goodbye. You uploaded 0 and downloaded 0 kbytes.
221 Logout.
ftp>
```

関連コマンド

close

4.2.11 display ftp client source

Syntax

display ftp client source

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display ftp client source コマンドは FTP クライアントの設定の送信元アドレスを表示します。

例

FTP クライアントの設定の送信元アドレスを表示します。

<Switch> display ftp client source

```
The source IP address of the FTP client is 1.1.1.1.
```

4.2.12 ftp

Syntax

ftp [*ftp-server* [*service-port*] [**dscp** *dscp-value* | **source** { **interface** *interface-type interface-number* | **ip** *source-ip-address* }]] *

View

User view

定義済みユーザロール

network-admin

パラメータ

ftp-server: FTP サーバの IPv4 アドレスあるいはホスト名を指定します。ホスト名の設定範囲は 1～253 です。大文字、小文字を区別しません。ホスト名で使用できる文字列は文字、数字、ハイフン（-）、アンダーライン（-）、ドット（.）です。

service-port: FTP サーバの TCP ポート番号を指定します。設定範囲は 0～65535 です。デフォルトは 21 です。

dscp *dscp-value*: 送信 FTP パケットで使用される IPv4 パケットの DSCP 値です。パケットの優先度を示します。設定範囲は 0～63 です。デフォルトは 0 です。

source { **interface** *interface-type interface-number* | **ip** *source-ip-address* }: FTP 接続を確立するために使用する送信元アドレスを指定します。

- **interface** *interface-type interface-number*: インタフェースのタイプと番号を指定します。インタフェースのプライマリ IPv4 アドレスは FTP パケットを送信する送信元アドレスとして使用されます。送信元インタフェースにプライマリ IPv4 アドレスが設定されていない場合、接続は確立できません。
- **ip** *source-ip-address*: IPv4 アドレスを指定します。すでに装置で設定されている必要があります。

説明

ftp コマンドは FTP サーバにログインし、FTP client view に移行します。

このコマンドは IPv4 ネットワークでのみ有効です。

パラメータが指定されない場合、FTP サーバにログインしないで FTP client view に移行します。

パラメータが指定されている場合、FTP にログインするためのユーザ名とパスワードを入力する画面が表示されます。

例

FTP サーバ 192.168.0.211 にログインし、FTP パケットの送信元 IPv4 アドレスを 192.168.0.212 として指定します。

<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>
```

4.2.13 ftp client ipv6 source

Syntax

ftp client ipv6 source { **interface** *interface-type interface-number* | **ipv6** *source-ipv6-address* }

undo ftp client ipv6 source

デフォルト

FTP パケットを送信する送信元 IPv6 アドレスは設定されていません。装置は自動で RFC3484 によって定義された送信元 IPv6 アドレスを選択します。

View

System view

定義済みユーザロール

network-admin

パラメータ

interface *interface-type interface-number*: インタフェースのタイプと番号を指定します。送信元インタフェースに設定された IPv4 アドレスは FTP パケットを送信する送信元アドレスです。インタフェースが UP であることを確認してください。そうでなければ転送が失敗します。

ipv6 *source-ipv6-address*: FTP パケットを送信する送信元 IPv6 アドレスを指定します。UP 状態のインタフェースの IPv6 アドレスが設定されていることを確認してください。そうでなければ転送が失敗します。

説明

ftp client ipv6 source コマンドは IPv6 FTP サーバに送信する FTP パケットの送信元 IPv6 アドレスを指定します。

undo ftp client ipv6 source コマンドはデフォルトに戻します。

このコマンドを複数実行した場合、最後に実行したコマンドが適用されます。

ftp ipv6 コマンドで送信元アドレスが指定されている場合、**ftp client ipv6source** コマンドで指定された送信元アドレスよりも優先されます。

ftp client ipv6source コマンドで指定された送信元アドレスはすべての FTP 接続に適用されます。**ftp ipv6** コマンドで指定された送信元アドレスは現在の FTP 接続に適用されます。

例

FTP パケットを送信する送信元 IPv6 アドレスを 2000::1 として指定します。

<Switch> system–view

[Switch] ftp client ipv6 source ipv6 2000::1

関連コマンド

ftp ipv6

4.2.14 ftp client source

Syntax

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

undo ftp client source

デフォルト

FTP パケットを送信する送信元 IPv4 アドレスは設定されていません。装置は送信元 IP アドレスとしてルートの送信インタフェースのプライマリ IPv4 アドレスを使用します。

View

System view

定義済みユーザロール

network-admin

パラメータ

interface *interface-type interface-number*: FTP 接続を確立する送信元インタフェースを指定します。送信元インタフェースのプライマリ IPv4 アドレスは FTP サーバに送信するパケットの送信元 IP アドレスとして使用されます。転送が成功するために、インタフェースが UP し、プライマリ IPv4 アドレスが設定されていることを確認してください。

ip *source-ip-address*: FTP パケットを送信する送信元 IP アドレスを指定します。UP 状態のインタフェースの IPv4 アドレスが設定されていることを確認してください。そうでなければ転送が失敗します。

説明

ftp client source コマンドは FTP パケットを送信する送信元 IPv4 アドレスを指定します。

undo ftp client source コマンドはデフォルトに戻します。

このコマンドを複数実行した場合、最後に実行したコマンドが適用されます。

ftp コマンドで送信元アドレスが指定されている場合、**ftp client source** コマンドで指定された送信元アドレスよりも優先されます。

ftp client source コマンドで指定された送信元アドレスはすべての FTP 接続に適用されます。**ftp** コマンドで指定された送信元アドレスは現在の FTP 接続に適用されます。

例

FTP パケットを送信する送信元 IPv4 アドレスとして 192.168.20.222 を指定します。

<Switch> system-view

[Switch] ftp client source ip 192.168.20.222

関連コマンド

ftp

4.2.15 ftp ipv6

Syntax

ftp ipv6 [*ftp-server* [*service-port*] [**dscp** *dscp-value* | **source** { **ipv6** *source-ipv6-address* | **interface** *interface-type interface-number* }] * [**-i** *interface-type interface-number*]]

View

User view

定義済みユーザロール

network-admin

パラメータ

ftp-server: FTP サーバの IPv6 アドレスあるいはホスト名を指定します。ホスト名の設定範囲は 1～253 です。大文字、小文字を区別しません。ホスト名で使用できる文字列は文字、数字、ハイフン（-）、アンダーライン（-）、ドット（.）です。

service-port: FTP サーバの TCP ポート番号を指定します。設定範囲は 0～65535 です。デフォルトは 21 です。

dscp *dscp-value*: 送信 FTP パケットで使用される IPv6 パケットの DSCP 値です。パケットの優先度を示します。設定範囲は 0～63 です。デフォルトは 0 です。

source { **ipv6** *source-ipv6-address* | **interface** *interface-type interface-number* }: FTP 接続を確立するために使用する送信元アドレスを指定します。

- **interface** *interface-type interface-number*: インタフェースのタイプと番号を指定します。FTP サーバのアドレスがリンクローカルアドレスで指定された送信インタフェースにリンクローカルアドレスが存在しているときのみ使用することができます。リンクローカルアドレスの詳細は、オペレーションマニュアルのセクション 4 *IP サービス* “*IPv6 の基本*”を参照してください。
- **ipv6** *source-ipv6-address*: IPv6 アドレスを指定します。FTP 接続が成功するために、装置のインタフェースが IPv6 アドレスで設定されていて、アップしていることを確認してください。

-i *interface-type interface-number*: 送信インタフェースのタイプと番号を指定します。FTP サーバのアドレスがリンクローカルアドレスで、指定された送信インタフェースにリンクローカルアドレスが存在しているときのみ使用することができます。

説明

ftp ipv6 コマンドは FTP サーバにログインし、FTP client view に移行します。

このコマンドは IPv6 ネットワークでのみ有効です。

パラメータが指定されない場合、FTP サーバにログインしないで FTP client view に移行します。

パラメータが指定されている場合、FTP にログインするためのユーザ名とパスワードを入力する画面が表示されます。

例

FTP サーバ 2000:154 にログインします。

<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
```

4.2.16 get

Syntax

get *remotefile* [*localfile*]

View

FTP client view

定義済みユーザロール

network-admin

パラメータ

remotefile: ダウンロードするファイル名を指定します。

localfile: ダウンロードされたファイルの名前を指定します。指定しない場合、ダウンロードするファイル名を使用します。

説明

get コマンドは FTP サーバからファイルをダウンロードし、ファイルに保存します。

FTP サーバにログインしたのち、このコマンドを行うことができます。

ftp コマンドによって作業ディレクトリにダウンロードされたファイルを保存するため、以下のどちらかの作業を行います。

- *localfile* パラメータを指定しない場合、元のファイル名を使用します。
- *localfile* パラメータを指定する場合、ファイル名にパス情報を入力しないでください。たとえば a.cfg です。

ダウンロードされたファイルをほかのディレクトリに保存する場合、*localfile* パラメータはターゲットディレクトリと flash:/subdirectory/a.cfg のようなファイル名を追加する必要があります。

例

ファイル a.txt をダウンロードし、b.txt として **ftp** コマンドの作業ディレクトリに保存します。

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)
```

ファイル a.txt をダウンロードし、b.txt として **ftp** コマンドの作業ディレクトリの下の test フォルダに保存します。

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)
```

ファイル a.txt をダウンロードし、メンバ装置のフラッシュメモリのルートディレクトリに c.txt として保存します。

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)
```

関連コマンド

put

4.2.17 help

Syntax

help [*command-name*]

View

FTP client view

定義済みユーザロール

network-admin

パラメータ

command-name: FTP クライアントでサポートされるコマンドを指定します。

説明

help コマンドは FTP クライアントでサポートされるすべてのコマンドを表示します。

help *command-name* コマンドはコマンドのヘルプ情報を表示します。

FTP client view において **help** コマンドは、**?**コマンドと同一です。

例

FTP クライアントでサポートされるすべてのコマンドを表示します。

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
```

dir コマンドのヘルプ情報を表示します。

ftp> help dir

```
dir             list contents of remote directory
```

関連コマンド

?

4.2.18 lcd

Syntax

lcd [*directory* | */*]

View

FTP client view

定義済みユーザロール

network-admin

パラメータ

directory: FTP クライアントのローカルディレクトリを指定します。/flash:/logfile のように記憶媒体の名前の前にスラッシュ（/）が必要です。

/: FTP クライアントのルートディレクトリを指定します。

説明

lcd コマンドは FTP クライアントのローカル作業ディレクトリを表示します。

lcd *directory* コマンドは FTP クライアントのローカル作業ディレクトリを指定したディレクトリに変更します。

例

ローカル作業ディレクトリを表示します。

ftp> lcd

```
Local directory now /flash:
```

ローカル作業ディレクトリを flash:/logfile に変更します。

ftp> lcd /flash:/logfile

```
Local directory now /flash:/logfile
```

4.2.19 ls

Syntax

ls [*remotefile* [*localfile*]]

View

FTP client view

定義済みユーザロール

network-admin

パラメータ

remotefile: FTP サーバのファイルあるいはディレクトリを指定します。

localfile: 表示された情報が保存されるローカルファイルの名前を指定します。

説明

ls コマンドは FTP サーバ上の、現在のディレクトリにあるファイルおよびサブディレクトリに関する詳細情報を表示します。

ls *remotefile* コマンドは FTP サーバのファイルあるいはディレクトリに関する詳細情報を表示します。

ls *remotefile localfile* コマンドはリモート FTP サーバ上の指定したファイルまたはディレクトリに関する詳細情報を表示し、表示された情報を引数 *localfile* で指定したローカルファイルに保存します。

FTP サーバにログインした後のみ実行できます。

FTP client view において、**ls** コマンドは **dir** コマンドと同一です。

例

FTP サーバの現在のディレクトリのファイル、サブディレクトリの詳細情報を表示します。

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
```

ファイル a.txt の詳細情報を s.txt に保存します。

ftp> ls a.txt s.txt

```
output to local-file: s.txt ? [Y/N]y
150 Connecting to port 50203
226-Glob: s.txt
```

ファイル s.txt の内容を表示します。

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
```

関連コマンド

dir

4.2.20 mkdir

Syntax

mkdir *directory*

View

FTP client view

定義済みユーザロール

network-admin

パラメータ

directory: 作成するディレクトリの名前を指定します。

説明

mkdir コマンドは FTP サーバの現在のディレクトリにサブディレクトリを作成します。

FTP サーバにログインした後のみ実行できます。

この動作を実行するため、FTP サーバの権限が必要です。

例

リモート FTP サーバの現在のディレクトリにサブディレクトリ newdir を作成します。

ftp> mkdir newdir

```
257 "newdir" : The directory was successfully created
```

4.2.21 newer

Syntax

newer *remotefile* [*localfile*]

View

FTP client view

定義済みユーザロール

network-admin

パラメータ

remotefile: FTP サーバのリモートファイルの名前を指定します。

localfile: アップデートされたローカルファイルの名前を指定します。

説明

newer コマンドは FTP サーバのリモートファイルをローカルファイルにアップデートします。

FTP サーバにログインした後のみ実行できます。

ローカルファイルが存在しない場合、FTP サーバからファイルをダウンロードし、ローカルに保存します。

FTP サーバのリモートファイルがローカルファイルよりも古い場合、ローカルファイルをアップデートしません。

例

FTP サーバのファイル a.txt をローカルファイルにアップデートします。

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)
```

4.2.22 open

Syntax

open *server-address* [*service-port*]

View

FTP client view

定義済みユーザロール

network-admin

パラメータ

server-address: FTP サーバの IPv4 アドレス、IPv6 アドレスあるいはホスト名を指定します。

service-port: FTP サーバの TCP ポート番号を指定します。設定範囲は 0～65535 です。デフォルトは 21 です。

説明

open コマンドは FTP client view で FTP サーバにログインします。

このコマンドを実行した後、システムはユーザ名とパスワードを入力する画面が表示されます。

ある FTP サーバにログインした後、別のサーバに **open** コマンドを使用してログインする前に、サーバから切断する必要があります。

例

FTP client view で FTP サーバ 192.168.40.7 にログインします。

<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>
```

4.2.23 passive

Syntax

passive

デフォルト

passive

View

FTP client view

定義済みユーザロール

network-admin

説明

passive コマンドは FTP 伝送モードを passive に設定します。

ftp は以下のいずれかのモードを実行することができます。

- **Active モード**—FTP サーバが TCP 接続を開始します。
- **Passive モード**—FTP クライアントが TCP 接続を開始します。

このコマンドはモードの切り替えを行うため、複数回実行することができます。FTP 伝送モードが passive であるとき、コマンドを実行すると active に切り替わります。FTP 伝送モードが active であるとき、コマンドを実行すると passive に切り替わります。

このコマンドは主にプライベートネットワークユーザとパブリックネットワークユーザ間の FTP セッションの確立を制御する Firewall と一緒に使用されます。

例

FTP 伝送モードを passive に設定します。

ftp> passive

```
Passive mode on.
```

ftp> passive

```
Passive mode off.
```

4.2.24 put

Syntax

put *localfile* [*remotefile*]

View

FTP client view

定義済みユーザロール

network-admin

パラメータ

localfile: アップロードするファイル名を指定します。

remotefile: FTP サーバでアップロードされたファイルを保存するファイル名を指定します。

説明

put コマンドはリモート FTP クライアントから FTP サーバにファイルをアップロードします。

FTP サーバにログインした後のみ実行できます。

ftp コマンドによって作業ディレクトリにアップロードするため、*localfile* パラメータで a.cfg のようなファイル名を指定する必要があります。

アップロードされたファイルをほかのディレクトリに保存する場合、*localfile* パラメータはターゲットディレクトリと flash:/subdirectory/a.cfg のようにファイル名を追加する必要があります。

例

ftp コマンドで作業ディレクトリにファイル a.txt をアップロードします。FTP サーバに b.txt として保存します。

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)
```

ftp コマンドで作業ディレクトリからフォルダ test の a.txt をアップロードします。FTP サーバに b.txt として保存します。

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)
```

メンバ装置の記憶媒体のルートディレクトリのファイル a.txt をアップロードします。FTP サーバに b.txt として保存します。

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)
```

関連コマンド

get

4.2.25 pwd

Syntax

pwd

View

FTP client view

定義済みユーザロール

network-admin

説明

pwd コマンドは FTP サーバの現在アクセスしているディレクトリを表示します。

FTP サーバにログインした後のみ実行できます。

例

リモート FTP サーバの現在アクセスしているディレクトリを表示します。

ftp> cd subdir

```
250 OK. Current directory is /subdir
```

ftp> pwd

```
257 "/subdir" is your current location
```

4.2.26 quit

Syntax

quit

View

FTP client view

定義済みユーザロール

network-admin

説明

quit コマンドは FTP サーバの接続を終了し、user view に戻ります。

例

FTP サーバの接続を終了し、user view に戻ります。

ftp> quit

```
221-Goodbye. You uploaded 0 and downloaded 0 kbytes.
221 Logout.
<Switch>
```

関連コマンド

bye

4.2.27 rhelp

Syntax

rhelp [*protocol-command*]

View

FTP client view

定義済みユーザロール

network-admin

パラメータ

protocol-command: FTP コマンドを指定します。

説明

rhelp コマンドは FTP サーバがサポートしている FTP 関連コマンドを表示します。

rhelp *protocol-command* コマンドは FTP サーバがサポートしている FTP 関連コマンドのヘルプ情報を表示します。

FTP サーバにログインした後のみ実行できます。

例

FTP サーバがサポートしている FTP 関連コマンドを表示します。

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
```

表 4-3 コマンド出力

フィールド	説明
USER	ユーザ名を表示します。
PASS	パスワードを表示します。
NOOP	Null動作です。
SYST	システムパラメータを表示します。
TYPE	要求タイプを表示します。
CWD	現在のディレクトリを変更します。
XCWD	CWDコマンドの拡張コマンドです。
PWD	現在のディレクトリを表示します。
CDUP	上位ディレクトリに移動します。
XCUP	CDUPコマンドの拡張コマンドです。
XPWD	PWDコマンドの拡張コマンドです。
LIST	ファイルリストを表示します。
NLST	ファイルの説明を概要表示します。
MLSD	ファイル内容を表示します。
PORT	アクティブモード（IPv4）です。
EPRT	アクティブモード（IPv6）です。
PASV	パッシブモード（IPv4）です。
EPSV	パッシブモード（IPv6）です。
REST	再起動します。
RETR	ファイルをダウンロードします。

フィールド	説明
STOR	ファイルをアップロードします。
APPE	アップロードを追記します。
DELE	ファイルを削除します。
MKD	フォルダを作成します。
XMKD	MKDコマンドの拡張コマンドです。
RMD	フォルダを削除します。
XRMD	RMDコマンドの拡張コマンドです。
ABOR	転送を中断します。
SIZE	転送ファイルのサイズを表示します。
RNFR	元の名前を表示します。
RNTO	新しい名前を表示します。

4.2.28 rmdir

Syntax

rmdir *directory*

View

FTP client view

定義済みユーザロール

network-admin

パラメータ

directory: リモート FTP サーバのディレクトリ名を指定します。

説明

rmdir コマンドは FTP サーバのディレクトリを完全に削除します。

FTP サーバにログインした後のみ実行できます。

この動作を実行するため、FTP サーバの削除権限が必要です。

ディレクトリを削除する前に、ディレクトリにあるすべてのファイルとサブディレクトリを削除する必要があります。ファイルを削除する方法については、**delete** コマンドを参照してください。

コマンドを実行すると、指定したディレクトリのごみ箱にあるファイルは削除しません。

例

空のディレクトリ subdir1 を削除します。

ftp>rmdir subdir1

```
250 The directory was successfully removed
```

関連コマンド

delete

4.2.29 user

Syntax

user *username* [*password*]

View

FTP client view

定義済みユーザロール

network-admin

パラメータ

username: ターゲットユーザアカウントのユーザ名を指定します。

password: ターゲットユーザアカウントのパスワードを指定します。

説明

user コマンドは現在の FTP 接続で FTP 認証を初期化します。

FTP サーバにアクセスしようとして認証に失敗した場合、FTP サーバへの接続が終了する前に再度アクセスすることができます。

FTP サーバにログイン後、新しいアカウントに FTP 認証を開始することができます。

新しいアカウントに変更することで、FTP 接続を再確立することなく、異なる権限を取得することができます。

ターゲットユーザアカウントのユーザ名とパスワードは設定されている必要があります。そうでなければ、ユーザアカウントの変更は失敗し、FTP 接続が切断されます。

例

FTP にログインしたのち、ユーザ名 ftp、パスワード 123456 を使用し、FTP サーバにログインします。（出力は FTP サーバによって変わる可能性があります）

- 方法 1:

ftp> user ftp 123456

```
331 Password required for ftp.
230 User logged in.
```

- 方法 2:

ftp> user ftp

```
331 Password required for ftp.
Password:
230 User logged in.
```

4.2.30 verbose

Syntax

verbose

デフォルト

装置は FTP 動作の詳細情報を表示します。

View

FTP client view

定義済みユーザロール

network-admin

説明

verbose コマンドは FTP 動作の詳細情報の表示機能を有効、あるいは無効にします。

このコマンドは現在のセッションのみ適用されます。再度ログインしたとき、デフォルトの設定に戻ります。

例

FTP 動作の詳細情報の表示機能を無効にします。

ftp> verbose

```
Verbose mode off.
```

get コマンドを実行します。

ftp> get a.cfg 1.cfg

FTP 動作の詳細情報の表示機能を有効にします。

ftp> verbose

```
Verbose mode on.
```

get コマンドを実行します。

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)
```

4.2.31 ?

Syntax

? [*command-name*]

View

FTP client view

定義済みユーザロール

network-admin

パラメータ

command-name: FTP クライアントでサポートされるコマンドを指定します。

説明

? コマンドは FTP クライアントでサポートされるすべてのコマンドを表示します。

? *command-name* コマンドはコマンドのヘルプ情報を表示します。

FTP client view において**?**コマンドは、**help** コマンドと同一です。

例

FTP クライアントでサポートされるすべてのコマンドを表示します。

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
```

 # dir コマンドのヘルプ情報を表示します。

ftp> ? dir

```
dir             list contents of remote directory
```

関連コマンド

help

目次

このセクションのページは **1-x-x** です。

5 章 TFTP 5-1
5.1 TFTP 設定コマンド 5-1
5.1.1 tftp 5-1
5.1.2 tftp client ipv6 source 5-3
5.1.3 tftp client source 5-4
5.1.4 tftp ipv6 5-5
5.1.5 tftp-server acl 5-7
5.1.6 tftp-server ipv6 acl 5-8

5章 TFTP

5.1 TFTP設定コマンド

5.1.1 tftp

Syntax

tftp *tftp-server* { **get** | **put** | **sget** } *source-filename* [*destination-filename*] [**dscp** *dscp-value* | **source** { **interface** *interface-type interface-number* | **ip** *source-ip-address* }] *

View

User view

定義済みユーザロール

network-admin

パラメータ

tftp-server: TFTP サーバの IPv4 アドレスあるいはホスト名を指定します。ホスト名の設定範囲は 1～253 文字で、大文字、小文字を区別しません。ホスト名で使用できる文字列は英字、数字、ハイフン（-)、アンダーライン（-)、ドット（.）です。

get: ファイルをダウンロードし、宛先ファイルにファイルのディレクトリを書き込みます。宛先ファイルがすでに存在する場合、システムはダウンロードを開始する前に既存のファイルを削除します。ダウンロードが失敗しても既存のファイルは完全に削除されます。

put: ファイルをアップロードします。

sget: ファイルをダウンロードし、宛先ファイルを書き込みする前に、メモリにファイルを保存します。ダウンロードされたファイルが正常にメモリにダウンロードされたのち宛先ファイルにダウンロードされたファイルの書き込みを行います。宛先ファイルがすでに存在する場合、ダウンロードされたファイルは既存のファイルに上書きします。ダウンロードあるいはメモリへの書き込みが失敗すると、既存のファイルは上書きされません。

source-filename: 送信元ファイル名を指定します。設定範囲は 1～255 文字で、大文字、小文字を区別しません。

destination-filename: 宛先ファイル名を指定します。設定範囲は 1～255 文字で、大文字、小文字を区別しません。この引数が指定されない場合、ファイルは送信元ファイル名を使用します。

dscp *dscp-value*: 送信する TFTP パケットの IPv4 パケットの DSCP 値です。パケットを転送する優先度を示します。設定範囲は 0～63 です。デフォルトは 0 です。

source { **interface** *interface-type interface-number* | ip *source-ip-address* }: 送信する TFTP パケットの送信元アドレスを指定します。キーワードが指定されない場合、装置は送信元 IPv4 アドレスとして TFTP サーバへのルートの出力インタフェースのプライマリ IPv4 アドレスを使用します。

- **interface** *interface-type interface-number*: インタフェースのタイプと番号を指定します。インタフェースのプライマリ IPv4 アドレスは送信する TFTP パケットの送信元 IPv4 アドレスとして使用されます。インタフェースが UP でプライマリ IPv4 アドレスが設定されている必要があります。そうでなければ転送が失敗します。
- **ip** *source-ip-address*: IPv4 アドレスを指定します。インタフェースが UP でアドレスが IPv4 アドレスである必要があります。そうでなければ転送が失敗します。

説明

tftp コマンドは TFTP サーバからファイルをダウンロードあるいは IPv4 ネットワークの TFTP サーバにファイルをアップロードします。

tftp コマンドで指定された送信元アドレスは **tftp client source** コマンドで指定された送信元アドレスよりも優先されます。

tftp client source コマンドで指定された送信元アドレスはすべての TFTP 接続に適用されます。**tftp** コマンドで指定された送信元アドレスは現在の TFTP 接続に適用されます。

例

TFTP サーバ 192.168.1.1 から new.bin ファイルをダウンロードし、new.bin として保存します。

<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>
```

表 5-1 コマンド出力

フィールド	説明
%	ファイル転送の進捗状況を% で示します。
Total	転送されたファイルサイズです。単位はbyteです。
%	全ファイルサイズに対する受信したファイルサイズの割合を% で示します。
Received	受信したファイルサイズです。単位はbyteです。
%	全ファイルサイズに対する送信したファイルサイズの割合を% で示します。

フィールド	説明
Xferd	送信したファイルサイズです。単位はbyteです。
Average Dload	平均ダウンロード速度です。単位はbpsです。
Speed Upload	平均アップロード速度です。単位はbpsです。
Writing file...	システムがダウンロードファイルを記憶媒体に書き込みを行っています。**get**パラメータあるいは**sget**パラメータを指定したときのみ表示されます。 処理が成功すると、フィールドの最後に**Done**と表示します。 処理が失敗すると、フィールドの最後に**Failed**と表示します。

関連コマンド

tftp client source

5.1.2 tftp client ipv6 source

Syntax

tftp client ipv6 source { **interface** *interface-type interface-number* | **ipv6** *source-ipv6-address* }

undo tftp client ipv6 source

デフォルト

IPv6 TFTP サーバに送信する TFTP パケットの送信元アドレスは設定されていません。装置は自動で RFC3484 によって定義された送信元 IPv6 アドレスを選択します。

View

System view

定義済みユーザロール

network-admin

パラメータ

interface *interface-type interface-number*: 確立する TFTP 接続の送信元インタフェースを指定します。送信元インタフェースのプライマリ IPv6 アドレスは TFTP サーバに送信されるパケットの送信元 IPv6 アドレスとして使用されます。インタフェースが UP である必要があります。そうでなければ転送が失敗します。

ipv6 *source-ipv6-address*: TFTP パケットを送信する送信元 IPv6 アドレスを指定します。UP 状態のインタフェースの IPv6 アドレスが設定されていることを確認してください。そうでなければ転送が失敗します。

説明

tftp client ipv6 source コマンドは TFTP クライアントによって送信される TFTP パケットの送信元 IPv6 アドレスを指定します。

undo tftp client ipv6 source コマンドはデフォルトに戻します。

このコマンドを複数実行した場合、最後に実行したコマンドが適用されます。

tftp ipv6 コマンドで送信元アドレスが指定されている場合、**tftp client ipv6 source** コマンドで指定された送信元アドレスよりも優先されます。

tftp client ipv6 source コマンドで指定された送信元アドレスはすべての TFTP 接続に適用されます。**tftp ipv6** コマンドで指定された送信元アドレスは現在の TFTP 接続に適用されます。

例

IPv6 TFTP サーバに送信する TFTP パケットの送信元 IPv6 アドレスを 2000::1 として指定します。

<Switch> system–view

[Switch] tftp client ipv6 source ipv6 2000::1

関連コマンド

tftp ipv6

5.1.3 tftp client source

Syntax

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

undo tftp client source

デフォルト

TFTP サーバに送信する TFTP パケットで設定された送信元 IPv4 アドレスはありません。装置はルートの出力インタフェースのプライマリ IPv4 アドレスを送信元 IP アドレスとして使用します。

View

System view

定義済みユーザロール

network-admin

パラメータ

interface *interface-type interface-number*: 確立する TFTP 接続の送信元インタフェースを指定します。送信元インタフェースのプライマリ IPv4 アドレスは TFTP サーバに送信されるパケットの送信元 IPv4 アドレスとして使用されます。インタフェースが UP でプライマリ IPv4 アドレスが設定されている必要があります。そうでなければ転送が失敗します。

ip *source-ip-address*: 送信する TFTP パケットの送信元 IPv4 アドレスを指定します。UP 状態のインタフェースのアドレスが IPv4 アドレスである必要があります。そうでなければ転送が失敗します。

説明

tftp client source コマンドは TFTP サーバに送信する TFTP パケットの送信元 IPv4 アドレスを指定します。

undo tftp client source コマンドはデフォルトに戻します。

このコマンドを複数実行した場合、最後に実行したコマンドが適用されます。

tftp コマンドで送信元アドレスが指定されている場合、**tftp client source** コマンドで指定された送信元アドレスよりも優先されます。

tftp client source コマンドで指定された送信元アドレスはすべての TFTP 接続に適用されます。**tftp** コマンドで指定された送信元アドレスは現在の TFTP 接続に適用されます。

例

TFTP サーバに送信する TFTP パケットの送信元 IP アドレスを 192.168.20.222 として指定します。

<Switch> system-view

[Switch] tftp client source ip 192.168.20.222

関連コマンド

tftp

5.1.4 tftp ipv6

Syntax

tftp ipv6 *tftp-server* [**-i** *interface-type interface-number*] { **get** | **put** | **sget** } *source-filename* [*destination-filename*] [**dscp** *dscp-value* | **source** { **interface** *interface-type interface-number* | **ipv6** *source-ipv6-address* }] *

View

User view

定義済みユーザロール

network-admin

パラメータ

tftp-server: TFTP サーバの IPv6 アドレスあるいはホスト名を指定します。ホスト名の設定範囲は 1～253 文字で、大文字、小文字を区別しません。ホスト名で使用できる文字列は英字、数字、ハイフン（-）、アンダーライン（-）、ドット（.）です。

-i *interface-type interface-number*: 送信インタフェースのタイプと番号を指定します。このパラメータは TFTP サーバアドレスがリンクローカルアドレスで送信インタフェースにリンクローカルアドレスが設定されているときのみ使用されます。リンクローカルアドレスの詳細は、オペレーションマニュアルのセクション 4 *IP サービス* “*IPv6 の基本*” を参照してください。

get: ファイルをダウンロードし、宛先ファイルにファイルのディレクトリを書き込みます。宛先ファイルがすでに存在する場合、システムはダウンロードを開始する前に既存のファイルを削除します。ダウンロードが失敗しても既存のファイルは完全に削除されます。

put: ファイルをアップロードします。

sget: ファイルをダウンロードし、宛先ファイルを書き込みする前に、メモリにファイルを保存します。ダウンロードされたファイルが正常にメモリにダウンロードされたのち宛先ファイルにダウンロードされたファイルの書き込みを行います。宛先ファイルがすでに存在する場合、ダウンロードされたファイルは既存のファイルに上書きします。ダウンロードあるいはメモリへの書き込みが失敗すると、既存のファイルは上書きされません。

source-file: 送信元ファイル名を指定します。設定範囲は 1～255 文字で、大文字、小文字を区別しません。

destination-file: 宛先ファイル名を指定します。設定範囲は 1～255 文字で、大文字、小文字を区別しません。この引数が指定されない場合、ファイルは送信元ファイル名を使用します。

dscp *dscp-value*: 送信する TFTP パケットの IPv6 パケットの DSCP 値です。パケットを転送する優先度を示します。設定範囲は 0～63 です。デフォルトは 0 です。

source { **interface** *interface-type interface-number* | **ipv6** *source-ipv6-address* }:送信する TFTP パケットの送信元アドレスを指定します。キーワードが指定されない場合、装置は自動で RFC3484 によって定義された送信元 IPv6 アドレスを選択します。

- **interface** *interface-type interface-number*: インタフェースのタイプと番号を指定します。インタフェースのプライマリ IPv6 アドレスは送信する TFTP パケットの送信元 IPv6 アドレスとして使用されます。インタフェースが UP でプライマリ IPv6 アドレスが設定されている必要があります。そうでなければ転送が失敗します。
- **ipv6** *source-ipv6-address*: IPv6 アドレスを指定します。インタフェースが UP でアドレスが IPv6 アドレスである必要があります。そうでなければ転送が失敗します。

説明

tftp ipv6 コマンドは TFTP サーバからファイルをダウンロードあるいは IPv6 ネットワークの TFTP サーバにファイルをアップロードします。

tftp ipv6 コマンドで指定された送信元アドレスは **tftp client ipv6 source** コマンドで指定された送信元アドレスよりも優先されます。

tftp client ipv6 source コマンドで指定された送信元アドレスはすべての TFTP 接続に適用されます。**tftp ipv6** コマンドで指定された送信元アドレスは現在の TFTP 接続に適用されます。

例

TFTP サーバ 2001::1 から new.bin ファイルをダウンロードし、new.bin として保存します。

<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.
```

コマンド出力の詳細は表 5-1 を参照してください。

5.1.5 tftp-server acl

Syntax

tftp-server acl *acl-number*

undo tftp-server acl

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

acl-number: 標準 ACL の番号を指定します。設定範囲は 2000～2999 です。

説明

tftp-server acl コマンドは IPv4 ネットワークの TFTP サーバへの装置のアクセスを制御する ACL を使用します。

undo tftp-server acl コマンドはデフォルトに戻します。

ACL を使用して、装置から指定された TFTP サーバへのアクセスを許可または禁止することができます。

例

TFTP サーバ 1.1.1.1 へのアクセスのみを許可します。

<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

Syntax

tftp-server ipv6 acl *ipv6-acl-number*

undo tftp-server ipv6 acl

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

ipv6-acl-number: 標準 ACL の番号を指定します。設定範囲は 2000～2999 です。

説明

tftp-server ipv6 acl コマンドは IPv6 ネットワークの TFTP サーバへの装置のアクセスを制御する ACL を使用します。

undo tftp-server ipv6 acl コマンドはデフォルトに戻します。

ACL を使用して、装置から指定された TFTP サーバへのアクセスを許可または禁止することができます。

例

TFTP サーバ 2001::1 へのアクセスのみを許可します。

<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

目次

このセクションのページは **1-x-x** です。

6 章 ファイルシステム管理 6-1
6.1 ファイルシステム管理設定コマンド 6-1
6.1.1 cd 6-2
6.1.2 copy 6-2
6.1.3 delete 6-6
6.1.4 dir 6-7
6.1.5 file prompt 6-9
6.1.6 fixdisk 6-10
6.1.7 format 6-11
6.1.8 gunzip 6-12
6.1.9 gzip 6-13
6.1.10 mkdir 6-14
6.1.11 more 6-14
6.1.12 move 6-15
6.1.13 pwd 6-16
6.1.14 rename 6-16
6.1.15 reset recycle-bin 6-17
6.1.16 rmdir 6-18
6.1.17 tar create 6-19
6.1.18 tar extract 6-20
6.1.19 tar list 6-21
6.1.20 undelete 6-22

6章 ファイルシステム管理

6.1 ファイルシステム管理設定コマンド

⚠ **注意：**

- 記録媒体、ファイル、ディレクトリを管理する前に、設定が装置に与える影響を確認してから行ってください。
- ピリオド（. ）の名前で始まるファイルあるいはディレクトリは、隠しファイルあるいは隠しディレクトリです。ファイルあるいはディレクトリの先頭にピリオド（. ）を使用しないでください。
- いくつかの隠しファイルと隠しディレクトリが存在します。ファイルシステムの管理を行う際は、隠しファイルや隠しディレクトリを修正しないでください。

⚠ **注意：**

- 表示される空き容量は実際のファイルサイズで計算されています。保存に必要なサイズはファイルの種類によって実際のファイルサイズと異なる場合がありますので、ファイルの保存は十分な空き容量があることを確認してから行ってください。
- ファイルのダウンロードやコピーを行う場合は、十分な空き容量を確保してから行ってください。空き容量が不足している場合には、エラーとなり異常なファイルが残る場合があります。保存に失敗した場合は、不要なファイルを削除してください。

ファイルシステムはフラッシュメモリなどの記憶媒体です。

ファイル名、ディレクトリ名はファイル名のフォーマットで指定されています。詳細はオペレーションマニュアルのセクション 1 *はじめに* “*ファイルシステム管理*”を参照してください。

ファイルシステムでのコピー、削除、フォーマット、ファイルの圧縮、解凍、フォルダの作成、移動、ファイル名の変更、フォルダの削除、ファイルの復元を行う前に、フラッシュメモリのプロテクトが解除されていることを確認してください。

別のユーザがファイルシステムの回復、フォーマットを行っている間、ファイルシステムにアクセスすることはできません。

ファイルシステムの回復、フォーマットの後、ファイルシステムにアクセスする場合、以下のいずれかの作業を行ってください。

- コマンドのファイルシステムの名前を指定してください。たとえば、フラッシュメモリのすべてのファイル、フォルダを表示する **dir flash:/**コマンドを使用してください。
- コマンドを使用する前に、ファイルシステムにディレクトリを変更する場合、**cd** コマンドを使用してください。たとえば、フラッシュメモリのルートディレクトリに移動する場合、コ **cd flash:/**コマンドを使用してください。そしてすべてのファイル、フォルダを表示するために **dir** コマンドを使用してください。

6.1.1 cd

Syntax

cd { *directory* | **..** }

View

User view

定義済みユーザロール

network-admin

パラメータ

directory: 宛先ディレクトリの名前を指定します。

..: 上位ディレクトリに戻ります。現在のディレクトリがルートディレクトリである場合、コマンドを実行したときエラーメッセージが表示されます。このパラメータに対するコマンドラインヘルプはありません。

説明

cd コマンドは現在の作業ディレクトリを変更します。

例

装置にログインした後、フォルダ test にアクセスします。

<Switch> cd test

上位ディレクトリに戻ります。

<Switch> cd ..

6.1.2 copy

Syntax

copy *source-file* { *dest-file* | *dest-directory* }

View

User view

定義済みユーザロール

network-admin

パラメータ

source-file: ファイルの名前あるいは URL を指定します。ファイルが装置上ではなく FTP、TFTP、HTTP サーバにある場合、ファイル URL を指定します。URL が大文字、小文字を区別するかどうかはサーバによって異なります。

dest-file: 宛先ファイルの名前あるいは URL を指定します。送信元ファイルを FTP、TFTP、あるいは HTTP サーバにコピーする場合、URL を指定します。ディレクトリを指定する場合、装置は指定したファイルをディレクトリにコピーしもとのファイル名で保存します。URL が大文字、小文字を区別するかどうかはサーバによって異なります。

dest-directory: 宛先ディレクトリの名前あるいは URL を指定します。送信元ファイルを FTP、TFTP、あるいは HTTP サーバにコピーする場合、URL を指定します。ディレクトリを指定する場合、装置は指定したファイルをディレクトリにコピーしもとのファイル名で保存します。URL が大文字、小文字を区別するかどうかはサーバによって異なります。

説明

copy コマンドはファイルをコピーします。

以下の処理を実行することができます。

- ローカルファイルをコピーし、ローカルに保存します。
- ローカルファイルをコピーし、FTP、TFTP、あるいは HTTP サーバに保存します。
- FTP、TFTP、あるいは HTTP サーバのファイルをコピーし、ローカルに保存します。

ファイルあるいはディレクトリを指定するため、以下のガイドラインを使用します。

位置	フォーマット	補足
装置	オペレーションマニュアルのセクション1 *はじめに*“*ファイルシステム管理*”の“*ファイル名のガイドライン*”を参照してください。	–

位置	フォーマット	補足
FTPサーバ	以下の形式のURLを入力します。 ftp://*FTPユーザ名*[:*パスワード*]@*サーバアドレス*[:*ポート番号*]/*ファイルパス*[/*ファイル名*].	ユーザ名とパスワードはFTPサーバで設定されているユーザ名とパスワードと同一にしてください。 サーバがユーザ名のみでユーザを認証する場合、パスワードを入力する必要はありません。 たとえばユーザ名1、パスワード1、FTPサーバ1.1.1.1で許可された作業ディレクトリのstartup.cfgを指定する場合、ftp://1:1@1.1.1.1/startup.cfgを入力します。
TFTPサーバ	以下の形式のURLを入力します。 tftp://*サーバアドレス*[:*ポート番号*]/*ファイルパス*[/*ファイル名*].	たとえば、TFTPサーバ1.1.1.1の作業ディレクトリのstartup.cfgをしている場合、tftp://1.1.1.1/startup.cfgを入力します。 IPv6アドレスを指定する場合、括弧内にIPv6アドレスを記載してください。 たとえば、tftp://[2001::1]/startup.cfgを入力します。
HTTPサーバ	以下の形式のURLを入力します。 http://*HTTPユーザ名*[:*パスワード*]@*サーバアドレス*[:*ポート番号*]/*ファイルパス*[/*ファイル名*].	ユーザ名とパスワードはHTTPサーバで設定されているユーザ名とパスワードと同一にしてください。 サーバがユーザ名のみでユーザを認証する場合、パスワードを入力する必要はありません。認証が必要ない場合、ユーザ名、あるいはパスワードを入力する必要はありません。 たとえばユーザ名a、パスワード1、HTTPサーバ1.1.1.1で許可された作業ディレクトリのstartup.cfgを指定する場合、http://a:1@1.1.1.1/startup.cfgを入力します。認証が必要ない場合、http://1.1.1.1/startup.cfgを入力します。

IPv6 アドレスを指定する場合、括弧内に IPv6 アドレスを記載してください。たとえば、ftp://test:test@[2001::1]:21/test.cfg を入力します。

例

現在のフォルダのファイル test.cfg をコピーし、ファイル名を testbackup.cfg として現在のフォルダに保存します。

<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.
```

現在のフォルダのファイル test.cfg をコピーし、ファイル名を testbackup.cfg としてメンバ ID2 のメンバ装置のフラッシュメモリのフォルダに保存します。

<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.
```

FTP サーバ 1.1.1.1 の作業ディレクトリからファイル test.cfg をコピーします。ファイル名を testbackup.cfg としてローカルの現在のフォルダにコピーを保存します。FTP のユーザ名は user、パスワードは private です。

<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.
```

現在のフォルダからファイル test.cfg をコピーします。ファイル名を testbackup.cfg として FTP サーバ 1.1.1.1 の作業ディレクトリにコピーします。FTP のユーザ名は user、パスワードは private です。

<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.
```

TFTP サーバ 1.1.1.1 の作業ディレクトリから test.cfg をコピーします。ファイル名を testbackup.cfg としてローカルの現在のフォルダにコピーを保存します。

<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.
```

現在のフォルダからファイル test.cfg をコピーします。ファイル名を testbackup.cfg として TFTP サーバ 1.1.1.1 の作業ディレクトリにコピーを保存します。

<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.
```

FTP サーバ 2001::1 の作業ディレクトリからファイル test.cfg をコピーします。ファイル名を testbackup.cfg としてローカルの現在のフォルダにコピーを保存します。FTP のユーザ名は user、パスワードは private です。

<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.
```

TFTP サーバ 2001::1 の作業ディレクトリからファイル test.cfg をコピーします。ファイル名を testbackup.cfg としてローカルの現在のフォルダにコピーを保存します。

<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.
```

HTTP サーバ 1.1.1.1 で許可されたディレクトリからファイル test.cfg をコピーします。ファイル名を testbackup.cfg としてローカルの現在のフォルダにコピーを保存します。HTTP ログインのユーザ名は user、パスワードは private です。

<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.
```

現在のフォルダからファイル test.cfg をコピーします。ファイル名を testbackup.cfg として HTTP サーバ 1.1.1.1 で許可されたディレクトリにコピーします。HTTP ログインのユーザ名は user、パスワードは private です。

<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.
```

HTTP サーバ 2001::1 で許可されたディレクトリからファイル test.cfg をコピーします。ファイル名を testbackup.cfg としてローカルの現在のフォルダにコピーを保存します。HTTP ログインのユーザ名は user、パスワードは private です。

<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

Syntax

delete [**/unreserved**] *file*

View

User view

定義済みユーザロール

network-admin

パラメータ

/unreserved: 指定されたファイルを完全に削除します。このパラメータを指定しない場合、ごみ箱にファイルを移動します。

file: 削除するファイル名を指定します。アスタリスク（*）はワイルドカードとして使用できます。たとえば、現在のディレクトリにある拡張子が”.txt”のファイルを削除する場合、”*.txt”と入力します。

説明

delete コマンドはファイルを削除します。

delete /unreserved *file* コマンドを使用する場合、削除されたファイルを復元することができません。

/unreserved パラメータを使用しないで **delete** *file* コマンドは指定したファイルをごみ箱に移動します。

ごみ箱に移動したファイルは **undelete** コマンドを使用して復元することができます。

ごみ箱のファイルを削除する際に **delete** コマンドを使用しないでください。ごみ箱のファイルを削除する場合、**reset recycle-bin** コマンドを使用してください。

以下の状況を除いて、ファイルは完全に削除されます。

- 装置の記憶領域を使い果たしています。
- 異なるディレクトリにある同一ファイル名の 2 つのファイルを削除する場合、2 つのファイルはごみ箱に保存されます。同一ディレクトリの同一ファイル名の 2 つのファイルを削除した場合、最後に削除されたファイルのみがごみ箱に保存されています。

例

現在のディレクトリからファイル 1.cfg を削除します。

<Switch> delete 1.cfg

```
Delete flash:/1.cfg? [Y/N]:y
Deleting file flash:/1.cfg...Done.
```

現在のディレクトリからファイル 1.cfg を完全に削除します。

<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.
```

関連コマンド

- **reset recycle-bin**
- **undelete**

6.1.4 dir

Syntax

dir [**/all**] [*file* | *directory* | **/all-filesystems**]

View

User view

定義済みユーザロール

network-admin

パラメータ

/all: 現在のディレクトリのすべてのファイルとフォルダを隠しファイル、隠しフォルダを含めてすべて表示します。このパラメータを指定しない場合、隠しファイル、隠しフォルダを除いたファイルとフォルダが表示されます。

file: 指定したファイルを表示します。アスタリスク（*）はワイルドカードとして使用できます。たとえば、現在のディレクトリにある拡張子が“.txt”のファイルを表示する場合、**dir** **.txt* と入力します。

directory: 指定したディレクトリを表示します。

/all-filesystems: 装置のすべてのファイルシステムのルートディレクトリのファイルとフォルダを表示します。

説明

dir コマンドはファイルあるいはフォルダを表示します。

パラメータを指定しない場合、現在のディレクトリの隠しファイル、隠しフォルダを除いたファイルとフォルダを表示します。

ごみ箱のフォルダ名は“.trash”です。ごみ箱のファイルを表示する場合、以下のどちらかの方法を使用します。

- **dir /all** *.trash* コマンドを実行します。
- **cd** *.trash* コマンドを実行し、**dir** コマンドを実行します。

例

現在のディレクトリにあるすべてのファイルとフォルダを表示します。

<Switch> dir /all

```
Directory of flash:/
...
```

装置のすべてのファイルシステムのルートディレクトリにあるすべてのファイルとフォルダを表示します。

<Switch> dir /all-filesystems

```
Directory of flash:/
...


Directory of usba0:/
...
```

表 6-1 コマンド出力

フィールド	説明
Directory of	現在のディレクトリです。
0 -rwh 3144 Apr 26 2014 13:45:28 xx.xx	ファイルあるいはフォルダ情報です。 • **0**—ファイルあるいはフォルダ番号です。システムによって自動で割り当てられます。 • **-rwh**—ファイルあるいはフォルダの属性です。最初の文字はフォルダを示します。**d**はフォルダで、ーはファイルです。2番目の文字はファイルあるいはフォルダが読み込み可能かどうかを示します。**r**は読み込み可能です。3番目の文字はファイルあるいはフォルダが書き込み可能かどうかを示します。**w**は書き込み可能です。4番目の文字はファイルあるいはフォルダが隠しファイルあるいは隠しフォルダかどうかを示します。**h**は隠しファイルあるいは隠しフォルダで、ーは通常のファイルあるいはフォルダです。変更、名前の変更、隠しファイルあるいは隠しフォルダの削除は機能に影響します。 • **3144**—ファイルサイズです。単位はbyteです。フォルダはハイフン（ー）が表示されます。 • **Apr 26 2014 13:45:28**—ファイルあるいはフォルダが変更された最後の日時です。 • **xx.xx**—ファイルあるいはフォルダ名です。

6.1.5 file prompt

Syntax

file prompt { **alert** | **quiet** }

undo file prompt

デフォルト

alert

View

System view

定義済みユーザロール

network-admin

パラメータ

alert: ファイルの破損やデータの損失など、望ましくない結果を引き起こす可能性のある操作について、システムが警告できるようにします。

quiet: ファイルあるいはディレクトリの操作に関する警告を行いません。

説明

file prompt コマンドはファイル、フォルダのプロンプトモードを設定します。

undo file prompt コマンドはデフォルトに戻します。

quiet モードである場合、システムはいかなるファイル操作に関しても警告を行いません。**alert** モードである場合、望ましくない結果を引き起こす可能性のある操作を中止できるように、警告を表示します。

例

ファイル、フォルダのプロンプトモードを alert に設定します。

<Switch> system-view

[Switch] file prompt alert

6.1.6 fixdisk

Syntax

fixdisk *filesystem*

View

User view

定義済みユーザロール

network-admin

パラメータ

filesystem: ファイルシステムの名前を指定します。値は装置の種類によって異なります。

説明

fixdisk コマンドは何らかの異常操作によりファイルシステムが使用できなくなった場合、ファイルシステムを確認し、ダメージ領域を復元します。

このコマンドは、ファイルシステムの空きスペースが使用できないあるいは異常な操作により解放されたとき、ファイルシステムを修正します。

ファイルシステムを修正する前に、ほかのユーザがファイルシステムにアクセスしていないことを確認してください。そうでなければ、修正作業が失敗します。

例

ファイルシステムの空きスペースを復元します。

<Switch> fixdisk flash:

```
Restoring flash: may take some time...
Restoring flash:...Done.
```

6.1.7 format

Syntax

format *filesystem*

View

User view

定義済みユーザロール

network-admin

パラメータ

filesystem: ファイルシステムの名前を指定します。値は装置の種類によって異なります。

説明

format コマンドはファイルシステムをフォーマットします。

装置は VFAT ファイルシステムのみサポートします。装置で異なるタイプのファイルシステムを使用する場合、ファイルシステムをフォーマットする必要があります。

ファイルシステムをフォーマットすると、ファイルシステムにあるすべてのファイルを完全に削除します。ファイルシステムに起動設定ファイルが保存されている場合、ファイルシステムを初期化すると、起動設定ファイルも失われます。

ファイルシステムへのアクセスがないときのみ、ファイルシステムをフォーマットすることができます。

例

ファイルシステムをフォーマットします。

<Switch> format flash:

```
All data on flash: will be lost, continue? [Y/N]:y
Formatting flash:... Done.
```

6.1.8 gunzip

Syntax

gunzip *file*

View

User view

定義済みユーザロール

network-admin

パラメータ

file: 解凍するファイルの名前を指定します。拡張子は“.gz”にする必要があります。

説明

gunzip コマンドはファイルを解凍します。

このコマンドは解凍した後、もとのファイルを削除します。

例

ファイル system.bin.gz を解凍します。

1) ファイルを解凍する前に、system の文字列で始まる名前のファイルを表示 します。

<Switch> dir system.*

```
Directory of flash:
  1 -rw-        20 Jun 14 2012 10:18:53   system.bin.gz


251904 KB total (193312 KB free)
```

2) ファイル system.bin.gz を解凍します。

<Switch> gunzip system.bin.gz

```
Decompressing file flash:/system.bin.gz..... Done.
```

3) 解凍した操作の確認を行います。

<Switch> dir system.*

```
Directory of flash:
  1 -rw-         0 May 30 2012 11:42:25   system.bin


251904 KB total (193312 KB free)
```

6.1.9 gzip

Syntax

gzip *file*

View

User view

定義済みユーザロール

network-admin

パラメータ

file: 圧縮するファイル名を指定します。圧縮するファイルの拡張子は、“.gz”で保存されます。

説明

gzip コマンドはファイルを圧縮します。

このコマンドは圧縮した後、もとのファイルを削除します。

例

ファイル system.bin を圧縮します。

1) ファイルを圧縮する前に、system の文字列で始まる名前のファイルを表示します。

<Switch> dir system.*

```
Directory of flash:
   1 -rw-          0 May 30 2012 11:42:24   system.bin


1251904 KB total (193312 KB free)
```

2) ファイル system.bin を圧縮します。

<Switch> gzip system.bin

```
Compressing file flash:/system.bin..... Done.
```

3) 圧縮した操作の確認を行います。

<Switch> dir system.*

```
Directory of flash:
   1 -rw-         20 Jun 14 2012 10:18:53   system.bin.gz


251904 KB total (193312 KB free)
```

6.1.10 mkdir

Syntax

mkdir *directory*

View

User view

定義済みユーザロール

network-admin

パラメータ

directory: フォルダの名前を指定します。

説明

mkdir コマンドは現在のディレクトリの下にフォルダを作成します。

フォルダの名前は指定されたディレクトリで重複しないように一意にする必要があります。

このコマンドを使用するため、現在のディレクトリは既に存在している必要があります。たとえば、フォルダ flash:/test/mytest を作成する場合、フォルダ test は既に存在している必要があります。そうでなければ、フォルダ mytest は作成されません。

例

現在のディレクトリにフォルダ test を作成します。

<Switch> mkdir test

```
Creating directory flash:/test... Done.
```

現在のディレクトリにフォルダ test/subtest を作成します。

<Switch> mkdir test/subtest

```
Creating directory flash:/test/subtest... Done.
```

6.1.11 more

Syntax

more *file*

View

User view

定義済みユーザロール

network-admin

パラメータ

file: ファイル名を指定します。

説明

more コマンドはテキストファイルの内容を表示します。

例

ファイル test.txt の内容を表示します。

<Switch> more test.txt

```
Have a nice day.
```

ファイル testcfg.cfg の内容を表示します。

<Switch> more testcfg.cfg

```
#
 version 7.1.070, Release 1201
#
 sysname Switch
#
vlan 2
#
return
<Switch>
```

6.1.12 move

Syntax

move *source-file* { *dest-file* | *dest-directory* }

View

User view

定義済みユーザロール

network-admin

パラメータ

source-file: ソースファイルの名前を指定します。

dest-file: ターゲットファイルの名前を指定します。

dest-directory: ターゲットファイルあるいはフォルダの名前を指定します。

説明

move コマンドはファイルを移動します。

ターゲットフォルダを指定する場合、システムはファイル名を変更しないで指定したフォルダにソースファイルを移動します。

例

ファイル flash:/test/sample.txt を flash:/に移動し、ファイル 1.txt に保存します。

<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.
```

ファイル b.cfg をフォルダ test2 に移動します。

<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.
```

6.1.13 pwd

Syntax

pwd

View

User view

定義済みユーザロール

network-admin

説明

pwd コマンドは現在の作業ディレクトリを表示します。

例

現在の作業ディレクトリを表示します。

<Switch> pwd

```
flash:
```

6.1.14 rename

Syntax

rename { *source-file* | *source-directory* } { *dest-file* | *dest-directory* }

View

User view

定義済みユーザロール

network-admin

パラメータ

source-file: ソースファイルの名前を指定します。

source-directory:ソースフォルダの名前を指定します。

dest-file: ターゲットファイルの名前を指定します。

dest-directory:ターゲットフォルダの名前を指定します。

説明

rename コマンドはファイルあるいはフォルダの名前を変更します。

現在の作業ディレクトリのファイルあるいはフォルダに変更しようとするファイルあるいはフォルダの名前が存在する場合、このコマンドは実行されません。

例

ファイル copy.cfg をファイル test.cfg に変更します。

<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.
```

6.1.15 reset recycle-bin

Syntax

reset recycle-bin [**/force**]

View

User view

定義済みユーザロール

network-admin

パラメータ

/force: 確認のプロンプトの表示を行わず、ごみ箱のすべてのファイルを削除します。このパラメータを指定しない場合、確認のプロンプトが表示されます。

説明

reset recycle-bin コマンドはごみ箱からファイルを削除します。

delete *file* コマンドはごみ箱にファイルを移動します。ファイルを完全に削除する場合、**reset recycle-bin** コマンドを使用してごみ箱を消去します。

例

2 つのファイルが存在しているごみ箱からファイルを削除します。

<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.
```

2 つのファイルが存在しているごみ箱からファイル b.cfg を削除します。

<Switch> reset recycle-bin

```
Clear flash:/a.cfg? [Y/N]:n
Clear flash:/b.cfg? [Y/N]:y
Clearing file flash:/b.cfg... Done.
```

関連コマンド

delete

6.1.16 rmdir

Syntax

rmdir *directory*

View

User view

定義済みユーザロール

network-admin

パラメータ

directory: フォルダ名を指定します。

説明

rmdir コマンドはフォルダを削除します。

ディレクトリを削除するため、ディレクトリのすべてのファイルとサブディレクトリを完全に削除するかごみ箱に移動する必要があります。ごみ箱に移動する場合、**rmdir** コマンドを実行して完全に削除することができます。

例

フォルダ subtest を削除します。

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.
```

6.1.17 tar create

Syntax

tar create [**gz**] *archive-file dest-file* [**verbose**] **source** { *source-file* | *source-directory* }&<1-5>

View

User view

定義済みユーザロール

network-admin

パラメータ

gz: ファイル、フォルダをアーカイブする前に **gzip** コマンドでファイル、フォルダを圧縮します。指定しない場合、圧縮しないでファイル、フォルダをアーカイブします。

archive-file dest-file: アーカイブファイル名を指定します。**gz** パラメータを指定する場合、引数の拡張子は“.tar.gz”にする必要があります。**gz** パラメータを指定しない場合、引数の拡張子は“.tar”にする必要があります。

verbose: 正常にアーカイブされたファイル、フォルダの名前を表示します。指定しない場合、ファイル、フォルダの名前を表示しません。

source { *source-file* | *source-directory* }&<1-5>: アーカイブされるファイル、フォルダを指定します。引数は半角スペースで区切ることで 5 つまで指定することができます。

説明

tar create コマンドはファイル、フォルダをアーカイブします。

例

ファイル 1.cfg、2.cfg、test ディレクトリをファイル a.tar にアーカイブします。

<Switch> tar create archive-file a.tar source 1.cfg 2.cfg test

```
Creating archive flash:/a.tar Done.
```

ファイル 1.cfg、2.cfg、test ディレクトリを圧縮し、ファイル b.tar.gz にアーカイブします。

<Switch> tar create gz archive-file b.tar.gz source 1.cfg 2.cfg test

```
Creating archive flash:/b.tar.gz Done.
```

ファイルとフォルダを圧縮、アーカイブします。アーカイブしたファイルとフォルダを表示します。

<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
```

関連コマンド

- **tar extract**
- **tar list**

6.1.18 tar extract

Syntax

tar extract archive-file *file* [**verbose**] [**screen** | **to** *directory*]

View

User view

定義済みユーザロール

network-admin

パラメータ

archive-file *file*: アーカイブファイル名を指定します。拡張子は “.tar” あるいは “.tar.gz” です。

verbose: 正常に解凍したファイルとフォルダの名前を表示します。

screen: 画面に解凍したファイルとフォルダの内容を表示します。解凍したファイルは保存されません。

to *directory-name*: 解凍したファイルとフォルダをパスに保存します。

説明

tar extract コマンドはファイルとフォルダを解凍します。

screen パラメータあるいは **to** *directory-name* パラメータを指定しない場合、解凍したファイルとフォルダを解凍し、解凍ファイルとして同一フォルダに保存します。

コマンドはもとの名前を使用して、解凍したファイル、ディレクトリを保存します。既に同一ファイル、ディレクトリが存在する場合、解凍したファイル、ディレクトリを既存のファイル、ディレクトリに上書きします。

例

アーカイブファイル a.tar からファイル、ディレクトリを解凍します。

<Switch> tar extract archive-file a.tar

```
Extracting archive flash:/a.tar Done.
```

アーカイブファイル a.tar からファイルとフォルダを解凍し、アーカイブしたファイルとフォルダの名前を表示します。

<Switch> tar extract archive-file b.tar.gz verbose

```
1.cfg
2.cfg
test/
test/a.log
test/subtest/
test/subtest/aa.log
```

アーカイブファイル a.tar からファイルを解凍し、アーカイブしたファイルの内容を表示します。

<Switch> tar extract archive-file c.tar.gz screen

```
#
 version 7.1.070, Release 1201
#
 sysname Switch
#
...
```

関連コマンド

- **tar create**
- **tar list**

6.1.19 tar list

Syntax

tar list archive-file *file*

View

User view

定義済みユーザロール

network-admin

パラメータ

archive-file *file*: アーカイブファイル名を指定します。拡張子は“.tar”あるいは“.tar.gz”です。

説明

tar list コマンドはアーカイブしたファイルとフォルダの名前を表示します。

例

アーカイブしたファイルとフォルダの名前を表示します。

<Switch> tar list archive-file a.tar

```
1.cfg
2.cfg
test/
test/a.log
test/subtest/
test/subtest/aa.log
```

関連コマンド

- **tar create**
- **tar extract**

6.1.20 undelete

Syntax

undelete *file*

View

User view

定義済みユーザロール

network-admin

パラメータ

file: 復元するファイルの名前を指定します。

説明

undelete コマンドはごみ箱からファイルを復元します。

ディレクトリに同一名のファイルが存在する場合、既存のファイルに上書きするかどうかの画面を表示します。”Y”を入力した場合、既存のファイルは上書きされます。”N”を入力した場合、このコマンドは実行されません。

例

copy.cfg ファイルを復元します。このファイルはディレクトリ flash:からごみ箱に移動されたファイルです。

<Switch>undelete copy.cfg

```
Undelete flash:/copy.cfg? [Y/N]:y
Undeleting file flash:/copy.cfg... Done.
```

ファイル startup.cfg を復元します。このファイルはディレクトリ flash:/seclog からごみ箱に移動されたファイルです。

- 方法 1:

<Switch>undelete seclog/startup.cfg

```
Undelete flash:/seclog/startup.cfg? [Y/N]:y
Undeleting file flash:/seclog/startup.cfg... Done.
<Switch>
```

- 方法 2:

<Switch> cd seclog

<Switch> undelete startup.cfg

```
Undelete flash:/seclog/startup.cfg? [Y/N]:y
Undeleting file flash:/seclog/startup.cfg... Done.
```

目次

このセクションのページは **1-x-x** です。

7章 コンフィグレーションファイル管理..... 7-1
7.1 コンフィグレーションファイル管理設定コマンド..... 7-1
7.1.1 backup startup-configuration 7-1
7.1.2 display current-configuration..... 7-2
7.1.3 display current-configuration diff 7-3
7.1.4 display default-configuration 7-5
7.1.5 display diff..... 7-5
7.1.6 display saved-configuration 7-7
7.1.7 display startup 7-8
7.1.8 display this 7-9
7.1.9 reset saved-configuration 7-10
7.1.10 restore startup-configuration 7-12
7.1.11 save.....7-13
7.1.12 startup saved-configuration 7-15

7章 コンフィグレーションファイル管理

7.1 コンフィグレーションファイル管理設定コマンド

7.1.1 backup startup-configuration

Syntax

backup startup-configuration to *ipv4-server* [*dest-filename*]

View

User view

定義済みユーザロール

network-admin

パラメータ

ipv4-server: IPv4 アドレスあるいはホスト名で TFTP サーバを指定します。ホスト名の設定範囲は 1～253 です。大文字、小文字を区別しません。ホスト名で使用できる文字列は文字、数字、ハイフン（-）、アンダーライン（-）、ドット（.）です。

dest-filename: サーバの次回起動時に使用する起動コンフィグレーションファイルを保存するためのターゲットファイル名を指定します。拡張子を除くファイル名の設定範囲は 1～255 です。ファイル名の拡張子は”.cfg”です。ターゲットファイル名を指定しない場合、ソースファイル名が使用されます。

説明

backup startup-configuration コマンドは TFTP サーバに次回の起動に使用する起動コンフィグレーションファイルをバックアップします。

例

TFTP サーバ 2.2.2.2 に次回の起動に使用する起動コンフィグレーションファイル 192-168-1-26.cfg をバックアップします。

<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.
```

関連コマンド

restore startup-configuration

7.1.2 display current-configuration

Syntax

display current-configuration [[**configuration** [*module-name*] | **interface** [*interface-type* [*interface-number*]]]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

configuration [*module-name*]: 機能の設定を表示します。*module-name* は機能モジュールを指定します。指定されない場合、設定されたすべての機能を表示します。有効な機能モジュールは装置の設定に依存します。

interface [*interface-type* [*interface-number*]]: インタフェースの設定を表示します。*interface-type* はインタフェースタイプで、*interface-number* はインタフェース番号を示します。*interface-type interface-number* パラメータを指定しない場合、すべてのインタフェースの現在の有効な設定を表示します。*interface-type* パラメータを指定した場合、指定したタイプのすべてのインタフェースの現在の有効な設定を表示します。

説明

display current-configuration コマンドは現在の有効な設定を表示します。

このコマンドを使用して、設定の確認を行うことができます。

システムは自動的にパラメータの設定を変更します。たとえば、システムの制限に合わない設定がある場合、自動的に変更します。設定が変更されると、システムの制限に適合した設定を表示します。

デフォルトの設定を使用しないパラメータは表示されません。

例

ローカルユーザの設定を表示します。

<Switch> display current-configuration configuration local-user

```
#
local-user ftp
 password                                                        hash
$h$6$Twd73mLrN8O2vvD5$Cz1vgdpR4KoTiRQNE9pg33gU14Br2p1VguczLSVyJLO2huV5Syx/LfD
If8ROLtVErJ/C31oq2rFtmNuyZf4STw==
 service-type ftp
 authorization-attribute user-role network-operator
```

```
#
local-user root
 password                                                                hash
$h$6$Twd73mLrN8O2vvD5$Cz1vgdpR4KoTiRQNE9pg33gU14Br2p1VguczLSVyJLO2huV5Syx/LfD
If8ROLtVErJ/C31oq2rFtmNuyZf4STw==
 service-type ssh telnet terminal
 authorization-attribute user-role network-admin
#
return
```

VLAN インタフェースの設定を表示します。

<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

Syntax

display current-configuration diff

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display current-configuration diff コマンドは現在のコンフィグレーションファイルと次回の起動に使用するコンフィグレーションファイル間の差分の設定を表示します。

例

現在のコンフィグレーションファイルと次回の起動に使用するコンフィグレーションファイル間の差分の設定を表示します。

<Switch> display current-configuration diff

```
--- Startup configuration
+++ Current configuration
@@ -17,7 +17,9 @@
```

```
 #
 vlan 200
 #
-vlan 300
+vlan 400
+#
+vlan 500
 #
<Switch>
```

出力では現在のコンフィグレーションファイルには VLAN 400、VLAN 500 が設定され、次回の起動に使用するコンフィグレーションファイルには VLAN 300 が含まれていることを示します。

表 7-1 コマンド出力

フィールド	説明
--- Startup configuration +++ Current configuration	---は比較元のコンフィグレーションファイルです。 +++は比較先のコンフィグレーションファイルです。
@@ *-linenumber1,number1* *+linenumber2,number2* @@	異なるコマンドラインの位置の概要です。 ● *-linenumber1*ー次回の起動に使用するコンフィグレーションファイルの異なるコマンドラインのライン番号です。 ● *+linenumber2*ー現在のコンフィグレーションファイルの異なるコマンドラインのライン番号です。 ● *number1*ー比較のため、次回の起動に使用するコンフィグレーションファイルからラインを抜粋した総数です。このラインによって相違の位置をより素早く突き止めることができます。 ● *number2*ー比較のため、現在のコンフィグレーションファイルからラインを抜粋した総数です。このラインによって相違の位置をより素早く突き止めることができます。
- cmd *+ cmd*	比較したコンフィグレーションファイルのコマンドラインの違いです。 ● 次回の起動に使用するコンフィグレーションファイルのコマンドラインはハイフン（-）で表示します。 ● 現在のコンフィグレーションファイルのコマンドラインはプラス（+）で表示します。

関連コマンド

- **display current-configuration**
- **display diff**
- **display saved-configuration**

7.1.4 display default-configuration

Syntax

display default-configuration

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display default-configuration コマンドは工場出荷状態のデフォルトコンフィグレーション設定を表示します。

工場出荷状態のコンフィグレーションはデフォルトコンフィグレーションファイルにあります。製品仕様のデフォルト設定は初期設定と異なります。設定ファイルがない場合あるいは設定ファイルが壊れている場合、デフォルト設定によって装置が起動し、正常に動作するようにします。

例

デフォルトコンフィグレーション設定を表示します。

<Switch> display default-configuration

7.1.5 display diff

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** }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

configfile *file-name-s*: 比較元のコンフィグレーションファイルを指定します。

configfile *file-name-d*: 比較先のコンフィグレーションファイルを指定します。

current-configuration: 現在のコンフィグレーションファイルを指定します。**display diff current-configuration** コマンドにおいて、このパラメータは、比較元のコンフィグレーションファイルを指定します。他の 2 つの **display diff** コマンドにおいて、このパラメータは比較先のコンフィグレーションファイルを指定します。

startup-configuration: 次回の起動に使用するコンフィグレーションファイルを指定します。**display diff startup-configuration** コマンドにおいて、このパラメータは比較元のコンフィグレーションファイルを指定します。他の 2 つの **display diff** コマンドにおいて、このパラメータは比較先のコンフィグレーションファイルを指定します。

説明

display diff コマンドは 2 つのコンフィグレーションファイルの設定の相違を表示します。

例

startup.cfg と test.cfg の設定の相違を表示します。

<Switch> display diff configfile startup.cfg configfile test.cfg

```
--- flash:/startup.cfg
+++ flash:/test.cfg
@@ -17,7 +17,9 @@
 #
 vlan 200
 #
-vlan 300
+vlan 400
+#
+vlan 500
 #
<Switch>
```

出力では、test.cfg は VLAN 400、VLAN 500 が含まれますが、startup.cfg は VLAN 300 が含まれます。

現在のコンフィグレーションファイルと次回の起動に使用するコンフィグレーションファイルの設定の相違を表示します。

<Switch> display diff current-configuration startup-configuration

```
--- Current configuration
+++ Startup configuration
@@ -17,9 +17,7 @@
 #
 vlan 200
```

```
 #
-vlan 400
-#
-vlan 500
+vlan 300
 #
<Switch>
```

出力では現在のコンフィグレーションファイルには VLAN 400、VLAN 500 が設定され、次回の起動に使用するコンフィグレーションファイルには VLAN 300 が含まれていることを示します。

出力の詳細は表 7-1 を参照してください。

関連コマンド

- **display current-configuration**
- **display current-configuration diff**
- **display saved-configuration**

7.1.6 display saved-configuration

Syntax

display saved-configuration

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display saved-configuration コマンドは装置が次回に起動に使用するために保存されているコンフィグレーションファイルの内容を表示します。

このコマンドは、装置の次回に起動するときに使用できるように重要な設定がコンフィグレーションファイルに保存されているかどうかを確認することができます。

以下の順番でコンフィグレーションファイルを選択します。

1) メインのコンフィグレーションファイルが有効である場合、メインのコンフィグレーションファイルの内容を表示します。
2) バックアップのコンフィグレーションファイルが有効である場合、バックアップのコンフィグレーションファイルの内容を表示します。

3) メインのコンフィグレーションファイルとバックアップのコンフィグレーションファイルが有効でない場合、何も表示されません。

例

次回に起動するコンフィグレーションファイルの内容を表示します。

<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 ----
```

関連コマンド

- **reset saved-configuration**
- **save**

7.1.7 display startup

Syntax

display startup

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display startup コマンドは現在のスタートアップコンフィグレーションファイルと次回に起動するコンフィグレーションファイルの名前を表示します。

すべての IRF スタックのメンバは Master と同一の現在のスタートアップコンフィグレーションファイルを使用します。

Master とメンバの切り替えが行われた後、現在のスタートアップコンフィグレーションファイルの名前は **NULL** と表示されます。これはスタートアップコンフィグレーションファイルで再起動するのではなく、新しい Master は現在の設定で動作し続けるためです。

例

スタートアップコンフィグレーションファイルの名前を表示します。

<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
```

表 7-2 コマンド出力

フィールド	説明
Current startup saved-configuration file	装置が起動した際のコンフィグレーションファイルです。
Next main startup saved-configuration file	次回起動する際に使用するメインコンフィグレーションファイルです。
Next backup startup saved-configuration file	次回起動する際に使用するバックアップコンフィグレーションファイルです。

関連コマンド

startup saved-configuration

7.1.8 display this

Syntax

display this

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display thisコマンドは現在の view の有効な設定を表示します。

現在の view で行った設定を確認するために使用します。

このコマンドはデフォルト設定のパラメータは表示されません。

パラメータに関する機能が無効であったとしても、パラメータを設定することができます。これらのパラメータは機能が有効になったのち、表示されます。

すべての line view でこのコマンドを使用すると、すべてのラインインタフェースで有効な設定情報を表示します。

例

VLAN インタフェース 1 で有効な設定を表示します。

<Switch> system-view

[Switch] interface vlan-interface 1

[Switch-Vlan-interface1] display this

```
#
interface Vlan-interface1
#
return
```

7.1.9 reset saved-configuration

Syntax

reset saved-configuration [**backup** | **main**]

View

User view

定義済みユーザロール

network-admin

パラメータ

backup: バックアップの次回の起動時に使用するコンフィグレーションファイルを削除します。

main: メインの次回の起動時に使用するコンフィグレーションファイルを削除します。

説明

注意:

すべての IRF スタックのメンバ装置から次回の起動時に使用するコンフィグレーションファイルを完全に削除します。IRF スタック装置で使用する場合には注意が必要です。

reset saved-configuration コマンドは次回の起動時に使用するコンフィグレーションファイルを削除します。

メイン、バックアップ、あるいは両方の次回の起動時に使用するコンフィグレーションファイルを削除することができます。

ソフトウェアバージョンが一致していない、あるいはコンフィグレーションファイルが壊れている場合、次回の起動時に使用するコンフィグレーションファイルを削除します。

メインとバックアップの次回の起動時に使用するコンフィグレーションファイルを削除するため、**reset saved-configuration backup** コマンドと **reset saved-configuration main** コマンドの両方を実行する必要があります。コマンドの一方を削除することで、ファイルの削除の代わりに指定したファイルの属性を削除することができます。

たとえば、**reset saved-configuration backup** コマンドが実行されるとバックアップの次回の起動時に使用するコンフィグレーションファイルは NULL に設定されます。しかしファイルはメインファイルとして使用されます。ファイルを削除するために、**reset saved-configuration main** コマンドを実行する必要があります。

コンフィグレーションファイルの属性が指定されていない場合、**reset saved-configuration** コマンドはメインの次回の起動時に使用するコンフィグレーションファイルを削除します。

例

メインの次回の起動時に使用するコンフィグレーションファイルを削除します。

<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.
```

関連コマンド

display saved-configuration

7.1.10 restore startup-configuration

Syntax

restore startup-configuration from *ipv4-server src-filename*

View

User view

定義済みユーザロール

network-admin

パラメータ

ipv4-server: IPv4 アドレスあるいはホスト名で TFTP サーバを指定します。ホスト名の設定範囲は 1～253 です。大文字、小文字を区別しません。ホスト名で使用できる文字列は文字、数字、ハイフン（-）、アンダーライン（-）、ドット（.）です。

src-filename: ダウンロードされたコンフィグレーションファイルのファイル名を指定します。拡張子を除くファイル名の設定範囲は 1～255 です。ファイル名の拡張子は”.cfg”です。

説明

restore startup-configuration コマンドは指定した TFTP サーバからコンフィグレーションファイルをダウンロードし、次回の起動時に使用するコンフィグレーションファイルとして指定します。

次回の起動時に使用するコンフィグレーションファイルを指定する前に、以下の要件を確認してください。

- サーバが到達可能です。
- サーバが TFTP サービスを有効にしています。
- サーバへの読み込み、書き込み許可があります。

このコマンドは、メインの次回の起動時に使用するコンフィグレーションファイルの復旧を自動で行うことで、コンフィグレーションファイルの復旧を簡単に行うことができます。

各メンバ装置の記憶媒体のルートディレクトリにコンフィグレーションファイルをダウンロードします。同時にメインの次回の起動時に使用するコンフィグレーションファイルとしてファイルを指定します。

このコマンドは、すべての IRF スタックメンバが同一タイプの記憶媒体を使うと仮定します。メンバ装置がマスタ装置と異なるタイプの記憶媒体を使用する場合、コマンドはメンバ装置にコンフィグレーションファイルを回復することができません。

たとえば、メンバ装置で USB メモリを使用し、マスタ装置でフラッシュメモリを使用すると仮定します。この場合、メンバ装置上に手動で次回の起動時に使用するスタートアップコンフィグレーションファイルを復旧しなければなりません。

例

TFTP サーバ 2.2.2.2 からコンフィグレーションファイル test.cfg をダウンロードし、次回の起動時に使用するコンフィグレーションファイルとして指定します。

<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.
```

関連コマンド

backup startup-configuration

7.1.11 save

Syntax

save *file-url* [**all** | **slot** *slot-number*]

save [**safely**] [**backup** | **main**] [**force**]

View

すべての view

定義済みユーザロール

network-admin

パラメータ

file-url: 稼働中の設定を指定したファイルに保存します。次回に起動するコンフィグレーションファイルとして指定しません。ファイルの拡張子は”.cfg”で、パス情報を含むことができます。拡張子を除くファイル名の設定範囲は 1～255 です。**all** パラメータあるいはメンバ ID が指定された場合、ファイルのパスはメンバ ID を含むことができません。ファイルのパスがフォルダ名を含む場合、フォルダはすでに存在する必要があります。

all: すべてのメンバ装置に稼働中の設定を保存します。パラメータを指定しないあるいは **slot** *slot-number* パラメータを指定しない場合、Master 装置のみ稼働中の設定を保存します。

slot *slot-number*: 稼働中の設定をメンバ装置に保存します。*slot-number* は装置の IRF スタックのメンバ ID を示します。このパラメータあるいは all パラメータを指定しない場合、Master 装置のみ稼働中の設定を保存します。

safely: safe モードでコンフィグレーションファイルを保存します。このパラメータを指定しない場合、装置は fast モードでコンフィグレーションファイルを保存します。safe モードは fast モードよりも保存に要する時間が遅くなりますが、安全に行うことができます。

backup: 稼働中の設定を指定したファイルに保存し、バックアップの次回に起動するコンフィグレーションファイルとして指定します。**backup** パラメータあるいは **main** パラメータを指定しない場合、保存したファイルをメインの次回に起動するコンフィグレーションファイルに指定します。

main: 稼働中の設定を指定したファイルに保存し、メインの次回に起動するコンフィグレーションファイルとして指定します。**main** パラメータあるいは **backup** パラメータを指定しない場合、保存したファイルをメインの次回に起動するコンフィグレーションファイルに指定します。

force: 稼働中の設定を確認の表示を行わずに保存します。このパラメータを指定しない場合、操作を実行する際に確認メッセージが表示されます。30 秒以内に操作を行わない場合、システムは自動で操作を中止します。30 秒以内に"Y"を入力すると、保存処理を継続し、処理中のターゲットファイル名を変更することができます。

説明

save *file-url* [**all** | **slot** *slot-number*]コマンドは稼働中の設定をコンフィグレーションファイルに保存します。次回に起動するコンフィグレーションファイルとして指定しません。

save [**safely**] [**backup** | **main**] [**force**]コマンドは記憶媒体のルートディレクトリのファイルに稼働中の設定を保存します。このコマンドは各メンバ装置に適用します。次回に起動するコンフィグレーションファイルとして自動的に指定します。

このコマンドで指定されたファイルが存在しない場合、設定を保存する前、システムはファイルを作成します。すでにファイルが存在する場合、システムはファイルを上書きするかどうか確認メッセージを表示します。ファイルを上書きしない場合、システムは **save** コマンドの操作を中止します。

コマンドの *file-url* パラメータを指定しない場合､コマンドはテキストファイル”.cfg”と、バイナリファイル”.mdb”に稼働中の設定を保存します。2 つのファイルは同一ファイル名です。バイナリファイル”.mdb”はテキストファイル”.cfg”よりも保存に要する時間が短くなります。

save [**safely**] [**backup** | **main**] [**force**]コマンドを使用した場合、以下のガイドラインに従ってください。

- safe モードでは、システムは一時ファイルに設定を保存し、保存が完了した後、ターゲットの次回の起動に使用するコンフィグレーションファイルの上書きを開始します。保存作業中に、再起動、電源の故障あるいはメモリ容量の不足が発生した場合、次回の起動に使用するコンフィグレーションファイルは保持されています。
- fast モードでは装置は直接、ターゲットの次回の起動に使用するコンフィグレーションファイルの上書きを開始します。存作業中に、再起動、電源の故障あるいはメモリ容量の不足が発生した場合、次回の起動に使用するコンフィグレーションファイルは消失します。

このコマンドを使用する場合、**safely** パラメータを使用することを推奨します。

例

稼働中の設定をコンフィグレーションファイル backup.cfg に保存し、次回に起動するコンフィグレーションファイルとして指定しません。

<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.
```

稼働中の設定をメインの次回の起動に使用するコンフィグレーションファイルに確認の表示を行わずに保存します。

<Switch> save force

```
Validating file. Please wait....
Saved the current configuration to mainboard device successfully.
```

稼働中の設定を記憶媒体のルートディレクトリのファイルに保存し、メインの次回の起動に使用するコンフィグレーションファイルとして指定します。

<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.
```

関連コマンド

- **display current-configuration**
- **display saved-configuration**

7.1.12 startup saved-configuration

Syntax

startup saved-configuration *cfgfile* [**backup** | **main**]

undo startup saved-configuration

デフォルト

設定なし

View

User view

定義済みユーザロール

network-admin

パラメータ

cfgfile: コンフィグレーションファイル”.cfg”の名前を指定します。”.cfg”ファイルはすでに記憶媒体のルートディレクトリに存在している必要があります。拡張子を除くファイル名の設定範囲は 1～255 です。ファイル名はファイル名のみ、あるいは記憶媒体＋ファイル名のどちらかを指定することができます。デフォルトの記憶媒体以外を指定する場合、記憶媒体の名前を指定する必要があります。

backup: コンフィグレーションファイルをバックアップの次回の起動に使用するコンフィグレーションファイルとして指定します。

main: コンフィグレーションファイルをメインの次回の起動に使用するコンフィグレーションファイルとして指定します。これは、装置が起動時に読み込みを行うメインのコンフィグレーションファイルです。読み込みに失敗した場合、装置はバックアップの次回の起動に使用するコンフィグレーションファイルの読み込みを行います。

説明

⚠ **注意:**

IRF スタックで **undo startup saved-configuration** コマンドを使用する場合は注意してください。IRF スタックあるいは IRF スタックメンバの再起動後に IRF スタックが分裂します。
IRF のメンバーID 設定は、**undo startup saved-configuration** コマンドでは変更されません。

---

startup saved-configuration コマンドは、ファイルをすべての IRF スタックのメンバ装置の次回の起動に使用するコンフィグレーションファイルとして指定します。

IRF スタックでは、**startup saved-configuration** コマンドはすべての IRF スタックのメンバに適用します。コマンドを設定するため、各メンバ装置の記憶媒体のルートディレクトリに指定されたファイルがすでに存在していることを確認します。

backup パラメータあるいは **main** パラメータの両方とも指定されていない場合、**startup saved-configuration** コマンドはメインの次回の起動に使用するコンフィグレーションファイルとして指定します。

メインとバックアップのコンフィグレーションファイルを同一にすることができます。また高可用性のため、複数のコンフィグレーションファイルを指定することができます。

undo startup saved-configuration コマンドはメインとバックアップの次回の起動に使用するコンフィグレーションファイルを未指定の状態に変更します。なお、本コマンド実行時に、既存のコンフィグレーションファイルは削除しません。

save コマンドで稼働中の設定を保存したとき、次回の起動に使用するコンフィグレーションファイルとして設定することができます。

例

メインの次回の起動に使用するコンフィグレーションファイルを指定します。

<Switch> startup saved-configuration testcfg.cfg

```
Please wait ....... Done.
```

関連コマンド

display startup

目次

このセクションのページは **1-x-x** です。

8 章 ソフトウェア管理 8-1
8.1 ソフトウェア管理設定コマンド 8-1
8.1.1 boot-loader file 8-1
8.1.2 bootrom update 8-4
8.1.3 display boot-loader 8-5

8章 ソフトウェア管理

8.1 ソフトウェア管理設定コマンド

8.1.1 boot-loader file

Syntax

boot-loader file boot *filename* **system** *filename* { **all** | **slot** *slot-number* } { **backup** | **main** }

boot-loader file *ipe-filename* { **all** | **slot** *slot-number* } { **backup** | **main** }

View

User view

定義済みユーザロール

network-admin

パラメータ

boot *filename*: Boot イメージファイル.bin のファイルパスを指定します。大文字、小文字を区別しません。ファイルはシステムの記憶媒体のルートディレクトリに格納されます。ファイルパスの記憶媒体:/ファイル名.bin セグメントの設定範囲は 1～63 文字です。この設定範囲には IRF スタックのメンバ ID あるいは記憶媒体の前のスロット番号が含まれません。ファイルパスの指定の詳細は、オペレーションマニュアルのセクション 1 の *はじめに*“*ファイルシステム管理*”を参照してください。

system *filename*: System イメージファイル.bin のファイルパスを指定します。大文字、小文字を区別しません。ファイルはシステムの記憶媒体のルートディレクトリに格納されます。ファイルパスの記憶媒体:/ファイル名.bin セグメントの設定範囲は 1～63 文字です。この設定範囲には IRF スタックのメンバ ID あるいは記憶媒体の前のスロット番号が含まれません。ファイルパスの指定の詳細は、オペレーションマニュアルのセクション 1 の *はじめに*“*ファイルシステム管理*”を参照してください。

ipe-filename: イメージパッケージファイル.ipe のファイルパスを指定します。大文字、小文字を区別しません。ファイルはシステムの記憶媒体のルートディレクトリに格納されます。ファイルパスの記憶媒体:/ファイル名.ipe セグメントの設定範囲は 1～63 文字です。この設定範囲には IRF スタックのメンバ ID あるいは記憶媒体の前のスロット番号が含まれません。ファイルパスの指定の詳細は、オペレーションマニュアルのセクション 1 の *はじめに*“*ファイルシステム管理*”を参照してください。

all: すべてのハードウェア構成の次回の起動に使用するイメージファイルを指定します。

slot *slot-number*: 次回の起動に使用するイメージが指定された装置の IRF スタックのメンバ ID を指定します。

backup: バックアップの次回の起動に使用するファイルを指定します。バックアップの次回の起動に使用するイメージファイルはメインの次回の起動に使用するイメージファイルが有効でないときのみ使用されます。

main: メインの次回の起動に使用するファイルを指定します。装置は起動時には常にメインの次回の起動に使用するファイルで起動を行います。

説明

boot-loader file コマンドは次回の起動に使用するソフトウェアイメージファイルを指定します。

次回の起動に使用するソフトウェアイメージファイルを読み込む場合、システムの再起動が必要です。

このコマンドは、各メンバ装置のソフトウェアイメージをアップグレードするために使用します。

次回の起動に使用するソフトウェアイメージファイルを指定する前に、以下の作業を行ってください。

- IRF スタックの記憶媒体のルートディレクトリにアップグレードファイルを保存してください。

  アップグレードする IRF スタックのメンバのフラッシュメモリにシステムはアップグレードファイルを自動的にコピーします。アップグレードファイルと同じ名前のファイルがすでに存在する場合、ファイルを上書きするかどうか選択する必要があります。

アップグレードのために”.ipe”イメージパッケージファイルを使用する場合、システムがファイルを解凍した後にファイルを削除するかどうかを選択する必要があります。

boot-loader file コマンドはすべての次回の起動に使用するソフトウェアイメージリストを上書きします。

例

IRF スタックのメンバ ID1 のバックアップの次回の起動に使用するソフトウェアイメージファイルとして flash:/all.ipe を指定します。

<Switch> boot-loader file flash:/all.ipe slot 1 main

```
Verifying the IPE file and the images.............Done.
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.
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.
```

IRF スタックのすべてのメンバ装置のメインの次回の起動に使用するソフトウェアイメージファイルとして flash:/all.ipe を指定します。

```
<Switch> boot-loader file slot4#flash:/all.ipe all main
Verifying the the file flash:/all.ipe on slot
1.............................Done.
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
```

関連コマンド

display boot-loader

8.1.2 bootrom update

Syntax

bootrom update file *file* **slot** *slot-number-list*

View

User view

定義済みユーザロール

network-admin

パラメータ

file *file*: フラッシュの Boot ROM イメージが含まれるファイルを指定します。設定範囲は 1～63 です。

slot *slot-number-list*: IRF スタックのメンバ装置のメンバ ID を半角スペースで区切って 7 つまで指定します。各アイテムはメンバ ID で IRF スタックのメンバ装置を指定するか、*start-member-id* **to** *end-member-id* の形式で IRF スタックのメンバ装置の範囲を指定します。*end-member-id* は *start-member-id* 以上の値にしてください。たとえば、**slot** 0 **to** 1 2 です。

説明

bootrom update コマンドはフラッシュの Boot ROM イメージを、Boot ROM の通常エリアに読み込みます。

ソフトウェアアップグレードを行う際、Boot ROM イメージのアップグレードが必要な場合、Comware イメージ（Boot イメージと System ソフトウェアイメージ）をアップグレードする前に、このコマンドを使用して Boot ROM に新しい Boot ROM イメージをアップグレードします。このコマンドは、予期しない電気的な故障によってアップグレードの失敗が発生するリスクを減少させ、アップグレードを行う時間を削減することができます。

アップグレードを完了させるために、装置を再起動します。

例

フラッシュメモリのルートディレクトリにあるファイル a.bin を使用して、Boot ROM イメージをアップグレードします。

<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.
```

関連コマンド

boot-loader file

8.1.3 display boot-loader

Syntax

display boot-loader [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

slot *slot-number*: IRF スタック装置のメンバ ID を指定します。メンバ装置が指定されない場合、各 IRF スタック装置のソフトウェアイメージを表示します。

説明

display boot-loader コマンドは現在のソフトウェアイメージと次回の起動に使用するソフトウェアイメージを表示します。

例

現在のソフトウェアイメージと次回の起動に使用するソフトウェアイメージを表示します。

<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
```

表 8-1 コマンド出力

フィールド	説明
Current software images	Comwareイメージが読み込まれました。
Main startup software images	次回の起動に使用するメインのComwareイメージです。
Backup startup software images	次回の起動に使用するバックアップのComwareイメージです。

関連コマンド

boot-loader file

目次

このセクションのページは **1-x-x** です。

9 章 装置管理 9-1
9.1 装置管理設定コマンド 9-1
9.1.1 clock datetime 9-1
9.1.2 clock protocol 9-2
9.1.3 clock summer-time 9-3
9.1.4 clock timezone 9-5
9.1.5 command 9-6
9.1.6 copyright-info enable 9-7
9.1.7 display clock 9-8
9.1.8 display cpu-usage 9-9
9.1.9 display cpu-usage configuration 9-10
9.1.10 display cpu-usage history 9-11
9.1.11 display device 9-13
9.1.12 display device manuinfo 9-14
9.1.13 display device manuinfo power 9-15
9.1.14 display diagnostic-information 9-15
9.1.15 display environment 9-17
9.1.16 display fan 9-18
9.1.17 display memory 9-19
9.1.18 display memory-threshold 9-21
9.1.19 display power 9-22
9.1.20 display scheduler job 9-23
9.1.21 display scheduler logfile 9-24
9.1.22 display scheduler reboot 9-25
9.1.23 display scheduler schedule 9-25
9.1.24 display transceiver interface 9-27
9.1.25 display version 9-29
9.1.26 header 9-29
9.1.27 job 9-30
9.1.28 locator blink 9-31
9.1.29 memory-threshold 9-32
9.1.30 monitor cpu-usage enable 9-33
9.1.31 monitor cpu-usage interval 9-35
9.1.32 monitor cpu-usage threshold 9-36
9.1.33 monitor resend cpu-usage 9-37
9.1.34 monitor resend memory-threshold 9-38

9.1.35 password-recovery enable 9-39
9.1.36 reboot 9-40
9.1.37 reset scheduler logfile 9-42
9.1.38 scheduler job 9-43
9.1.39 scheduler logfile size 9-44
9.1.40 scheduler reboot at 9-45
9.1.41 scheduler reboot delay 9-46
9.1.42 scheduler schedule 9-47
9.1.43 shutdown-interval 9-48
9.1.44 sysname 9-49
9.1.45 temperature-limit 9-50
9.1.46 time at 9-53
9.1.47 time once 9-54
9.1.48 time repeating 9-56
9.1.49 user-role 9-58

9章 装置管理

9.1 装置管理設定コマンド

9.1.1 clock datetime

Syntax

clock datetime *time date*

デフォルト

UTC 時間で 2013 年 1 月 1 日の 00:00:00

View

User view

定義済みユーザロール

network-admin

パラメータ

time: 設定時刻（形式は *hh:mm:ss* （時/分/秒））を指定します。*hh* の設定範囲は 0～23 です。*mm* の設定範囲は 0～59 です。*ss* の設定範囲は 0～59 です。*hh, mm, ss* において最初の 0 は省略可能です。*ss* が 00 の場合 *hh:mm* で表し、*mm* と *ss* が 00 の場合 *hh* で示します。たとえば 08:00:00 を指定する場合、*hh* に 8 を設定できます。

date: 現在の日付（形式は *MM/DD/YYYY* あるいは *YYYY/MM/DD*）を指定します。*MM* は 1～12 の月、*DD* は各月の日付、*YYYY* は 2000～2035 の年です。

説明

clock datetime コマンドは、装置の現在の日時を設定します。

正しいシステムクロックの設定はネットワーク管理と通信に不可欠です。ネットワークで装置を動作させる前に、装置のシステム時間を設定してください。

装置は **clock protocol none** コマンドでローカルシステム時間を使用し、**clock datetime** コマンドを実行することで現在の日時を設定します。**clock datetime** コマンドを設定すると即座に適用されます。装置はシステム時間を維持するため、装置内部の水晶発振器によって生成されたクロック周波数を使用します。

装置の再起動を行うとローカルシステム時間はデフォルトに戻るため、再度コマンドを設定してください。

例

装置の現在の日時を UTC 時間で 08:08:08 01/01/2015 に設定します。

<Switch> clock datetime 8:8:8 1/1/2015

装置の現在の日時を UTC 時間で 08:10:00 01/01/2015 に設定します。

<Switch> clock datetime 8:10 2015/1/1

関連コマンド

- **clock protocol**
- **clock summer-time**
- **clock timezone**
- **display clock**

9.1.2 clock protocol

Syntax

clock protocol { **none** | **ntp** }

undo clock protocol

デフォルト

ntp

View

System view

定義済みユーザロール

network-admin

パラメータ

none: **clock datetime** コマンドを使用したローカルシステム時間です。

ntp: NTP クロックソースです。装置が NTP のシステムクロックを使用したとき、手動でシステムクロックを変更できません。NTP の詳細はオペレーションマニュアルのセクション 11 *システム管理*”*NTP*”を参照してください。

説明

clock protocol コマンドはシステムクロックソースを指定します。

undo clock protocol コマンドはデフォルトに戻します。

正しいシステムクロックの設定はネットワーク管理と通信に不可欠です。ネットワークで装置を動作させる前に、装置のシステム時間を設定してください。

システムクロックソースがローカルシステム時間である場合、システム時間は以下の値によって変更します。

- タイムゾーン
- UTC 時間

- サマータイム

装置は以下のどちらかの方法でシステム時間を設定します。

- ローカルシステム時間を使用します。
- NTP を使用して信頼されたクロックソースから UTC 時間を取得し、システム時間を計算します。

複数コマンドを設定した場合、最後に指定した設定が適用されます。

例

ローカルシステム時間を使用するように設定します。

<Switch> system-view

[Switch] clock protocol none

9.1.3 clock summer-time

Syntax

clock summer-time *name start-time start-date end-time end-date add-time*

undo clock summer-time

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

パラメータ

name: サマータイム名を指定します。設定範囲は 1～32 文字です。

start-time: 開始時刻を指定します。形式は *hh:mm:ss* （時/分/秒）です。*hh* の設定範囲は 0～23 です。mm の設定範囲は 0～59 です。ss の設定範囲は 0～59 です。*hh, mm, ss* において最初の 0 は省略可能です。*ss* が 00 の場合 *hh:mm* で表し、*mm* と *ss* が 00 の場合 *hh* で示します。たとえば 08:00:00 を指定する場合、*hh* に 8 を設定できます。

start-date: 開始日を以下の形式の 1 つで指定します。

- *MM*/*DD*：*MM* の設定範囲は 1～12 です。*DD* の設定範囲は月によって変わります。
- *month week date*
  - **month**−月を指定します。January、February、March、April、May、June、July、August、September、October、November、December が指定できます。

- **week**−月で開始する週を指定します。first、second、third、fourth、fifth、last が指定できます。
- **day**−日を指定します。Sunday、Monday、Tuesday、Wednesday、Thursday、Friday、Saturday が指定できます。

end-time: 終了時刻を指定します。形式は *hh:mm:ss* （時/分/秒）です。*hh* の設定範囲は 0～23 です。mm の設定範囲は 0～59 です。ss の設定範囲は 0～59 です。*hh, mm, ss* において最初の 0 は省略可能です。*ss* が 00 の場合 *hh:mm* で表し、*mm* と *ss* が 00 の場合 *hh* で示します。たとえば 08:00:00 を指定する場合、*hh* に 8 を設定できます。

end-date: 終了日を以下の形式の 1 つで指定します。

- *MM*/*DD*：*MM* の設定範囲は 1～12 です。*DD* の設定範囲は月によって変わります。
- *month week date*
  - **month**−月を指定します。January、February、March、April、May、June、July、August、September、October、November、December が指定できます。
  - **week**−月で開始する週を指定します。first、second、third、fourth、fifth、last が指定できます。
  - **day**−日を指定します。Sunday、Monday、Tuesday、Wednesday、Thursday、Friday、Saturday が指定できます。

add-time: 標準時刻に追加する時間です。形式は *hh:mm:ss* （時/分/秒）です。*hh* の設定範囲は 0～23 です。mm の設定範囲は 0～59 です。ss の設定範囲は 0～59 です。*hh, mm, ss* において最初の 0 は省略可能です。*ss* が 00 の場合 *hh:mm* で表し、*mm* と *ss* が 00 の場合 *hh* で示します。たとえば 08:00:00 を指定する場合、*hh* に 8 を設定できます。

説明

clock summer-time コマンドは指定した期間、サマータイムを使用するために設定します。

undo clock summer-time コマンドは設定を解除します。

正しいシステムクロックの設定はネットワーク管理と通信に不可欠です。ネットワークで装置を動作させる前に、装置のシステム時間を設定してください。

サマータイムを設定したのち、装置はシステム時間を再計算します。システムクロックを確認する場合 **display clock** コマンドを使用します。

ローカルシステム時間を使用する場合、ネットワークのすべての装置で同一のサマータイムを使用していることを確認してください。

例

08/01 の 06:00:00 から 09/01 の 06:00:00 の間、システムの時計を 1 時間進めます。

<Switch> system-view

[Switch] clock summer-time PDT 6 08/01 6 09/01 1

関連コマンド

- **clock datetime**
- **clock timezone**

- **display clock**

9.1.4 clock timezone

Syntax

clock timezone *zone-name* { **add** | **minus** } *zone-offset*

undo clock timezone

デフォルト

UTC 時間

View

System view

定義済みユーザロール

network-admin

パラメータ

zone-name: タイムゾーン名を指定します。範囲は 1～32 文字で、大文字、小文字を区別します。

add: UTC 時間（協定世界時 : universal time coordinated）に対する正（+）のオフセットです。

minus: UTC 時間に対する負（-）のオフセットです。

zone-offset: UTC 時間に対するオフセットです。形式は *hh:mm:ss* （時/分/秒）です。*hh* の設定範囲は 0～23 です。mm の設定範囲は 0～59 です。ss の設定範囲は 0～59 です。*hh, mm, ss* において最初の 0 は省略可能です。*ss* が 00 の場合 *hh:mm* で表し、*mm* と *ss* が 00 の場合 *hh* で示します。たとえば 08:00:00 を指定する場合、*hh* に 8 を設定できます。

説明

clock timezone コマンドはローカルタイムゾーンを設定します。

undo clock timezone コマンドはデフォルトに戻します。

正しいシステムクロックの設定はネットワーク管理と通信に不可欠です。ネットワークで装置を動作させる前に、装置のシステム時間を設定してください。

タイムゾーンを設定したのち、装置はシステム時間を再計算します。システムクロックを確認する場合 **display clock** コマンドを使用します。

ローカルシステム時間を使用する場合、ネットワークのすべての装置で同一のタイムゾーンを使用していることを確認してください。

例

UTC より 5 時間進めたローカルタイムゾーン名を Z5 に設定します。

<Switch> system-view

[Switch] clock timezone Z5 add 5

関連コマンド

- **clock datetime**
- **clock summer-time**
- **display clock**

9.1.5 command

Syntax

command *id command*

undo command *id*

デフォルト

設定なし

View

Job view

定義済みユーザロール

network-admin

パラメータ

id: コマンドの ID を指定します。設定範囲は 0～4294967295 です。コマンドの ID は job を一意に識別します。job のコマンドは昇順で実行されます。

command: job に割り当てられたコマンドを指定します。

説明

command コマンドは job にコマンドを割り当てます。

undo command コマンドを取り消します。

command コマンドが存在するコマンドの ID を使用する場合、存在するコマンドは置き換わります。

job にコマンドを割り当てる場合、最初にコマンドの view に移行してください。

command コマンドが存在するコマンドの ID を使用する場合、存在するコマンドは置き換わります。

スケジュール自動実行を行う場合、実行する view と *command* のパラメータをチェックしません。*command* のパラメータを正確に設定してください。コマンドの syntax が設定されているか、および正しい view に設定されているかどうかを含みます。そうでなければ、**command** コマンドは自動で実行することができません。

コマンドで Yes あるいは No の入力が必要な場合、システムは常に Y あるいは Yes が適用されます。コマンドで文字列の入力が必要な場合、システムはデフォルトの文字列あるいは Null が適用されます。

job は **telnet** コマンド、**ftp** コマンド、**ssh2** コマンドおよびモニタリングの設定を行うことができません。

例

job 名が backupconfig の job に、コンフィグレーションファイル startup.cfg を TFTP サーバ 192.168.100.11 にバックアップを行うコマンドを割り当てます。

<Switch> system-view

[Switch] scheduler job backupconfig

[Switch-job-backupconfig] command 2 tftp 192.168.100.11 put flash:/startup.cfg backup.cfg

job 名が shutdownGE の job に GigabitEthernet 1/0/1 をシャットダウンするコマンドを割り当てます。

<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

関連コマンド

scheduler job

9.1.6 copyright-info enable

Syntax

copyright-info enable

undo copyright-info enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

copyright-info enable コマンドは、著作権情報の表示を有効にします。

undo copyright-info enable コマンドは、著作権情報の表示を無効にします。

例

著作権情報の表示を有効にします。

<Switch> system-view

[Switch] copyright-info enable

9.1.7 display clock

Syntax

display clock

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display clock コマンドはシステムの現在時刻、日付、タイムゾーン、サマータイムを表示します。

例

ローカルタイムゾーンが指定されていないとき、システム時間を表示します。

<Switch> display clock

```
10:09:00 UTC Fri 03/16/2015
```

ローカルタイムゾーン Z5 が指定されているとき、システム時間を表示します。

<Switch> display clock

```
15:10:00 Z5 Fri 03/16/2015
Time Zone : Z5 add 05:00:00
```

ローカルタイムゾーン Z5 が指定され､サマータイム時間 JST が指定されているとき、システム時間を表示します。

<Switch> display clock

```
15:11:00 Z5 Fri 03/16/2015
Time Zone : Z5 add 05:00:00
Summer Time : JST 06:00:00 08/01 06:00:00 09/01 01:00:00
```

関連コマンド

- **clock datetime**
- **clock timezone**
- **clock summer-time**

9.1.8 display cpu-usage

Syntax

display cpu-usage [**slot** *slot-number* [**cpu** *cpu-number*]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

slot *slot-number*: メンバ ID によって IRF スタックのメンバ装置を指定します。もしこのパラメータが指定されない場合、すべての IRF スタックにあるメンバ装置の CPU 使用率の統計情報を表示します。

cpu *cpu-number*: CPU 番号を指定します。*cpu-number* は 0 で固定です。

説明

display cpu-usage コマンドは CPU 使用率の統計情報を表示します。

例

現在の CPU 使用率の統計情報を表示します。

<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
```

表 9-1 コマンド出力

フィールド	説明
x% in last 5 seconds	最後の5秒のCPU使用率の平均です。
y% in last 1 minute	最後の1分のCPU使用率の平均です。
z% in last 5 minutes	最後の5分のCPU使用率の平均です。

9.1.9 display cpu-usage configuration

Syntax

display cpu-usage configuration [**slot** *slot-number* [**cpu** *cpu-number*]]

View

すべての view

定義済みユーザロール

network-admin

パラメータ

slot *slot-number*: IRF スタックメンバをそのメンバ ID で指定します。メンバ装置を指定しない場合、このコマンドは Master 装置の CPU 使用率監視設定を表示します。

cpu *cpu-number*: CPU を番号で指定します。

説明

display cpu-usage configuration コマンドは CPU 使用率モニタリング設定を表示します。

例

CPU 使用率モニタリング設定を表示します。

<Switch> display cpu-usage configuration

```
CPU usage monitor is enabled.
Current monitor interval is 60 seconds.
Current severe alarm threshold is 99%.
Current minor alarm threshold is 98%.
Current recovery-threshold is 50%.
```

関連コマンド

- **monitor cpu-usage enable**
- **monitor cpu-usage interval**

- **monitor cpu-usage threshold**

9.1.10 display cpu-usage history

Syntax

display cpu-usage history [**job** *job-id*] [**slot** *slot-number* [**cpu** *cpu-number*]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

job *job-id*: job の ID のプロセスを指定します。設定範囲は 1～2147483647 です。指定しない場合、すべてのプロセスのシステム全体の CPU 使用率履歴の統計情報を表示します。

slot *slot-number*: メンバ ID によって IRF スタックのメンバ装置を指定します。指定しない場合、IRF スタックユニットの Master の CPU 使用率履歴の統計情報を表示します。

cpu *cpu-number*: CPU 番号を指定します。*cpu-number* は 0 で固定です。CPU を指定しない場合、デフォルト CPU の使用率履歴の統計情報を表示します。プロセスあるいは CPU を指定しない場合、すべての CPU 使用率履歴の統計情報を表示します。

説明

display cpu-usage history コマンドは表で CPU 使用率履歴の統計情報を表示します。

CPU 使用率のモニタリングが有効にされたのち、システムはある時間での CPU 使用率統計情報を取得し、履歴記録領域に統計結果を保存します。このコマンドは最後の 60 分間の CPU 使用率の統計情報レコードを座標で表示します。

- Y 座標は、CPU 使用率を示します。もし統計情報が使用率のステップの倍数でない場合、もっとも近いステップに切り下げあるいは切り上げされます。たとえば CPU 使用率のステップが 5%である場合、統計情報が 53%である場合 55%に切り上げされます。統計情報が 52%である場合、50%に切り下げられます。
- X 座標は時間を示します。
- シャープ（#）は、ある時点における CPU 使用率を示します。ある時点上で#マークが 1 つ以上あるとき、一番高い位置の#マークが、現時点での CPU 使用率です。

例

CPU 使用率履歴の統計情報を表示します。

<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)
```

出力では以下のアイテムを示します。

- プロセス名：SYSTEM（全システムを示します。）
- プロセスの CPU：スロット 1 の CPU 0
- 最後の 60 分間の CPU 使用率
  - 12 分前：5%
  - 13 分前：10%
  - 14 分前：15%
  - 15 分前：10%
  - 16 分前：5%
  - 17 分前：5%
  - 18 分前：10%
  - 19 分前：5%
  - その他の時間：2%または 2%未満

関連コマンド

- **monitor cpu-usage enable**
- **monitor cpu-usage interval**

9.1.11 display device

Syntax

display device [**slot** *slot-number* | **verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

slot *slot-number*: メンバ ID によって IRF スタックのメンバ装置を指定します。

verbose: 詳細なハードウェア情報を表示します。指定しない場合、概要情報を表示します。

説明

display device コマンドは装置情報を表示します。

例

装置情報を表示します。

<Switch> display device

```
Slot Type            State    Subslot  Soft Ver          Patch Ver
1    QX-S5148GT-4X    Master   0       7.1.1             None
```

表 9-2 コマンド出力

フィールド	説明
Type	装置のハードウェアタイプです。
State	IRFスタックユニットの装置の役割です。 ● **Master**—装置がマスタです。 ● **Standby**—装置がメンバです。
Soft Ver	ソフトウェアバージョンです。
Patch Ver	パッチバージョンです。この装置はパッチバージョンをサポートしていません。**None**と表示されます。

9.1.12 display device manuinfo

Syntax

display device manuinfo [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

slot *slot-number*: メンバ ID によって IRF スタックのメンバ装置を指定します。指定しない場合、すべての IRF スタックユニットのラベル情報を表示します。

説明

display device manuinfo コマンドは装置のラベル情報を表示します。

ラベル情報は、固定構成データまたはアーカイブ情報とも呼ばれており、デバック中あるいはテスト中に装置の記憶媒体に書き込まれます。装置のシリアル番号、製造日、MAC アドレス、ベンダ名を含む情報です。このコマンドは、装置のラベル情報の一部を表示します。

例

ラベル情報を表示します。

<Switch> display device manuinfo

```
Slot 1 CPU 0:
DEVICE_NAME         : QX-S5148GT-4X
DEVICE_SERIAL_NUMBER : 219801A1QP9208Q00022
MAC_ADDRESS         : 6893-20DA-2535
MANUFACTURING_DATE   : 2020-08-04
VENDOR_NAME         : NEC
Fan 1:
The operation is not supported on the specified fan.
Power 1:
The operation is not supported on the specified power.
```

9.1.13 display device manuinfo power

Syntax

display device manuinfo slot *slot-number* **power** *power-id*

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

slot *slot-number*： IRF スタックメンバをそのメンバ ID で指定します。

power-id： 電源装置をその ID で指定します。

説明

display device manuinfo power コマンドは電源装置の電子ラベル情報を表示します。

例

電源装置の電子ラベル情報を表示します。

<Switch> display device manuinfo slot 1 power 1

. . .

(省略します)

9.1.14 display diagnostic-information

Syntax

display diagnostic-information [**hardware** | **infrastructure** | **l2** | **l3** | **service**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

hardware: ハードウェアに関する稼働状態の統計情報を表示します。

infrastructure: 基本モジュールに関する稼働状態の統計情報を表示します。

l2: レイヤ 2 機能に関する稼働状態の統計情報を表示します。

l3: レイヤ 3 機能に関する稼働状態の統計情報を表示します。

service: 上位レイヤ機能に関する稼働状態の統計情報を表示します。

説明

display diagnostic-information コマンドは、システム内にある複数の機能モジュールの稼働状態に関する統計情報を表示します。

装置に異常がある場合、以下の方法の 1 つを用いて、問題を特定するために多くの情報を収集する必要があります。

- モジュールごとの稼働中のデータを収集するため、個別の display コマンドを使用します。
- 複数のモジュールの稼働中の大量のデータを収集するため、**display diagnostic-information** コマンドを使用します。

記憶媒体の

この **display** コマンドは**| by-linenum**、**>** *filename*、**>>** *filename* パラメータをサポートしていません。このコマンドはファイルに保存するか、あるいは画面に出力するかどうか確認メッセージが表示されます。ファイルは自動的に記憶媒体に圧縮して保存されます。

圧縮された統計情報を表示する場合、以下の方法を行います。

1) **tar extract** コマンドでファイルを解凍します。
2) **gunzip** コマンドでファイルを解凍します。
3) 解凍したファイルの内容を **more** コマンドで表示します。

例

システム内のすべての機能モジュールの稼働状態を表示します。

<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===============
...
```

システム内のすべての機能モジュールの稼働状態を保存します。

<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_Sysname_20160101-024601.tar.gz]:
Diagnostic information is outputting to
flash:/diag_Sysname_20160101-024601.tar.gz.
```

```
Please wait...
Save successfully.
Press Enter when the system prompts you to enter the file name.
```

関連コマンド

- **gunzip**
- **more**
- **tar extract**

9.1.15 display environment

Syntax

display environment [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

slot *slot-number*: メンバ ID によって IRF スタックのメンバ装置を指定します。指定しない場合、すべての IRF スタックのメンバ装置の温度情報を表示します。

説明

display environment コマンドは装置の現在の温度および温度しきい値などの温度情報を表示します。

例

装置の温度情報を表示します。

<Switch> display environment

```
System temperature information (degree centigrade):
---------------------------------------------------------------------
Slot  Sensor    Temperature  Lower  Warning  Alarm  Shutdown
1     hotspot 1 49           0      84       98     115
1     hotspot 2 46           0      100      110    NA
1     hotspot 3 46           0      100      110    NA
```

表 9-3 コマンド出力

フィールド	説明
System temperature information (degree centigrade)	温度情報（°C）です。
sensor	センサ温度（hotspot:ホットスポットセンサ）です。
Slot	センサの場所です。
Temperature	現在の温度です。
Lower	温度の下限しきい値です。装置がこのフィールドをサポートしていない場合、**NA**と表示します。
Warning	ワーニングとなる温度のしきい値です。装置がこのフィールドをサポートしていない場合、**NA**と表示します。
Alarm	アラームとなる温度のしきい値です。装置がこのフィールドをサポートしていない場合、**NA**と表示します。
Shutdown	自動でシャットダウンとなる温度のしきい値です。装置がこのフィールドをサポートしていない場合、**NA**と表示します。

9.1.16 display fan

Syntax

display fan [**slot** *slot-number* [*fan-id*]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

slot *slot-number*: メンバ ID によって IRF スタックのメンバ装置を指定します。指定しない場合、すべての IRF スタックのメンバ装置の内蔵ファンの稼働状態を表示します。

fan-id: 内蔵ファンの番号を示し、指定したファンの稼動状態を表示します。指定しない場合、すべてのファンの稼動状態を表示します。

説明

display fan コマンドはファンの稼働状態を表示します。

例

すべてのファンの稼動状態を表示します。

<Switch> display fan

```
Slot 1:
Fan 1:
State    : Normal
```

表 9-4 コマンド出力

フィールド	説明
Slot 1	IRFスタック装置のIDです。
Fan 1	内蔵ファンの番号です。
State	ファンの稼働状態を示します。 • **Absent**–ファンスロットにファンがありません。 • **Normal**–ファンが正常に動作しています。 • **Fault**–ファンに問題があります。

9.1.17 display memory

Syntax

display memory [**slot** *slot-number* [**cpu** *cpu-number*]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

slot *slot-number*: メンバ ID によって IRF スタックのメンバ装置を指定します。指定しない場合、すべての IRF スタックのメンバ装置のメモリ使用率を表示します。

cpu *cpu-number*: CPU 番号を指定します。*cpu-number* は 0 で固定です。

説明

display memory コマンドは装置のメモリ使用率を表示します。

例

メモリ使用率を表示します。

<Switch> display memory

```
Memory statistics are measured in KB:
Slot 1:
           Total     Used     Free    Shared   Buffers    Cached   FreeRatio
Mem:       498284    293884    204400        0     1316     76332      41.0%
-/+ Buffers/Cache:    216236    282048
Swap:          0        0        0
```

表 9-5 コマンド出力

フィールド	説明
Mem	メモリ使用率です。
Total	割り当てることができる物理メモリサイズの合計です。 メモリサイズは2つの部分に分けられます。 1番目は単独でカーネルコード、カーネル管理に使用されます。2番目は稼働サービスモジュールのようなタスク、ファイルの格納に使用されます。2番目のサイズはトータルの物理メモリサイズから1番目のメモリサイズを引いたサイズとなります。
Used	使用されている物理メモリです。
Free	使用されていない物理メモリです。
Shared	プロセスによって共有されている物理メモリです。
Buffers	バッファで使用されている物理メモリです。
Cached Caches	キャッシュで使用されている物理メモリです。
FreeRatio	使用されていないメモリの割合です。
-/+ Buffers/Cache	-/+ Buffers/Cache:Used = Mem:Used － Mem:Buffers － Mem:Cached ここで物理メモリはアプリケーションで使用されていることを示します。 -/+ Buffers/Cache:Free = Mem:Free + Mem:Buffers + Mem:Cached ここで物理メモリはアプリケーションで使用可能であることを示します。
Swap	スワップメモリです。

9.1.18 display memory-threshold

Syntax

display memory-threshold [**slot** *slot-number* [**cpu** *cpu-number*]]

View

すべての view

定義済みユーザロール

network-admin

パラメータ

slot *slot-number*: メンバ ID によって IRF スタックのメンバ装置を指定します。指定しない場合、IRF スタックの Master 装置のメモリしきい値とメモリ使用率通知の統計情報を表示します。

cpu *cpu-number*: CPU 番号を指定します。*cpu-number* は 0 で固定です。

説明

display memory-threshold コマンドは装置のメモリしきい値とメモリ使用率通知の統計情報を表示します。

メモリ使用率通知の詳細は以下のログ情報を参照してください。

MEM_EXCEED_THRESHOLD あるいは MEM_BELOW_THRESHOLD

例

装置のメモリしきい値とメモリ使用率通知の統計情報を表示します。

<Switch> display memory-threshold

```
Memory usage threshold: 100%
Free memory threshold:
    Minor: 64M
    Severe: 48M
    Critical: 32M
    Normal: 96M
Current memory state: Normal
Event statistics:
 [Back to normal state]
   First notification: 2015-5-15 09:21:35.546
   Latest notification: 2015-5-15 09:21:35.546
   Total number of notifications sent: 1
 [Enter minor low-memory state]
   First notification at: 2015-5-15 09:07:05.941
   Latest notification at: 2015-5-15 09:07:05.941
   Total number of notifications sent: 1
```

```
[Back to minor low-memory state]
  First notification at: 0.0
  Latest notification at: 0.0
  Total number of notifications sent: 0
[Enter severe low-memory state]
  First notification at: 0.0
  Latest notification at: 0.0
  Total number of notifications sent: 0
[Back to severe low-memory state]
  First notification at: 0.0
  Latest notification at: 0.0
  Total number of notifications sent: 0
[Enter critical low-memory state]
  First notification at: 0.0
  Latest notification at: 0.0
  Total number of notifications sent: 0
```

9.1.19 display power

Syntax

display power [**slot** *slot-number* [*power-id*]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

slot *slot-number*: メンバ ID によって IRF スタックのメンバ装置を指定します。指定しない場合、すべてのメンバ装置の電源ユニットの情報を表示します。

power-id: 電源ユニットを ID で指定します。指定しない場合、すべての電源ユニットの情報を表示します。

説明

display power コマンドは電源ユニットの情報を表示します。

例

電源ユニットの情報を表示します。

<Switch> display power

```
Slot 1:
 PowerID State    Mode   Current(A)  Voltage(V)  Power(W)
 1       Normal   AC       --          --          --
```

9.1.20 display scheduler job

Syntax

display scheduler job [*job-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

job-name: job の名前を指定します。設定範囲は 1～47 文字で、大文字、小文字を区別します。指定しない場合、すべての job の設定情報を表示します。

説明

display scheduler job コマンドはスケジュール自動実行機能の job の設定情報を表示します。

例

すべての job の設定情報を表示します。

<Switch> display scheduler job

```
Job name: saveconfig
 copy startup.cfg backup.cfg

Job name: backupconfig

Job name: creat-VLAN100
 system-view
 vlan 100
```

// 出力では、装置は 3 つの job があることを示します。最初のジョブには 1 つのコマンドがあります。2 番目の job にはコマンドがありません。3 番目の job には 2 つのコマンドがあります。job は空白行で区切られます。

9.1.21 display scheduler logfile

Syntax

display scheduler logfile

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display scheduler logfile コマンドはスケジュール自動実行機能の実行された job のログ情報を表示します。

例

実行された job のログ情報を表示します。

<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
```

表 9-6 コマンド出力

フィールド	説明
Logfile Size	ログファイルのサイズです。byteで表示されます。
Schedule name	jobが所属するスケジュールです。
Execution time	jobが開始されたときの時間です。
Completion time	jobが完了したときの時間です。jobが実行されなかった、あるいはjobにコマンドがない場合、このフィールドは表示されません。

フィールド	説明
Job output	jobのコマンドと出力です。

関連コマンド

reset scheduler logfile

9.1.22 display scheduler reboot

Syntax

display scheduler reboot

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display scheduler reboot コマンドは、スケジュール再起動機能のユーザが設定した装置の再起動時刻を表示します。

例

装置の再起動時刻を表示します。

<Switch> display scheduler reboot

```
System will reboot at 16:32:00 05/23/2015 (in 1 hours and 39 minutes).
```

関連コマンド

- **scheduler reboot at**
- **scheduler reboot delay**

9.1.23 display scheduler schedule

Syntax

display scheduler schedule [*schedule-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

schedule-name: スケジュール名を指定します。設定範囲は 1～47 文字で大文字、小文字を区別します。指定しない場合、すべてのスケジュールの情報を表示します。

説明

display scheduler schedule コマンドはスケジュール自動実行機能のスケジュール情報を表示します。

例

すべてのスケジュールの情報を表示します。

<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
```

表 9-7 コマンド出力

フィールド	説明
Schedule type	スケジュールが実行される時間です。実行時間が指定されていない場合、このフィールドは表示されません。
Start time	初回にスケジュールが実行される時間です。実行時間が指定されていない場合、このフィールドは表示されません。
Last execution time	スケジュールが実行されたときの最後の時間です。実行時間が指定されていない場合、このフィールドは表示されません。スケジュールが実行されていない場合、"**Yet to be executed**"と表示されます。
Last completion time	スケジュールが完了した最後の時間です。実行時間が指定されていない場合、このフィールドは表示されません。

フィールド	説明
Execution counts	スケジュールが実行された回数です。実行時間が指定されていない場合、このフィールドは表示されません。
Job name	スケジュールのjob名です。
Last execution status	最後に実行された結果です。 ● Successful ● Failed ● **Waiting**–装置はスケジュールを実行し、jobが実行待ちです。 ● **In process**–jobが実行されています。 ● **-NA-**–実行時間になっていません。 jobのコマンドが実行されたかどうかについての情報および実行結果を表示するには、**display scheduler logfile**コマンドを実行してください。

9.1.24 display transceiver interface

Syntax

display transceiver interface [*interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface-type interface-number: インタフェースのタイプと番号を指定します。指定しない場合、各トランシーバモジュールの主なパラメータを表示します。

説明

display transceiver interface コマンドはトランシーバモジュールの主なパラメータを表示します。

例

GigabitEthernet 1/0/1 のトランシーバモジュールの主なパラメータを表示します。

<Switch> display transceiver interface gigabitethernet 1/0/9

```
GigabitEthernet1/0/9 transceiver information:
  Transceiver Type            : 1000_BASE_T_AN_SFP
  Connector Type              : RJ45
  Wavelength(nm)              : N/A
  Transfer Distance(m)         : 100(TP)
  Digital Diagnostic Monitoring : NO
  Vendor Name                 : FINISAR CORP.
  Part Number                 : FCLF8521P2BTL
  Serial Number               : PJA5YMU
```

表 9-8 コマンド出力

フィールド	説明
transceiver information	トランシーバ情報です。
Transceiver Type	トランシーバタイプです。
Connector Type	コネクタタイプです。 ● **LC**：1.25 mm/RJ-45 ファイバコネクタです。 ● **RJ-45**：RJ-45コネクタです。
Wavelength(nm)	● **光ファイバトランシーバ**：送信されたレーザの中心波長（mm）です。もし複数の波長をサポートしている場合、コンマで区切られて波長が記載されます。 ● **電気モジュール**：NAと表示されます。
Transfer Distance(xx)	転送距離です。xxは、シングルモードのトランシーバではkm、その他のトランシーバではmを示します。トランシーバが複数の転送媒体をサポートしている場合、 2つの値はコンマで区切られます。対応する転送媒体は、転送距離の値の後にカッコに入れて示されます。転送媒体には下記のものがあります。 ● **9 um**：9/125 umシングルモードファイバです。 ● **50 um**：50/125 umマルチモードファイバです。 ● **62.5 um**：62.5/125 umマルチモードファイバです。 ● **TP**：ツイストペアケーブルです。 ● **CX4**：CX4 ケーブルです。
Digital Diagnostic Monitoring	デジタル診断機能がサポートされているかどうかを示します。 ● **YES**：サポートされています。 ● **NO**：サポートされていません。

9.1.25 display version

Syntax

display version

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display version コマンドは現在のソフトウェアバージョンなどシステムのバージョン情報を表示します。

例

システムのバージョン情報を表示します。

<Switch> display version

（省略します）

9.1.26 header

Syntax

header { **incoming** | **legal** | **login** | **motd** | **shell** } *text*

undo header { **incoming** | **legal** | **login** | **motd** | **shell** }

デフォルト

shell *%Please change the password from the default settings.%*

View

System view

定義済みユーザロール

network-admin

パラメータ

incoming: Modem ログインユーザが user view に移行する際に表示されるバナーを設定します。認証が必要な場合、認証にパスしたのちバナーが表示されます。

legal:ユーザがユーザ名およびパスワードをCLIにアクセスして入力する前にバナーを設定します。

login:ログインユーザによってパスワードまたは scheme 認証される前にバナーを設定します。

motd:**legal** バナーが表示される前に greeting（あいさつ）バナーを設定します。

shell: 非 Modem ログインユーザが user view に移行する際に表示されるバナーを設定します。

text: バナーメッセージです。パラメータあるいは複数行の 2 つの形式で入力できます。詳細は、オペレーションマニュアルのセクション 1 *はじめに*”*装置管理*”を参照してください。

説明

header コマンドはバナーを作成します。

undo header コマンドはバナーを削除します。

例

legal バナーを作成します。

<Switch> system-view

[Switch] header legal

```
Please input banner content, and quit with the character '%'.
Welcome to use the legal banner%
```

9.1.27 job

Syntax

job *job-name*

undo job *job-name*

デフォルト

設定なし

View

Schedule view

定義済みユーザロール

network-admin

パラメータ

job-name: job 名を指定します。設定範囲は 1～47 文字で、大文字、小文字を区別します。

説明

job コマンドはスケジュール自動実行機能のスケジュールに job を割り当てます。

undo job コマンドは job を削除します。

スケジュールに複数の job を割り当てることができます。スケジュールの job は連続して実行されます。

スケジュールに割り当てられる job はあらかじめ作成されている必要があります。job を作成する場合、**scheduler job** コマンドを使用します。

例

スケジュール saveconfig に job 名が save-job の job を割り当てます。

<Switch> system-view

[Switch] scheduler schedule saveconfig

[Switch-schedule-saveconfig] job save-job

関連コマンド

- **scheduler job**
- **scheduler schedule**

9.1.28 locator blink

Syntax

locator [**slot** *slot-number*] **blink** *blink-time*

locator [**slot** *slot-number*] **blink stop**

View

User view

定義済みユーザロール

network-admin

パラメータ

slot *slot-number*: IRF スタックメンバ ID によってメンバ装置を指定します。メンバ装置を指定しない場合、コマンドはすべてのメンバ装置に適用されます。

blink-time:Power LED を点滅させる時間を秒単位で指定します。設定範囲は 5 から 120 秒です。

stop:Power LED の点滅を停止します。

説明

locator blink *blink-time* コマンドは、指定した装置の Power LED を *blink-time* で指定した時間すばやく赤色と緑色で交互に点滅させます。**locator blink stop** コマンドを実行すると、**locator blink** *blink-time* コマンドによる Power LED の点滅を停止します。

本機能は装置の位置を特定する際に役立ちます。

例

点滅時間を 30 秒に指定して slot1 の装置の Power LED の点滅を開始します。

<Switch> locator slot 1 blink 30

Power LED の点滅を停止します。

<Switch> locator blink stop

🕮 **メモ：**

locator blink コマンドは Version7.1.4 を含む以降のソフトウェアからサポートしています。

9.1.29 memory-threshold

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*]]

デフォルト

minor：96MB

severe：64MB

critical：48MB

normal：128MB

View

System view

定義済みユーザロール

network-admin

パラメータ

minor *minor-value*: **minor** アラームのしきい値を指定します。設定範囲は 0～884 です。しきい値は **normal** しきい値以下にする必要があります。0 に指定すると **minor** アラーム機能を無効にします。

severe *severe-value*: **severe** アラームのしきい値を指定します。設定範囲は **minor** アラームのしきい値によって変わります。しきい値は **minor** しきい値以下にする必要があります。0 に指定すると **severe** アラーム機能を無効にします。

critical *critical-value*: **critical** アラームのしきい値を指定します。設定範囲は **severe** アラームのしきい値によって変わります。しきい値は **severe** しきい値以下にする必要があります。0 に指定すると **critical** アラーム機能を無効にします。

normal *normal-value*: **normal** アラームのしきい値を指定します。設定範囲は **minor** アラームのしきい値によって変わります。しきい値はメモリサイズの合計以下にする必要があります。

slot *slot-number*: メンバ ID によって IRF スタックのメンバ装置を指定します。指定しない場合、IRF スタックの Master 装置の空きメモリのしきい値を設定します。

cpu *cpu-number*: CPU 番号を指定します。*cpu-number* は 0 で固定です。

説明

memory-threshold コマンドは空きメモリ容量のしきい値を設定します。

undo memory-threshold コマンドはデフォルトに戻します。

正常な動作とメモリ使用率を改善するため、システムはリアルタイムで使用可能なメモリサイズをモニタします。しきい値が超過すると、モジュールあるいはプロセスで対策を行うことができるように、システムはアラーム通知あるいはアラーム解除通知を関係するモジュールあるいはプロセスに通知します。しきい値の詳細はオペレーションマニュアルのセクション 1 *はじめに*”*装置管理*”を参照してください。

例

minor アラームを 64MB、severe アラームを 48MB、critical アラームを 32MB、normal アラームを 96MB に設定します。

<Switch> system-view

[Switch] memory-threshold minor 64 severe 48 critical 32 normal 96

関連コマンド

display memory-threshold

9.1.30 monitor cpu-usage enable

Syntax

monitor cpu-usage enable [**slot** *slot-number* [**cpu** *cpu-number*]]

undo monitor cpu-usage enable [**slot** *slot-number* [**cpu** *cpu-number*]]

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

パラメータ

slot *slot-number*: メンバ ID によって IRF スタックのメンバ装置を指定します。もしこのパラメータが指定されない場合、すべての IRF スタックにあるメンバ装置の CPU 使用率の記録を有効にします。

cpu *cpu-number*: CPU 番号を指定します。*cpu-number* は 0 で固定です。

説明

monitor cpu-usage enable コマンドは CPU 使用率の記録を有効にします。

undo monitor cpu-usage enable コマンドは CPU 使用率の記録を無効にします。

CPU 使用率の記録を有効にしたのち、**monitor cpu-usage interval** コマンドで指定したサンプリング間隔で CPU 使用率を記録し、保存します。最新の CPU 使用率を表示する場合、**display cpu-usage history** コマンドを使用します。

例

CPU 使用率の記録を有効にします。

<Switch> system-view

[Switch] monitor cpu-usage enable

関連コマンド

- **display cpu-usage configuration**
- **display cpu-usage history**
- **monitor cpu-usage interval**

9.1.31 monitor cpu-usage interval

🕮 メモ：

monitor cpu-usage interval コマンドは **monitor cpu-usage threshold** コマンドの CPU 使用率を取得する間隔ではありません。**display cpu-usage history** コマンドの情報を取得する間隔です。

Syntax

monitor cpu-usage interval *interval* [**slot** *slot-number* [**cpu** *cpu-number*]]

デフォルト

1 分

View

System view

定義済みユーザロール

network-admin

パラメータ

interval: CPU 使用率のサンプリング間隔を指定します。5Sec、1Min、5Min から指定します。5Sec は 5 秒、1Min は 1 分、5Min は 5 分です。

slot *slot-number*: メンバ ID によって IRF スタックのメンバ装置を指定します。もしこのパラメータが指定されない場合、すべての IRF スタックにあるメンバ装置の CPU 使用率のサンプリング間隔を設定します。

cpu *cpu-number*: CPU 番号を指定します。*cpu-number* は 0 で固定です。

説明

monitor cpu-usage interval コマンドは CPU 使用率のサンプリング間隔を設定します。

CPU 使用率の記録を有効にしたのち、指定したサンプリング間隔で CPU 使用率を記録し、保存します。最新の CPU 使用率を表示する場合、**display cpu-usage history** コマンドを使用します。

例

CPU 使用率のサンプリング間隔を 5 秒に設定します。

<Switch> system-view

[Switch] monitor cpu-usage interval 5Sec

関連コマンド

- **display cpu-usage configuration**
- **display cpu-usage history**
- **monitor cpu-usage enable**

9.1.32 monitor cpu-usage threshold

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*]]

デフォルト

threshold：99%

minor-threshold : 98%

recovery-threshold：50%

View

System view

定義済みユーザロール

network-admin

パラメータ

severe-threshold: 重大な CPU 使用率のアラームのしきい値を指定します。設定範囲は 2～100%です。

minor-threshold *minor-threshold*: マイナーな CPU 使用率のアラームのしきい値を指定します。設定範囲は 1～*severe-threshold*－1%です。

recovery-threshold *recovery-threshold*: CPU 使用率のリカバリのしきい値を指定します。設定範囲は 1～*minor-threshold*－1%です。

slot *slot-number*: メンバ ID によって IRF スタックのメンバ装置を指定します。もしこのパラメータが指定されない場合、すべての IRF スタックにあるメンバ装置の CPU 使用率のしきい値を指定します。

cpu *cpu-number*: CPU 番号を指定します。*cpu-number* は 0 で固定です。

説明

monitor cpu-usage threshold コマンドは CPU 使用率のしきい値を設定します。

undo monitor cpu-usage threshold コマンドはデフォルトに戻します。

装置は 1 分間隔で CPU 使用率をサンプリングします。サンプリングした値と CPU の使用率のしきい値を比較します。CPU 使用率のしきい値より大きい場合、装置は trap を送信します。

例

重大な CPU 使用率のしきい値を 90%、マイナーな CPU 使用率のしきい値を 80%、CPU 使用率のリカバリのしきい値を 70%に設定します。

<Switch> system-view

[Switch] monitor cpu-usage threshold 90 minor-threshold 80 recovery-threshold 70

関連コマンド

display cpu-usage configuration

9.1.33 monitor resend cpu-usage

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*]]

デフォルト

minor アラームの再送信間隔は 300 秒です。severe アラームの再送信間隔は 60 秒です。

View

System view

定義済みユーザロール

network-admin

パラメータ

minor-interval *minor-interval*: minor アラームの再送信間隔を 10～3600 の範囲で 5 の倍数で指定します。（秒単位）

severe-interval *severe-interval*: severe アラームの再送信間隔を 10～3600 の範囲の 5 の倍数で指定します。（秒単位）

slot *slot-number*: IRF スタックメンバをそのメンバ ID で指定します。メンバ装置を指定しない場合、このコマンドは Master 装置の CPU 使用率アラームの再送信間隔を設定します。

cpu *cpu-number*: CPU を番号で指定します。

説明

monitor resend cpu-usage コマンドは CPU 使用率アラームの再送信間隔を設定します。

undo monitor resend cpu-usage コマンドはデフォルト設定に戻します。

装置は、定期的に CPU 使用率をサンプリングし、そのサンプルを CPU 使用率のしきい値と比較します。サンプルがアラームしきい値を超えると、CPU 使用率はアラーム状態になり、装置はアラームを送信します。

CPU 使用率が minor アラーム状態にある間、装置は、CPU 使用率が severe しきい値を超えるか、minor アラームが削除されるまで、minor アラームを定期的に送信します。

CPU 使用率が severe アラーム状態にある間、装置は、severe アラームが削除されるまで、定期的に severe アラームを送信します。

このコマンドを使用すると、CPU 使用率アラームの再送間隔を変更できます。

minor-interval または **severe-interval** を指定しない場合、**undo monitor resend cpu-usage** コマンドは、minor アラームと severe アラームの再送信間隔の両方のデフォルト設定を復元します。

例

スロット 1 の CPU0 に対する CPU 使用率 minor アラームの再送間隔を 60 秒に設定します。

<Switch> system-view

[Switch] monitor resend cpu-usage minor-interval 60 slot 1 cpu 0

9.1.34 monitor resend memory-threshold

Syntax

monitor resend memory-threshold { **critical-interval** *critical-interval* | **minor-interval** *minor-interval* | **severe-interval** *severe-interval* } * [**slot** *slot-number* [**cpu** *cpu-number*]]

undo monitor resend memory-threshold [**critical-interval** | **minor-interval** | **severe-interval**] * [**slot** *slot-number* [**cpu** *cpu-number*]]

デフォルト

- Minor アラーム再送信間隔：12 時間。
- Severe アラーム再送信間隔：3 時間
- Critical アラーム再送信間隔：1 時間

View

System view

定義済みユーザロール

network-admin

パラメータ

critical-interval *critical-interval*: critical アラームの再送信間隔を指定します。設定範囲は 1～48 です。単位は時間です。

minor-interval *minor-interval*: minor アラームの再送信間隔を指定します。設定範囲は 1～48 です。単位は時間です。

severe-interval *severe-interval*: severe アラームの再送信間隔を指定します。設定範囲は 1～48 です。単位は時間です。

slot *slot-number*: IRF スタックメンバをそのメンバ ID で指定します。メンバ装置を指定しない場合、このコマンドは Master 装置のアラーム再送信間隔を設定します。

cpu *cpu-number*: CPU を番号で指定します。

説明

monitor resend memory-threshold コマンドはメモリ不足アラームの再送信間隔を設定します。

undo monitor resend memory-threshold コマンドはデフォルトに戻します。

装置は、定期的に空きメモリ容量をサンプリングし、そのサンプルを空きメモリしきい値と比較します。サンプルがしきい値以下になると、装置はメモリ不足アラーム状態に入り、アラームを送信します。

critical アラーム状態では、装置は critical アラームが削除されるまで定期的に critical アラーム通知を送信します。

低いアラーム状態では、装置は高いアラーム状態になるか、または現在のアラームが削除されるまで、アラーム状態の通知を定期的に送信します。

このコマンドを使用して、アラームの再送間隔を変更できます。

例

スロット 1 の CPU0 の minor メモリ不足アラームの再送間隔を 12 時間に設定します。

<Switch> system-view

[Switch] monitor resend memory-threshold minor-interval 12 slot 1 cpu 0

9.1.35 password-recovery enable

Syntax

password-recovery enable

undo password-recovery enable

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

password-recovery enable コマンドはパスワードリカバリ機能を有効にします。

undo password-recovery enable コマンドはパスワードリカバリ機能を無効にします。

パスワードリカバリ機能は Boot ROM メニューからデバイス構成と SDRAM へのアクセスを制御できます。

パスワードリカバリ機能が有効である場合、コンソールからのユーザは認証なしで装置にアクセスでき、新しいパスワードを設定することができます。

パスワードリカバリ機能が無効である場合、コンソールからのユーザは、新しいパスワードを設定する前に、工場出荷状態にする必要があります。工場出荷状態に戻すと次回に起動で使用するコンフィグレーションファイルを削除します。

本機能は、主に管理者が設定したパスワードを忘れたときに使用します。パスワードリカバリ機能が有効な場合、保存してある current-configuration や super password を読み込まずに装置を起動できます。コンフィグを読み込まずに起動する操作は Boot メニューから行います。

例

パスワードリカバリ機能を無効にします。

<Switch> system-view

[Switch] undo password-recovery enable

9.1.36 reboot

Syntax

reboot [**slot** *slot-number*] [**force**]

View

User view

定義済みユーザロール

network-admin

パラメータ

slot *slot-number*: メンバ ID によって IRF スタックのメンバ装置を指定します。指定しない場合、すべての IRF スタックの装置を再起動します。

force: ソフトウェアの確認を行わず、すぐさま装置を再起動します。指定しない場合、システムは、再起動によってデータ紛失あるいはシステムの故障が発生するかどうかを確認します。たとえば、システムはメインシステムソフトウェアのファイルが存在するか、および書き込み操作が記憶媒体で進行中であるかどうか確認します。再起動によって問題は発生すると認識した場合、システムは装置の再起動を行いません。

説明

⚠ **注意**：

- 装置を再起動するためネットワークサービスが中断されます。
- **force** パラメータは、**force** パラメータを指定しないと再起動できないときのみ使用してください。**force** パラメータを指定した場合、ソフトウェアの確認を行わないため、ファイルシステムの故障が発生する可能性があります。

reboot コマンドは IRF スタックのメンバ装置あるいはすべての IRF スタックの装置を再起動します。

メインのシステムソフトウェアファイルがエラー、または存在しない場合、装置は **reboot** コマンドで再起動できません。この場合、システムソフトウェアファイルを再指定してから装置を再起動してください。

データ保護のため、装置がファイルの操作を実行している間、装置の再起動を行わないでください。

すべての IRF スタックのメンバ装置を再起動する場合、slot パラメータを指定しません。

IRF スタックのマスタ装置を再起動する場合、IRF スタックユニットのメンバ装置を認識し、正常に動作しているかどうかを確認します。

IRF スタックユニットが 1 台のメンバ装置のみで構成されている場合、IRF スタックユニットは再起動します。IRF スタックユニットが複数のメンバ装置で構成され、正常に動作している場合、マスタ/メンバの切り替えが発生します。

重要：

IRF スタックユニットを正常に動作させるため、メンバ装置が正常に動作していない場合、マスタ装置の切り替えを行わないでください。

例

稼働中のコンフィグレーションを保存してから、設定が変更されていないとき、装置を再起動します。

<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 flash successfully.
This command will reboot the device. Continue? [Y/N]:y
Now rebooting, please wait...
```

ソフトウェアの確認を行わず、すぐさま装置を再起動します。

<Switch> reboot force

```
A forced reboot might cause the storage medium to be corrupted. Continue? [Y/N]:y
Now rebooting, please wait...
```

9.1.37 reset scheduler logfile

Syntax

reset scheduler logfile

View

User view

定義済みユーザロール

network-admin

説明

reset scheduler logfile コマンドはスケジュール自動実行機能のログ情報の削除を行います。

例

スケジュール自動実行機能のログ情報を削除します。

<Switch> reset scheduler logfile

関連コマンド

display scheduler logfile

9.1.38 scheduler job

Syntax

scheduler job *job-name*

undo scheduler job *job-name*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

job-name: job 名を指定します。設定範囲は 1～47 文字で大文字、小文字を区別します。

説明

scheduler job コマンドはスケジュール自動実行機能の job を作成し、job view に移行します。すべに job が存在する場合、直接 job view に移行します。

undo scheduler job コマンドは job を削除します。

job は複数のスケジュールから割り当てることができます。job view で job にコマンドを割り当てることができます。

例

job 名が backupconfig の job を作成し、job view に移行します。

<Switch> system-view

[Switch] scheduler job backupconfig

[Switch-job-backupconfig]

関連コマンド

- **command**
- **scheduler schedule**

9.1.39 scheduler logfile size

Syntax

scheduler logfile size *value*

デフォルト

16KB

View

System view

定義済みユーザロール

network-admin

パラメータ

value: job を実行するログファイルのサイズを設定します。設定範囲は 16～1024KB です。

説明

scheduler logfile size コマンドはスケジュール自動実行機能の job を実行するログファイルのサイズを設定します。

job を実行するログファイルは、job が実行される情報を保存します。ファイルの容量が一杯である場合、古い記録が削除され、新しい記録が保存されます。もしファイルサイズよりもログファイルのサイズが大きい場合、実行される情報はファイルに保存されません。

例

job を実行するログファイルのサイズを 32KB に設定します。

<Switch> system-view

[Switch] scheduler logfile size 32

関連コマンド

display scheduler logfile

9.1.40 scheduler reboot at

Syntax

scheduler reboot at *time* [*date*]

undo scheduler reboot

デフォルト

設定なし

View

User view

定義済みユーザロール

network-admin

パラメータ

time: 再起動する時間を指定します。形式は *hh*:*mm* です。*hh* の設定範囲は 0～23 です。*mm* の設定範囲は 0～59 です。

date: 再起動する日時を指定します。形式は *MM*/*DD*/*YYYY* あるいは *YYYY*/*MM*/*DD* です。*YYYY* の設定範囲は 2000～2035 です。*MM* の設定範囲は 1～12 です。*DD* の設定範囲は月によって変わります。

説明

⚠ **注意**：

装置を再起動するためネットワークサービスが中断されます。

scheduler reboot at コマンドはスケジュール再起動機能の日時、時間を指定します。

undo scheduler reboot コマンドはスケジュール再起動機能の設定を削除します。

日時が指定されていないとき、以下の動作を行います。

- 再起動時間が現在時刻より遅い場合、再起動は当日の再起動時間に行われます。
- 再起動時間が現在時刻より早い場合、再起動は次の日の再起動時間に行われます。

装置はスケジュール再起動機能を 1 回のみサポートします。もし **schedule reboot delay** コマンドと **scheduler reboot at** コマンドの両方が設定されている場合、あるいはどちらかのコマンドを複数回設定した場合、最後に設定したコマンドが適用されます。

データ保護のため、ファイルの操作を実行している間、システムは装置の再起動を行いません。

例

装置を PM12:00 に再起動します。現在時刻は 2015 年 6 月 6 日の 11:43 であると仮定します。

<Switch> scheduler reboot at 12:00

```
Reboot system at 12:00:00 06/06/2015 (in 0 hours and 16 minutes). Confirm? [Y/N]:
```

関連コマンド

scheduler reboot delay

9.1.41 scheduler reboot delay

Syntax

scheduler reboot delay *time*

undo scheduler reboot

デフォルト

設定なし

View

User view

定義済みユーザロール

network-admin

パラメータ

time: 再起動する時間を指定します。形式は *hh*:*mm* あるいは *mm* です。パラメータは 6 文字まで設定することができます。形式が *hh*:*mm* である場合、*mm* の設定範囲は 0～59 です。

説明

注意：

装置を再起動するためネットワークサービスが中断されます。

scheduler reboot delay コマンドはスケジュール再起動機能の再起動遅延時間を指定します。

undo scheduler reboot コマンドはスケジュール再起動機能の再起動遅延時間を削除します。

装置はスケジュール再起動機能を 1 回のみサポートします。もし **schedule reboot delay** コマンドと **scheduler reboot at** コマンドの両方が設定されている場合、あるいはどちらかのコマンドを複数回設定した場合、最後に設定したコマンドが適用されます。

データ保護のため、ファイルの操作を実行している間、システムは装置の再起動を行いません。

例

装置を 88 分後に再起動します。現在時刻は 2015 年 6 月 6 日の 11:48 であると仮定します。

<Switch> scheduler reboot delay 88

```
Reboot system at 13:16 06/06/2015(in 1 hours and 28 minutes). Confirm? [Y/N]:
```

9.1.42 scheduler schedule

Syntax

scheduler schedule *schedule-name*

undo scheduler schedule *schedule-name*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

schedule-name: スケジュール名を指定します。設定範囲は 1～47 文字で大文字、小文字を区別します。

説明

scheduler schedule コマンドはスケジュール自動実行機能のスケジュールを作成し、schedule view に移行します。すでにスケジュールが存在する場合、直接 schedule view に移行します。

undo scheduler schedule コマンドはスケジュールを削除します。

管理者を妨げることなく、自動でコマンドあるいはコマンドセットを実行するように job のスケジュールを行うことができます。

スケジュールを設定するには以下を行います。

1) **scheduler job** コマンドを使用して job を作成します。

2) job view で **command** コマンドを使用して job にコマンドを割り当てます。
3) **scheduler schedule** コマンドを使用してスケジュールを作成します。
4) schedule view で **job** コマンドを使用してスケジュールに job を割り当てます。複数の job をスケジュールに割り当てることができます。job はすでに作成している必要があります。
5) schedule view で **user-role** コマンドを使用してスケジュールにユーザロールを割り当てます。スケジュールに最大 64 のユーザロールを割り当てることができます。
6) schedule view で **time at** コマンド、**time once** コマンド、あるいは **time repeating** コマンドを使用して、スケジュールを実行する時間を指定します。1 つのスケジュールに 1 つの実行時間のみ指定することができます。

例

スケジュール名が saveconfig のスケジュールを作成します。

<Switch> system-view

[Switch] scheduler schedule saveconfig

関連コマンド

- **job**
- **time at**
- **time once**

9.1.43 shutdown-interval

Syntax

shutdown-interval interval

undo shutdown-interval

デフォルト

30 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

time: 検出間隔を指定します。設定範囲は 0～300 秒です。0 秒に設定すると検出を行いません。

説明

shutdown-interval コマンドはポートの状態を検出する検出間隔を設定します。

undo shutdown-interval コマンドはデフォルトに戻します。

プロトコルがポートをシャットダウンするとき、装置は検出間隔タイマを開始します。

タイマが経過すると、装置はポートの物理状態を反映するため、ポートの状態を UP にします。

ポートの検出間隔中に、タイマが変更した場合、装置は新しい設定 T1 とポートがシャットダウンしてから経過した時間 T を比較します。

- もし T<T1 の場合、ポートは T1-T 秒後に UP にします。
- もし T>=T1 の場合、ポートはすぐさま UP にします。

たとえば、ポートがシャットダウンしてから 2 秒後に、タイマを 30 秒から 10 秒に変更した場合、ポートは 8 秒後に UP になります。もしポートがシャットダウンしてから 10 秒後にタイマを 30 秒から 2 秒に変更した場合、ポートはすぐさま UP になります。

例

ポートの状態を検出する検出間隔を 100 秒に設定します。

<Switch> system-view

[Switch] shutdown-interval 100

9.1.44 sysname

Syntax

sysname *sysname*

undo sysname

デフォルト

装置名

View

System view

定義済みユーザロール

network-admin

パラメータ

sysname: 装置の名前を指定します。設定範囲は 1～64 文字です。

説明

sysname コマンドは装置名を設定します。

undo sysname コマンドはデフォルトに戻します。

装置名はネットワークの装置を識別し、CLI の user view のプロンプトとして使用されます。装置名が Switch である場合、user view のプロンプトは<Switch>です。

例

装置の名前を R2000 に設定します。

<Switch> system-view

[Switch] sysname R2000

[R2000]

9.1.45 temperature-limit

Syntax

temperature-limit slot *slot-number* **hotspot** *sensor-number lowlimit warninglimit* [*alarmlimit*]

undo temperature-limit slot *slot-number* **hotspot** *sensor-number*

デフォルト

表 9-9、表 9-10 に温度アラームのしきい値のデフォルトを示します。

表 9-9 温度アラームのしきい値のデフォルトと推奨値

装置	センサ	下限温度	ワーニング温度の推奨	ワーニング温度のデフォルト	アラーム温度の推奨	アラーム温度のデフォルト
QX-S5124GT-4X	Hotspot 1	0	79	84	84	98
	Hotspot 2	0	94	100	99	110
	Hotspot 3	0	97	100	102	110
	Hotspot 4	0	93	100	98	110
QX-S5148GT-4X	Hotspot 1	0	87	84	92	98
	Hotspot 2	0	94	84	99	98
	Hotspot 3	0	102	100	107	110
	Hotspot 4	0	100	100	105	110

装置	センサ	下限温度	ワーニング温度の推奨	ワーニング温度のデフォルト	アラーム温度の推奨	アラーム温度のデフォルト
	Hotspot 5	0	108	100	113	110
	Hotspot 6	0	113	100	118	110
	Hotspot 7	0	111	100	116	110
	Hotspot 8	0	105	100	110	110
QX-S5124GP-4X	Hotspot 1	0	76	88	81	102
	Hotspot 2	0	77	100	82	115
	Hotspot 3	0	79	100	84	115
	Hotspot 4	0	79	100	84	115
	Hotspot 5	0	76	100	81	115
	Hotspot 6	0	78	100	83	115
	Hotspot 7	0	80	100	85	115
QX-S5124GT-4X-PW	Hotspot 1	0	71	84	76	98
	Hotspot 2	0	92	100	97	110
	Hotspot 3	0	93	100	98	110
	Hotspot 4	0	83	100	88	110
	Hotspot 5	0	81	100	86	110
	Hotspot 6	0	71	110	76	130
QX-S5148GT-4X-PW	Hotspot 1	0	88	84	93	98
	Hotspot 2	0	92	84	97	98

装置	センサ	下限温度	ワーニング温度の推奨	ワーニング温度のデフォルト	アラーム温度の推奨	アラーム温度のデフォルト
	Hotspot 3	0	101	100	106	110
	Hotspot 4	0	102	100	107	110
	Hotspot 5	0	107	100	112	110
	Hotspot 6	0	114	100	119	110
	Hotspot 7	0	113	100	118	110
	Hotspot 8	0	106	100	111	110
	Hotspot 9	0	88	100	93	130

View

System view

定義済みユーザロール

network-admin

パラメータ

slot *slot-number*: メンバ ID によって IRF スタックのメンバ装置を指定します。

hotspot: ホットスポットセンサの温度アラームしきい値を設定します。ホットスポットセンサは通常、高温となるチップの側に置かれ、チップをモニタします。

sensor-number: 番号でセンサを指定します。各番号は装置の温度センサを示します。設定範囲は 1～4 です。

lowlimit: 摂氏温度表示による下限温度を指定します。

warninglimit: 摂氏温度表示による高温時のワーニングしきい値を指定します。しきい値は下限温度よりも高い値にする必要があります。

alarmlimit: 摂氏温度表示による高温時のアラームしきい値を指定します。しきい値はワーニングしきい値よりも高い値にする必要があります。

表 9-10 温度アラームのしきい値の設定範囲

装置	センサ	下限温度	ワーニング温度	アラーム温度
QX-S5124GT-4X	Hotspot 1～4	-10℃ ～ +70℃	15℃ ～ 125℃	20℃ ～ 135℃

装置	センサ	下限温度	ワーニング温度	アラーム温度
QX-S5148GT-4X	Hotspot 1～8	-10℃ ～ +70℃	15℃ ～ 125℃	20℃ ～ 135℃
QX-S5124GP-4X	Hotspot 1～7	-10℃ ～ +70℃	15℃ ～ 125℃	20℃ ～ 135℃
QX-S5124GT-4X-PW	Hotspot 1～6	-10℃ ～ +70℃	15℃ ～ 125℃	20℃ ～ 135℃
QX-S5148GT-4X-PW	Hotspot 1～9	-10℃ ～ +70℃	15℃ ～ 125℃	20℃ ～ 135℃

説明

temperature-limit コマンドは、装置の温度アラームのしきい値を設定します。

undo temperature-limit コマンドは、デフォルトに戻します。

装置の温度が下限温度を下回った、高温時のワーニング温度、あるいは高温時のアラーム温度に到達したとき、装置は以下の動作を行います。

- ログメッセージを作成し、trap を送信します。
- 装置の前面にある LED 表示で通知します。

🕮 **メモ**：

設定温度をデフォルトのしきい値から推奨温度のしきい値に変更することを推奨します。

例

IRF スタックのメンバ装置 1 の hotspot 1 の温度アラームしきい値を設定します。

<Switch> system-view

[Switch] temperature-limit slot 1 hotspot 1 -10 50 60

関連コマンド

display environment

9.1.46 time at

Syntax

time at *time date*

undo time

デフォルト

設定なし

View

Schedule view

定義済みユーザロール

network-admin

パラメータ

time: スケジュールを自動で実行する時間を指定します。形式は *hh*:*mm* です。*hh* の設定範囲は 0～23 です。*mm* の設定範囲は 0～59 です。

date: スケジュールを自動で実行する実行日を指定します。形式は *MM*/*DD*/*YYYY* あるいは *YYYY*/*MM*/*DD* です。YYYY の設定範囲は 2000～2035 です。MM の設定範囲は 1～12 です。DD の設定範囲は月によって変わります。

説明

time at コマンドは 1 回のみのスケジュール自動実行機能の実行日と時間を指定します。

undo time コマンドはスケジュール自動実行機能の実行日と時間の設定を削除します。

指定時間（実行日と時間）は現在時刻よりも、後にする必要があります。

time at コマンド、**time once** コマンド、**time repeating** コマンドは、同時に設定することはできません。最後に設定したコマンドが適用されます。

例

2015 年 5 月 11 日の AM01:01 にスケジュール saveconfig を実行するように設定します。

<Switch> system-view

[Switch] scheduler schedule saveconfig

[Switch-schedule-saveconfig] time at 1:1 2015/05/11

関連コマンド

scheduler schedule

9.1.47 time once

Syntax

time once at *time* [**month-date** *month-day* | **week-day** *week-day*&<1-7>]

time once delay *time*

undo time

デフォルト

設定なし

View

Schedule view

定義済みユーザロール

network-admin

パラメータ

at *time*: スケジュールを実行する時間を指定します。形式は *hh*:*mm* です。*hh* の設定範囲は 0～23 です。*mm* の設定範囲は 0～59 です。

month-date *month-day*: 今月の日を指定します。設定範囲は 1～31 です。今月の日で指定した日が存在しない場合、次の月の該当する日が適用されます。

week-day *week-day*&<1-7>: スケジュールを実行する曜日を指定します。半角スペースで区切り、最高 7 週間まで Mon、Tue、Wed、Thu、Fri、Sat、Sun を指定します。

delay *time*: スケジュールを実行する時間を指定します。形式は *hh*:*mm* あるいは *mm* です。パラメータは 6 文字まで設定することができます。形式が *hh*:*mm* である場合、*mm* の設定範囲は 0～59 です。

説明

time once コマンドは 1 回のみのスケジュール自動実行機能の複数の実行日と時間を指定します。

undo time コマンドはスケジュール自動実行機能の実行日と時間の設定を削除します。

指定された時間が過ぎている場合、次の日の指定された時間が適用されます。

指定された月日が過ぎている場合、次の月の指定された日が適用されます。

指定された曜日が過ぎている場合、次の週の指定された曜日が適用されます。

time at コマンド、**time once** コマンド、**time repeating** コマンドは、同時に設定することはできません。最後に設定したコマンドが適用されます。

例

15:00 にスケジュール saveconfig を実行するように設定します。

<Switch> system-view

[Switch] scheduler schedule saveconfig

[Switch-schedule-saveconfig] time once at 15:00

```
Schedule starts at 15:00 5/11/2011.
```

今月の 15 日後の 15:00 にスケジュール saveconfig を実行するように設定します。

<Switch> system-view

[Switch] scheduler schedule saveconfig

[Switch-schedule-saveconfig] time once at 15:00 month-date 15

次の月曜日、金曜日の PM12:00 にスケジュール saveconfig を実行するように設定します。

<Switch> system-view

[Switch] scheduler schedule saveconfig

[Switch-schedule-saveconfig] time once at 12:00 week-day mon fri

10 分後にスケジュール saveconfig を実行するように設定します。

<Switch> system-view

[Switch] scheduler schedule saveconfig

[Switch-schedule-saveconfig] time once delay 10

関連コマンド

scheduler schedule

9.1.48 time repeating

Syntax

time repeating [**at** *time* [*date*]] **interval** *interval-time*

time repeating at *time* [**month-date** [*month-day* | **last**] | **week-day** *week-day*&<1-7>]

undo time

デフォルト

設定なし

View

Schedule view

定義済みユーザロール

network-admin

パラメータ

at *time*: スケジュールを実行する時間を指定します。形式は *hh*:*mm* です。*hh* の設定範囲は 0～23 です。*mm* の設定範囲は 0～59 です。指定しない場合、現在のシステム時間が指定されます。

date: スケジュールを定期的に自動で実行する開始日を指定します。形式は *MM*/*DD*/*YYYY* あるいは *YYYY*/*MM*/*DD* です。YYYY の設定範囲は 2000～2035 です。MM の設定範囲は 1～12 です。DD の設定範囲は月によって変わります。指定しない場合、指定した時間になったときの最初の日が指定されます。

interval *interval-time*: スケジュールを実行する時間を指定します。形式は *hh*:*mm* あるいは *mm* です。*mm* は 6 文字まで設定することができます。形式が *hh*:*mm* である場合、

mm の設定範囲は 0～59 です。形式が *mm* である場合、パラメータは 1 分以上にする必要があります。

month-date [*month-day* | **last**]: 今月の日を指定します。設定範囲は 1～31 です。今月の日で指定した日が存在しない場合、次の月の該当する日が適用されます。

week-day *week-day*&<1-7>: スケジュールを実行する曜日を指定します。半角スペースで区切り、最高 7 週間まで Mon、Tue、Wed、Thu、Fri、Sat、Sun を指定します。

説明

time repeating コマンドは定期的にスケジュールを実行する時間テーブルを指定します。

undo time コマンドはスケジュール自動実行機能の時間の設定を削除します。

time repeating [**at** *time* [*date*]] **interval** *interval-time* コマンドは 1 日内の指定した時間で定期的にスケジュールを実行するように設定します。

time repeating at *time* [**month-date** [*month-day* | **last**] | **week-day** *week-day*&<1-7>] コマンドは月あるいは曜日内の指定した日で定期的にスケジュールを実行するように設定します。

time at コマンド、**time once** コマンド、**time repeating** コマンドは、同時に設定することはできません。最後に設定したコマンドが適用されます。

例

本日の 8:00 から 1 時間ごとにスケジュール saveconfig を実行するように設定します。

<Switch> system-view

[Switch] scheduler schedule saveconfig

[Switch-schedule-saveconfig] time repeating at 8:00 interval 60

毎日の PM12:00 にスケジュール saveconfig を実行するように設定します。

<Switch> system-view

[Switch] scheduler schedule saveconfig

[Switch-schedule-saveconfig] time repeating at 12:00

毎月の 5 日の AM8:00 にスケジュール saveconfig を実行するように設定します。

<Switch> system-view

[Switch] scheduler schedule saveconfig

[Switch-schedule-saveconfig] time repeating at 8:00 month-date 5

毎月の最終日の AM8:00 にスケジュール saveconfig を実行するように設定します。

<Switch> system-view

[Switch] scheduler schedule saveconfig

[Switch-schedule-saveconfig] time repeating at 8:00 month-date last

各金曜日と各土曜日の AM8:00 にスケジュール saveconfig を実行するように設定します。

<Switch> system-view

[Switch] scheduler schedule saveconfig

[Switch-schedule-saveconfig] time repeating at 8:00 week-day fri sat

関連コマンド

scheduler schedule

9.1.49 user-role

Syntax

user-role *role-name*

undo user-role *role-name*

デフォルト

スケジュールには、スケジュール作成者のユーザロールがあります。

View

Schedule view

定義済みユーザロール

network-admin

パラメータ

role-name：ユーザロール名を指定します。設定範囲は 1～63 文字です。大文字、小文字を区別します。ユーザロールは、ユーザ定義または事前定義済みにすることができます。定義済みのユーザロールには、network-admin、network-operator、および level-0～level-15 があります。

説明

user-role コマンドはユーザロールをスケジュールに割り当てます。

undo user-role コマンドはスケジュールからユーザロールを削除します。

スケジュールには 1 つ以上のユーザロールが必要です。スケジュール内のコマンドは、スケジュールの 1 つ以上のユーザ役割によって許可されていれば実行できます。ユーザロールの詳細については、セクション 1 *はじめに オペレーションマニュアル*の“*RBAC*”を参照してください。

スケジュールは最大 64 のユーザ役割を持つことができます。制限に達すると、追加のユーザ役割をスケジュールに割り当てることはできません。

例

スケジュール **test** にユーザロール **rolename** を割り当てます。

<Switch> system-view

[Switch] scheduler schedule test

[Switch-schedule-test] user-role rolename

関連コマンド

- **command**
- **scheduler schedule**

目次

このセクションのページは **1-x-x** です。

10 章 Python 10-1
.....10-1
10.1 Python 設定コマンド 10-1
10.1.1 exit() 10-1
10.1.2 python 10-1
10.1.3 python *filename* 10-2

10章 Python

10.1 Python設定コマンド

10.1.1 exit()

Syntax

exit()

View

Python shell

定義済みユーザロール

network-admin

説明

exit()コマンドを使用して、Python shell を終了します。

Python shell から user view に戻るには、**quit** コマンドは使用できません。**exit()**コマンドを使用してください。

例

Python shell を終了します。

```
Python 2.7.3 (default)
[GCC 4.4.1] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>>
>>> exit()
<Switch>
```

10.1.2 python

Syntax

python

View

User view

定義済みユーザロール

network-admin

説明

python コマンドで Python shell に移行します。

Python shell では、以下を使用可能です。

- Python 2.7 コマンド
- Python 2.7 標準 API
- Comware 7 拡張 API

例

Python shell に移行します。

<Switch> python

```
Python 2.7.3 (default)
[GCC 4.4.1] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

10.1.3 python *filename*

Syntax

python *filename* [*param*]

View

System view

定義済みユーザロール

network-admin

パラメータ

filename: 装置に保存されている Python スクリプトファイル名を指定します。スクリプト名は、大文字、小文字を区別し、拡張子は“.py”である必要があります。拡張子“.py”は、大文字、小文字を区別しません。

param: スクリプトに渡すパラメータを指定します。複数指定するには、スペース文字で区切ります。

説明

python *filename* コマンドで Python スクリプトを実行します。

Python スクリプト実行中は、他の操作はできません。

スクリプトの文法が正しい事を確認してください。文法エラーが発生すると、スクリプトの実行は停止します。

スクリプト実行中、対話形式のコマンドではデフォルトが使用されます。ユーザー入力待ちで停止しません。

例

Python スクリプト test.py を実行します。

<Switch> python test.py 1 2

```
['/flash:/test.py', '1', '2']
```

QX-S5100G シリーズ Ethernet スイッチ

コマンドマニュアル

2.IRF スタック

本マニュアルは以下に示す章で構成されています。

01-IRF スタック

目次

このセクションのページは **2-x-x** です。

1 章 IRF スタック 1-1
1.1 IRF スタック設定コマンド 1-1
1.1.1 display irf 1-1
1.1.2 display irf configuration 1-2
1.1.3 display irf link 1-4
1.1.4 display irf topology 1-5
1.1.5 display irf-port load-sharing mode 1-6
1.1.6 display mad 1-8
1.1.7 irf auto-update enable 1-10
1.1.8 irf domain 1-11
1.1.9 irf link-delay 1-12
1.1.10 irf mac-address persistent 1-13
1.1.11 irf member description 1-15
1.1.12 irf member priority 1-15
1.1.13 irf member renumber 1-16
1.1.14 irf-port 1-18
1.1.15 irf-port-configuration active 1-18
1.1.16 mad arp enable 1-20
1.1.17 mad bfd enable 1-21
1.1.18 mad enable 1-23
1.1.19 mad exclude interface 1-24
1.1.20 mad ip address 1-26
1.1.21 mad restore 1-27
1.1.22 port group interface 1-28

1章 IRF スタック

1.1 IRFスタック設定コマンド

1.1.1 display irf

Syntax

display irf

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display irf コマンドは IRF スタックユニットの情報を表示します。

例

表示されるフィールドの説明を表 1-1 に示します。

表 1-1 コマンド出力

フィールド	説明
MemberID	IRFスタックのメンバIDです。 ● メンバIDはアスタリスク（*）で表示されます。 ● ログインしている装置のメンバIDは(+)で表示されます。
Role	IRFスタックユニットのメンバ装置の役割です。 ● **Standby**–メンバ装置です。 ● **Master**–Master装置です。 ● **Loading**–装置がソフトウェアイメージを読み込んでいます。
Priority	IRFスタックのメンバのプライオリティです。
CPU-MAC	装置のCPU-MACアドレスです。

フィールド	説明
Description	メンバ装置の説明です。 ● 説明が設定されていない場合、ハイフン線（-----）と表示されます。 ● 文字の最大数を超過している場合、超過している個所が省略され、（…）と表示されます。すべての説明を表示する場合、**display current-configuration**コマンドを使用します。
Auto upgrade	ソフトウェアオートアップグレード機能の状態です。 ● **yes**–有効です。MasterはソフトウェアイメージをIRFスタックユニットに追加する装置に自動的に送信します。 ● **no**–無効です。IRFスタックユニットへ追加する装置に、Masterと同一のソフトウェアイメージを手動でアップグレードする必要があります。ソフトウェアイメージが異なる場合、新しい装置はIRFスタックユニットに加入することができません。
MAC persistent	IRFスタックのBridge MACアドレスを保持する設定です。 ● **6 min**–Master装置が離脱したのち、IRFスタックユニットのBridge MACアドレスは6分間変更しません。 ● **always**–Masterが離脱した後、IRFスタックユニットのBridge MACアドレスは変更しません。 ● **no**–Masterが離脱した後、すぐに新しいMasterのBridge MACアドレスに切り替わります。
Domain ID	IRFスタックユニットのドメインIDです。IRFスタックユニットに割り当てたドメインIDは、IRFスタックユニットを識別するために使用されます。

関連コマンド

- **display irf configuration**
- **display irf topology**

1.1.2 display irf configuration

Syntax

display irf configuration

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display irf configuration コマンドは基本的な IRF スタックの設定を表示します。

例

すべてのメンバの基本的な IRF スタックの設定を表示します。

<Switch> display irf configuration

```
MemberID  NewID    IRF-Port1                IRF-Port2
2         2       GigabitEthernet2/0/49   GigabitEthernet2/0/51
5         5       GigabitEthernet5/0/49   GigabitEthernet5/0/51
                  GigabitEthernet5/0/50
10        10      GigabitEthernet10/0/49  GigabitEthernet10/0/51
                                          GigabitEthernet10/0/52
```

表 1-2 コマンド出力

フィールド	説明
MemberID	装置の現在のメンバIDです。
NewID	装置に割り当てられたメンバIDです。メンバIDは再起動後に適用されます。
IRF-Port1	IRFスタックポート1に関連付けられたIRFスタック物理ポートです。再起動後に適用されます。IRFスタック物理ポートがIRFスタックポート1に関連付けられていない場合、**disable** と表示されます。
IRF-Port2	IRFスタックポート2に関連付けられたIRFスタック物理ポートです。再起動後に適用されます。IRFスタック物理ポートがIRFスタックポート2に関連付けられていない場合、**disable** と表示されます。

関連コマンド

- **display irf**
- **display irf topology**

1.1.3 display irf link

Syntax

display irf link

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display irf link コマンドは IRF スタックのリンク情報を表示します。

例

IRF スタックのリンク情報を表示します。

<Switch> display irf link

```
Member 1
 IRF Port   Interface                    Status
 1          disable                      --
 2          GigabitEthernet1/0/49        UP
            GigabitEthernet1/0/50        ADM
Member 2
 IRF Port   Interface                    Status
 1          GigabitEthernet2/0/49        UP
            GigabitEthernet2/0/50        DOWN
 2          disable                      --
```

表 1-3 コマンド出力

フィールド	説明
Member *ID*	IRFスタックのメンバIDです。
IRF Port	IRFスタックポート番号です。 ● **1**－IRFスタックポート1です。 ● **2**－IRFスタックポート2です。
Interface	IRFスタックポートに関連付けられたIRFスタック物理ポートです。IRFスタック物理ポートがIRFスタックポートに関連付けられていない場合、**disable**と表示されます。

フィールド	説明
Status	IRFスタック物理ポートのリンク状態です。 ● **UP**－リンクがアップ状態です。 ● **DOWN**－リンクがダウン状態です。 ● **ADM**－ポートが**shutdown**コマンドにより手動でシャットダウンしています。

1.1.4 display irf topology

Syntax

display irf topology

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display irf topology コマンドは IRF スタックユニットのトポロジ情報を表示します。

例

表示されるフィールドの説明を表 1-4 に示します。

表 1-4 コマンド出力

フィールド	説明
IRF-Port1	リンク状態、隣接情報を含むIRFスタックポート1の情報です。
IRF-Port2	リンク状態、隣接情報を含むIRFスタックポート2の情報です。
MemberID	IRFスタックのメンバIDです。

フィールド	説明

Link	IRFスタックポートのリンク状態です。
	• **UP**–IRFスタックのリンクがアップ状態です。
	• **DOWN**–IRFスタックのリンクがダウン状態です。ポートの物理リンクがない、あるいは**irf-port-configuration active**コマンドで動作していません。
	• **DIS**–IRFスタックポートに関連付けられたIRFスタック物理ポートがありません。**port group interface**コマンドで少なくとも1つのIRFスタック物理ポートをIRFスタックポートに割り当てる必要があります。
	• **TIMEOUT**–IRFスタックのhelloパケットの送信がタイムアウトしています。接続の故障などリンクを確認してください。
	• **ISOLATE**–装置がIRFスタックから分裂しています。
	  • IRFスタックユニットが装置をサポートしていません。
	  • メンバ装置の最大数が上限を超過しました。

neighbor	装置のIRFスタックのメンバIDがIRFスタックポートに接続しています。 もし装置がポートに接続されていない場合、3つハイフン（---）が表示されます。
Belong To	IRFスタックユニットがあります。IRFスタックユニットのMasterのCPU-MACアドレスで示します。

関連コマンド

- **display irf**
- **display irf configuration**

1.1.5 display irf-port load-sharing mode

Syntax

display irf-port load-sharing mode [**irf-port** [*member-id*/*port-number*]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

irf-port: IRF スタックポートのロードシェアリングモードを表示します。

member-id/*port-number*: IRF スタックポート番号を指定します。*member-id* は IRF スタックのメンバ ID です。*port-number* はメンバ装置の IRF スタックポートのインデックス番号(1 あるいは 2)を示します。

説明

display irf-port load-sharing mode コマンドは IRF スタックポートのロードシェアリングモードを表示します。

IRF スタックリンクのグローバルのロードシェアリングモードを表示する場合、パラメータを使用しないで実行します。

各 IRF スタックユニットの IRF スタックポートで使用されるロードシェアリングモードを表示する場合、IRF スタックポートを指定しないで **irf-port** キーワードを指定します。もし IRF スタックポートが up 状態でない場合、No IRF link exists.と表示されます。

指定した IRF スタックポートで使用されるロードシェアリングモードを表示する場合、**irf-port** と *member-id*/*port-number* を指定します。

QX-S5100G シリーズはデフォルトのロードシェアリングモードのみサポートしています。デフォルトでは L2 トラフィックは送信元 MAC と宛先 MAC、L3 トラフィックは送信元 IP と宛先 IP でロードシェアリングを行います。

例

IRF スタックリンクのグローバルでのロードシェアリングモードを表示します。デフォルトのグローバルでのロードシェアリングモードが適用されます。

<Switch> display irf-port load-sharing mode

```
irf-port Load-Sharing Mode:
Layer 2 traffic: packet type-based sharing
Layer 3 traffic: packet type-based sharing
```

表 1-5 コマンド出力

フィールド	説明
irf-port Load-Sharing Mode	IRFスタックリンクのグローバルでのロードシェアリングモードです。 • グローバルのIRFスタックのロードシェアリングモードが設定されていない場合、デフォルトのグローバルでのロードシェアリングモードが適用されます。 • ユーザ定義のロードシェアリングモードが設定されている場合、設定されたモードが適用されます。

フィールド	説明
irf-port1/1 Load-Sharing Mode	IRFスタックポート1/1のIRFスタックリンクのロードシェアリングモードです。 • ポートのロードシェアリングモードが設定されていない場合、グローバルでのIRFスタックリンクのロードシェアリングモードが適用されます。 • ポートのロードシェアリングモードが設定されている場合、設定されたモードが適用されます。
Layer 2 traffic: packet type-based sharing	IPヘッダがないトラフィックのデフォルトでのロードシェアリングモードです。デフォルトで、このトラフィックタイプのパケットをもとにして負荷分散を行います。
Layer 3 traffic: packet type-based sharing	非TCP/UDPのIPパケットのデフォルトのロードシェアリングモードです。デフォルトで、このトラフィックタイプのパケットをもとにして負荷分散を行います。
destination-ip address source-ip address	設定されたグローバルのロードシェアリングモードです。この宛先IPアドレス、送信元IPアドレスをもとにして負荷分散を行います。
destination-mac address	設定されたIRFスタックポート1/1のロードシェアリングモードです。宛先MACアドレスをもとにして負荷分散を行います。

1.1.6 display mad

Syntax

display mad [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

verbose: 詳細な MAD 情報を表示します。指定しない場合、MAD の設定が有効あるいは無効かどうかを表示します。

説明

display mad コマンドは MAD の状態と設定を表示します。

例

MAD 情報の概要を表示します。

<Switch> display mad

```
MAD ARP enabled.
MAD ND disabled.
MAD LACP disabled.
MAD BFD disabled.
```

MAD 情報の詳細を表示します。

<Switch> display mad verbose

```
Multi-active recovery state: No
Excluded ports(user-configured):
  Bridge-Aggregation4
  Vlan-interface999
Excluded ports(system-configured):
IRF physical interfaces:
  GigabitEthernet1/0/49
  GigabitEthernet1/0/50
  GigabitEthernet1/0/51
  GigabitEthernet1/0/52
Member interfaces of excluded interface Bridge-Aggregation 4:
  GigabitEthernet1/0/11
  GigabitEthernet2/0/11
MAD ARP enabled interface:
  Vlan-interface2
MAD ND disabled.
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 disabled.
```

表 1-6 コマンド出力

フィールド	説明
MAD ARP enabled.	ARP MADの状態です。ARP MADが無効の場合は、**MAD ARP disabled**と表示します。
MAD ND disabled.	ND MADの状態です。 現在のソフトウェアバージョンはサポートしていません。
MAD LACP disabled.	ARP MADの状態です。ARP MADが無効の場合は、**MAD LACP disabled**と表示します。

フィールド	説明
MAD BFD disabled.	BFD MADの状態です。BFD MADが場合は、**MAD BFD disabled** と表示します。
Multi-active recovery state	IRFスタックユニットがRecovery状態であるかどうかを示します。 ● **Yes**– IRFスタックユニットがRecovery状態です。IRFスタックユニットが複数のIRFスタックユニットに分裂したとMADが検出したとき、1つのIRFスタックユニットにトラフィックを転送します。ほかのすべてのIRFスタックユニットがRecovery状態に設定されます。Recovery状態ではMADは、IRFスタック物理ポートとシャットダウンに設定されていないポートを除いてIRFスタックユニットのすべてのIRFスタック物理ポートをシャットダウンします。 ● **No**–IRFスタックユニットがRecovery状態でありません。アクティブでトラフィックを転送できます。
Excluded ports(user-configured)	IRFスタックユニットがRecovery状態へ遷移時にシャットダウンしないよう、手動で設定されたポートです。
Excluded ports(system-configured)	IRFスタックユニットがRecovery状態へ遷移時にシャットダウンしないよう、デフォルトで設定されたポートです。このポートはユーザが設定することができません。 システムで設定されたポートは以下です。 ● IRFスタック物理ポートです。 ● アグリゲートインタフェースがMADシャットダウンのアクションから除外されている場合、アグリゲートインタフェースのメンバインタフェースです。
MAD status	MAD動作モードの状態です。 ● **Normal**–MADが正常に動作しています。 ● **Faulty**–MADがインタフェースあるいはポートで正常に動作していません。インタフェースあるいはポートの接続あるいは設定を確認してください。
Member ID	ローカル装置のIRFスタックのメンバIDです。
Port	LACP MADで使用されるアグリゲートインタフェースのメンバポートです。

1.1.7 irf auto-update enable

Syntax

irf auto-update enable

undo irf auto-update enable

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

irf auto-update enable コマンドは、すべての IRF スタックユニットのメンバのソフトウェアを自動で更新する機能を有効にします。

undo irf auto-update enable コマンドはソフトウェア自動更新機能を無効にします。

このコマンドで、IRF スタックユニットの Master 装置の現在のソフトウェアイメージを IRF スタックユニットに追加するすべての装置に自動的に伝えます。

ソフトウェア自動更新機能を有効にする場合、装置に新しいシステムソフトウェアのための有効な領域があることを確認してください。適切な領域がない場合、装置は現在のソフトウェアイメージを自動的に削除します。もし再利用された空き領域が十分でない場合、装置はソフトウェア自動更新機能を完了することができません。装置を再起動し、ファイルを削除するために Boot メニューに移行してください。

例

ソフトウェア自動更新機能を有効にします。

<Switch> system-view

[Switch] irf auto-update enable

1.1.8 irf domain

Syntax

irf domain *domain-id*

undo irf domain

デフォルト

0

View

System view

定義済みユーザロール

network-admin

パラメータ

domain-id: IRF スタックユニットのドメイン ID を指定します。設定範囲は 0～4294967295 です。

説明

irf domain コマンドは IRF スタックユニットにドメイン ID を割り当てます。

undo irf domain コマンドはデフォルトに戻します。

1 つの IRF スタックユニットは 1 つの IRF スタックのドメインを形成します。IRF スタックは IRF スタックユニットを一意に識別し、別の IRF スタックユニットからの干渉を防ぐために IRF スタックのドメイン ID を使用します。

1 つの IRF スタックユニットが LACP MAD、ARP MAD の中継装置として別の IRF スタックユニットを使用する場合、IRF スタック分裂の検出失敗を避けるために、中継装置と異なるドメイン ID を割り当てなければなりません。間違って検出されると、IRF スタックの分裂を引き起こします。

IRF スタックユニットは IRF スタックのドメイン ID が 1 つのみあります。**irf domain**、**mad enable**、**mad arp enable** コマンドで IRF スタックのドメイン ID を変更することができます。これらのコマンドで設定された IRF スタックのドメイン ID は互いに上書きされます。

例

IRF スタックのドメイン ID を 10 に設定します。

<Switch> system-view

[Switch] irf domain 10

1.1.9 irf link-delay

Syntax

irf link-delay *interval*

undo irf link-delay

デフォルト

500 ミリ秒

View

System view

定義済みユーザロール

network-admin

パラメータ

interval: リンクレイヤが IRF スタックポートのリンクダウンのイベントを報告する遅延時間です。設定範囲は 0～10000 ミリ秒です。0 に設定した場合、遅延なくリンクダウンのイベントが報告されます。

説明

irf link-delay コマンドは IRF スタックポートのリンクダウンのイベントを報告する遅延時間を設定します。

設定をデフォルトに戻す場合は、**irf link-delay** 500 コマンドを実行してください。**undo irf link-delay** は 4000 ミリ秒で動作します。

装置は IRF スタックポートのリンクステータス変更イベントの報告を遅延させますが、IRF スタック物理インタフェースの報告は遅延しません。

BFD が設定されている場合、link-delay を 0 秒に設定してください。

🕮 **メモ**:

undo irf link-delay コマンドを実行しても、デフォルト設定には戻りません。**undo** コマンドを実行した場合は、4000 ミリ秒の遅延時間で動作する設定となります。

例

IRF スタックポートのリンクダウンのイベントを報告する遅延時間を 300 ミリ秒に設定します。

<Switch> system-view

[Switch] irf link-delay 300

1.1.10 irf mac-address persistent

Syntax

irf mac-address persistent { **always** | **timer** }

undo irf mac-address persistent

デフォルト

Master 装置が離脱した後、IRF スタックユニットの Bridge MAC アドレスは 6 分間変更されません。

View

System view

定義済みユーザロール

network-admin

パラメータ

always: IRF スタックユニットの Bridge MAC アドレスを変更しません。新しい Master の選定が行われたのち IRF スタックユニットは Bridge MAC アドレスを変更しません。

timer: 新しい Master の選定が行われたのち IRF スタックユニットの Bridge MAC アドレスは 6 分間変更しません。時間以内に IRF スタックユニットに装置が再加入した場合、IRF スタックの Bridge MAC アドレスを変更しません。時間以内に IRF スタックユニットに装置が再加入しない場合、IRF スタックユニットは新しい Master の Bridge MAC アドレスを使用します。

説明

irf mac-address persistent コマンドは IRF スタックの Bridge MAC アドレスを保持するように設定します。

undo irf mac-address persistent コマンドは Master の離脱後、すぐに Bridge MAC アドレスを変更します。

ARP MAD が使用される場合、IRF スタックの Bridge MAC アドレスの保持を無効にするため、**undo irf mac-address persistent** コマンドを使用します。

デイジーチェーン構成の IRF スタックが上位または下位の装置とリンクアグリゲーションで接続されている場合、Bridge MAC アドレスの変更によって Master の再選定で転送遅延やパケットロスを引き起こさないように **irf mac-address persistent always** コマンドを設定してください。

Bridge MAC アドレスの変更によって Master の再選定で転送遅延やパケットロスを引き起こさないように **irf mac-address persistent always** コマンドを設定してください。

デフォルトで IRF スタックユニットは Master 装置の Bridge MAC アドレスを使用します。

Bridge MAC アドレスの重複を防ぐため、IRF スタックユニットは Master の離脱後、自動的に Bridge MAC アドレスを変更することができます。しかし変更を行うとサービスの中断を引き起こします。ネットワークの状況に依存して、Master の離脱後に IRF スタックユニットの Bridge MAC アドレスを保持するか変更するかを設定することができます。

2 つの IRF スタックユニットが同じ Bridge MAC アドレスを持っている場合、結合することができません。

例

IRF スタックの Bridge MAC アドレスの保持時間を永久保持に設定します。

<Switch> system-view

[Switch] irf mac-address persistent always

1.1.11 irf member description

Syntax

irf member *member-id* **description** *text*

undo irf member *member-id* **description**

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

member-id: IRF スタックのメンバ ID を指定します。

text: IRF スタックのメンバの説明を設定します。設定範囲は 1～127 文字です。

説明

irf member description コマンドは IRF スタックのメンバの説明を設定します。

undo irf member description コマンドはデフォルトに戻します。

例

IRF スタックのメンバ 1 の説明に F1Num001 を設定します。

<Switch> system-view

[Switch] irf member 1 description F1Num001

1.1.12 irf member priority

Syntax

irf member *member-id* **priority** *priority*

undo irf member *member-id* **priority**

デフォルト

1

View

System view

定義済みユーザロール

network-admin

パラメータ

member-id: IRF スタックのメンバ ID を指定します。設定範囲は 1～10 です。

priority: プライオリティを指定します。設定範囲は 1～32 です。プライオリティの値が高い場合、プライオリティは高くなります。Master はプライオリティが高い装置が優先されます。

説明

irf member priority コマンドは IRF スタックのメンバのプライオリティを変更します。

undo irf member priority コマンドはデフォルトに戻します。

メンバのプライオリティの変更は次回の Master の選定に影響します。Master の選定は開始しません。

例

IRF スタックのメンバ 2 のプライオリティを 32 に設定します。

<Switch> system-view

[Switch] irf member 2 priority 32

1.1.13 irf member renumber

Syntax

irf member *member-id* **renumber** *new-member-id*

undo irf member *member-id* **renumber**

デフォルト

1

View

System view

定義済みユーザロール

network-admin

パラメータ

member-id: IRF スタックのメンバ ID を指定します。設定範囲は 1～10 です。

new-member-id: IRF スタックのメンバに新しい ID を割り当てます。設定範囲は 1～10 です。

説明

⚠ **注意：**

IRF スタックのメンバ ID の変更を行うと、再起動により IRF スタック物理ポートの設定を含むメンバ ID に関する設定が変更され、パケットロスが発生する可能性があります。

irf member renumber コマンドは装置の IRF スタックのメンバ ID を変更します。

undo irf member renumber コマンドは装置の IRF スタックのメンバ ID をもとに戻します。

メンバ ID を適用する場合、IRF スタックのメンバの再起動が必要です。IRF スタックユニットの設定を行う前に IRF スタックのメンバ ID の割り当てを検討し、ほかの機能を設定する前に、メンバ ID を変更してください。

装置を IRF スタックユニットに追加するとき、装置に一意の IRF スタックのメンバ ID を割り当てる必要があります。IRF スタックのメンバ ID が IRF スタックユニットで使用されている場合、装置は IRF スタックユニットに加入することができません。

IRF スタックのメンバ装置間のメンバ ID の置換は、予期しない設定の変更やデータロスを引き起こす可能性があります。たとえば、Device A、Device B の IRF スタックのメンバ ID がそれぞれ 2、3 であるとします。メンバ ID を置換した後、ポートの設定も変更されます。

例

IRF スタックのメンバ ID を 1 から 2 に変更します。

<Switch> display irf

[Switch] irf member 1 renumber 2

```
Renumbering the member ID may result in configuration change or loss.
Continue?[Y/N]Y
```

装置の再起動を行う前に、変更の中断を行います。

[Switch] undo irf member 1 renumber

```
Renumbering the member ID may result in configuration change or loss.
Continue?[Y/N]y
```

irf member 1 renumber 2 コマンドを実行したのち、装置を再起動した場合、メンバ ID は 2 となります。**undo irf member 1 renumber** コマンドはメンバ ID を 1 に戻すことはできません。メンバ ID を再度設定する場合、**irf member 2 renumber 1** コマンドを使用する必要があります。

1.1.14 irf-port

Syntax

irf-port *member-id*/*port-number*

undo irf-port *member-id*/*port-number*

View

System view

定義済みユーザロール

network-admin

パラメータ

member-id: IRF スタックのメンバ装置を指定します。

irf-port-number: メンバ装置の IRF スタックポートのインデックスを示します。1 あるいは 2 です。

説明

irf-port コマンドは IRF port view に移行します。

undo irf-port コマンドは IRF スタックポートのすべてのポートの割り当てを削除します。

IRF スタック接続の IRF スタックポートに IRF スタック物理ポートを割り当てるため、IRF port view に移行する必要があります。

例

IRF-port 2/1 view に移行します。

<Switch> system-view

[Switch] irf-port 2/1

[Switch-irf-port2/1]

関連コマンド

port group interface

1.1.15 irf-port-configuration active

Syntax

irf-port-configuration active

View

System view

定義済みユーザロール

network-admin

説明

irf-port-configuration active コマンドは装置に設定したすべての IRF スタックポートの設定を有効にします。

2つの装置間の IRF スタック物理ポートを接続し、IRF スタックポートに関連付けたのち、IRF スタックポートの設定を有効にするために、このコマンドを使用します。このコマンドは 2 つの装置を 1 つの IRF スタックユニットに結合します。

システムは以下の状況において自動で IRF スタックポートの設定を有効にします。

- 装置が起動するコンフィグレーションファイルが IRF スタックポートの関連付けを含みます。
- IRF スタックが形成したのち、IRF スタックポートに IRF スタック物理ポートを関連付けます。

例

ポートが DIS 状態になったとき、IRF スタックポート 1/2 の設定を有効にします。

IRF スタックポート 1/2 を GigabitEthernet 1/0/49 に関連付けます。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/49

[Switch-GigabitEthernet1/0/49] shutdown

[Switch-GigabitEthernet1/0/49] quit

[Switch] irf-port 1/2

[Switch-irf-port1/2] port group interface 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 gigabitethernet 1/0/49

[Switch-GigabitEthernet1/0/49] undo shutdown

[Switch-GigabitEthernet1/0/49] quit

IRF スタックのセットアップを行うため、以下の作業を行います。

IRF スタックの設定を完了した後、設定を保存します。

[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.
```

IRF スタックポートを有効にします。

[Switch] irf-port-configuration active

1.1.16 mad arp enable

Syntax

mad arp enable

undo mad arp enable

デフォルト

無効

View

VLAN interface view

定義済みユーザロール

network-admin

説明

mad arp enable コマンドは ARP MAD を有効にします。

undo mad arp enable コマンドは ARP MAD を無効にします。

ARP MAD は拡張 ARP パケットを使用して、マルチアクティブの衝突を検知します。

ARP MAD は BFD MAD と一緒に設定することができますが、LACP MAD と一緒に設定することはできません。

ARP MAD を設定する場合、以下の制限とガイドラインに従ってください。

カテゴリ	制限とガイドライン

ARP MAD VLAN	• VLANインタフェース1でARP MADを設定することはできません。
	• 中継装置を使用する場合、中継装置とIRFスタックユニットの両方で以下の作業を行ってください。
	  • ARP MADのVLAN、VLANインタフェースを作成してください。
	  • ARP MAD VLANにARP MADリンクのポートを割り当ててください。
	• ARP MADのVLANはほかの目的で使用しないでください。

カテゴリ	制限とガイドライン
ARP MADと機能の設定	中継装置を使用する場合、以下の要件に従ってください。 ● 転送状態のARP MADリンクを1つのみ存在させるため、IRFスタックユニットと中継装置の間でスパニングツリー機能を動作させてください。スパニングツリー機能の詳細は、オペレーションマニュアルのセクション3 *アクセス "STP"* を参照してください。 ● IRFスタックユニットからMasterが離脱した際にbridge MACアドレスが即座に変更されるようにIRFスタックユニットを設定してください。 ● IRFスタックユニットに中継装置がある場合、分裂を間違って検出しないようにARP MADを有効にしたIRFスタックユニットと異なるドメインIDを割り当ててください。

例

VLAN インタフェース 3 で ARP MAD を有効にします。

<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
```

関連コマンド

irf domain

1.1.17 mad bfd enable

Syntax

mad bfd enable

undo mad bfd enable

デフォルト

無効

View

VLAN interface view

定義済みユーザロール

network-admin

説明

mad bfd enable コマンドは BFD MAD を有効にします。

undo mad bfd enable コマンドは BFD MAD を無効にします。

BFD MAD は BFD プロトコルを使用して、マルチアクティブの衝突を検知します。MAD メカニズムは中間装置の存在に関わらず、動作させることができます。

BFD MAD は ARP MAD と一緒に設定することができますが、LACP MAD と一緒に設定することはできません。

VLAN インタフェースで BFD MAD を設定するとき、以下のガイドラインに従います。

カテゴリ	制限とガイドライン
BFD MAD VLAN	• VLANインタフェース1でBFD MADを有効にすることはできません。 • 中継装置を使用する場合、BFD MADリンクのポートは装置のBFD MADのVLANに接続してください。 • ネットワークのIRFスタックユニットは異なるBFD MAD VLANを使用してください。 • 正しいトラフィックの転送を行うため、BFD MAD VLANはBFD MADリンクのポートのみを使用してください。もしBFD MADリンクのポートでない場合、BFD MAD VLANからのポートを取り除いてください。たとえば**port trunk permit vlan all**コマンドですべてのVLANにポートが割り当てられている場合、BFD MAD VLANからポートを除外するため、**undo port trunk permit**コマンドを使用してください。
BFD MAD VLANと機能の互換性	BFD MAD のVLANをほかの用途で使用しないでください。 • BFD MADで使用されるVLANインタフェースでは**mad bfd enable**コマンドと**mad ip address**コマンドのみ設定できます。もしほかの機能を設定する場合、BFD MADとインタフェースのほかの機能の両方は正常に動作しない可能性があります。 • BFD MADのVLANのポートでは、スパニングツリー機能を無効にしてください。MAD機能はスパニングツリー機能と同時に使用することはできません。

カテゴリ	制限とガイドライン
MAD IPアドレス	● BFD MADを有効にしたVLANインタフェースでMADのIPアドレスを設定する場合、**ip address**コマンドの代わりに**mad ip address**コマンドを使用してください。 ● BFD MAD が有効なVLANインタフェースのすべてのMAD IPアドレスは、同じサブネット上にある必要があります。

例

VLAN インタフェース 3 で BFD MAD を有効にします。

<Switch> system-view

[Switch] interface vlan-interface 3

[Switch-Vlan-interface3] mad bfd enable

1.1.18 mad enable

Syntax

mad enable

undo mad enable

デフォルト

無効

View

Aggregate interface view

定義済みユーザロール

network-admin

説明

mad enable コマンドは LACP MAD を有効にします。

undo mad enable コマンドは LACP MAD を無効にします。

LACP MAD は拡張 LACP パケットを使用して、マルチアクティブの衝突を検知します。MAD 機能は拡張 LACP パケットをサポートする中継装置が必要です。

LACP MAD は、BFD MAD、ARPMAD とは異なる方法で衝突を処理します。LACP MAD は、IRF スタックユニットでその他の MAD と併用しないでください。BFD MAD、ARP MAD は併用できます。

IRF スタックユニットと中継装置間ですべての IRF スタックメンバ装置に接続するダイナミックリンクアグリゲーショングループを設定する必要があります。

ダイナミックリンクアグリゲーションを有効にするため、アグリゲーションインタフェースで **link-aggregation mode dynamic** コマンドを設定します。

1 つの IRF スタックユニットが、LACP MAD の中継装置として別の IRF スタックユニットを使用する場合、正しく検出を行うため、異なるドメイン ID の 2 つの IRF スタックユニットを割り当てる必要があります。そうでない場合、IRF スタックの分裂の検出が誤って行われます。

mad enable コマンドを使用するとき、システムはドメイン ID を入力するように画面が表示されます。現在のドメイン ID を変更しない場合、Enter キーを押下します。

IRF スタックユニットは 1 つの IRF スタックのドメイン ID のみサポートします。**irf domain**、**mad enable**、**mad arp enable** のコマンドを使用して IRF スタックのドメイン ID を変更することができます。

例

Bridge-Aggregation 1 でレイヤ 2 ダイナミックアグリゲートインタフェースに LACP MAD を有効にします。

<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.
```

関連コマンド

irf domain

1.1.19 mad exclude interface

Syntax

mad exclude interface *interface-type interface-number*

undo mad exclude interface *interface-type interface-number*

デフォルト

IRF スタック物理ポートを除いて Recovery 状態の IRF スタックユニットのすべてのネットワークポートがシャットダウンです。

システムは自動で以下のポートを除外します。

- IRF スタック物理ポート
- アグリゲートインタフェースがシャットダウンから除外されている場合、アグリゲートインタフェースのメンバインタフェース

View

System view

定義済みユーザロール

network-admin

パラメータ

interface-type interface-number: ポートのタイプと番号を指定します。

説明

mad exclude interface コマンドは、multi-active 衝突の検出により Recovery 状態の IRF スタックユニットのすべてのネットワークポートをシャットダウンしないように設定します。

undo mad exclude interface コマンドは IRF スタック物理ポートの MAD のアクションをデフォルトに戻します。

Telnet 接続のような特別の目的のためにポートの状態を UP に継続する必要がある場合、シャットダウンを行うアクションからポートを除外します。不正なトラフィックの転送を防ぐため、Telnet、MAD で使用するポートを除いたポートを除外しないことを推奨します。

MAD によってシャットダウンとなったポートは、メンバ装置が回復した IRF スタックユニットに加入するために再起動するときに、up となります。現在の Master が故障あるいはほかの例外処理が発生したために自動回復が行われなかった場合、**mad restore** コマンドを使用して手動でメンバ装置とポートを up 状態に回復します。

例

MAD が Recovery 状態に遷移したときにシャットダウンとならないように GigabitEthernet 1/0/1 を除外します。

<Switch> system-view

[Switch] mad exclude interface gigabitethernet 1/0/1

関連コマンド

mad restore

1.1.20 mad ip address

Syntax

mad ip address *ip-address* { *mask* | *mask-length* } **member** *member-id*

undo mad ip address *ip-address* { *mask* | *mask-length* } **member** *member-id*

デフォルト

設定なし

View

VLAN interface view

定義済みユーザロール

network-admin

パラメータ

ip-address: ドットが付いた 10 進数で IP アドレスを指定します。IP アドレスは BFD 検出の IRF スタックメンバに割り当てられ、MAD IP アドレスと呼ばれます。

mask: ドットが付いた 10 進数でサブネットマスクを指定します。

mask-length: サブネットマスク長を指定します。設定範囲は 0～32 です。

member *member-id*: IRF スタックのメンバ ID を指定します。

説明

mad ip address コマンドは BFD MAD の VLAN インタフェースの IRF スタックのメンバに MAD IP アドレスを割り当てます。

undo mad ip address コマンドは MAD IP アドレスを削除します。

BFD MAD を使用するため、各 IRF スタックのメンバの BFD MAD が有効な VLAN インタフェースで MAD IP アドレスを設定します。すべての MAD IP アドレスが同一サブネット上にある必要があります

この問題を防ぐため、BFD MAD が有効な VLAN インタフェースで IP アドレスを設定するコマンドを使用することができます。ほかのコマンドを使用して IP アドレスを設定しないでください。（たとえば **ip address** コマンド）

Master は送信元 IP アドレスとして MAD IP アドレスを使用することで、ほかのメンバ装置と BFD セッションを確立しようとします。

- もし IRF スタックユニットが正常に動作しているとき、Master の MAD IP アドレスのみが有効です。Master はほかのメンバと BFD セッションを確立することができません。**display bfd session** コマンドを実行した場合、BFD セッションの状態はダウンです。
- IRF スタックユニットが分裂しているとき、分裂した IRF スタックユニットの Master の IP アドレスが適用されます。Master は BFD セッションを確立することが

できます。**display bfd session** コマンドを実行した場合、2 つの装置間の BFD セッションの状態はアップです。

例

VLAN インタフェース 3 の IRF スタックのメンバ 1 に MAD IP アドレスを割り当てます。

<Switch> system-view

[Switch] interface vlan-interface 3

[Switch-Vlan-interface3] mad ip address 192.168.0.1 255.255.255.0 member 1

VLAN インタフェース 3 の IRF スタックのメンバ 2 に MAD IP アドレスを割り当てます。

[Switch-Vlan-interface3] mad ip address 192.168.0.2 255.255.255.0 member 2

関連コマンド

mad bfd enable

1.1.21 mad restore

Syntax

mad restore

View

System view

定義済みユーザロール

network-admin

説明

mad restore コマンドは Recovery 状態にある IRF スタックユニットの正常な MAD を回復します。

IRF スタックの分裂が回復する前にアクティブの IRF スタックユニットが故障した場合、**mad restore** コマンドを使用して Recovery 状態の IRF スタックユニットを回復します。

回復した IRF スタックユニットはアクティブの IRF スタックユニットの役割を引き継ぎます。

例

Recovery 状態にある IRF スタックユニットの正常な MAD を回復します。

<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...
```

1.1.22 port group interface

Syntax

port group interface *interface-type interface-number* **mode normal**

undo port group interface *interface-name*

デフォルト

設定なし

View

IRF port view

定義済みユーザロール

network-admin

パラメータ

interface-type interface-number: IRF スタック物理ポートのタイプと番号を指定します。

interface-name: *interface-type interface-number* の形式で IRF スタック物理ポートを指定します。*interface-type interface-number* の引数の間に半角スペースは入りません。

mode normal: インタフェースのモードを指定します。**normal** のみサポートします。

説明

port group interface コマンドは IRF スタックポートに IRF スタック物理ポートを割り当てます。

undo port group interface コマンドは IRF スタック物理ポートと IRF スタックポートの割り当てを削除します。

IRF スタックポートに複数の IRF スタック物理ポートを割り当てる場合、複数回、コマンドを実行してください。

QX-S5100G シリーズは最大 8 つの IRF スタック物理ポートを 1 つの IRF スタックポートに関連付けることができます。

IRF スタックポートから IRF スタック物理ポートに関連付ける、あるいは関連付けを削除する前に、ポートグループのすべてのポートを **shutdown** コマンドでシャットダウンします。関連付け、あるいは削除の処理が完了した後、すべての IRF スタック物理ポートを **undo shutdown** コマンドでアップします。IRF スタック物理ポートの関連付けの設定要件の詳細は、オペレーションマニュアルのセクション 2 *IRF スタック* “*IRF スタックの設定*”を参照してください。

例

IRF スタックのメンバ 1 の IRF スタックポート 1/1 に GigabitEthernet 1/0/49 を割り当てます。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/49

[Switch-GigabitEthernet1/0/49] shutdown

[Switch-GigabitEthernet1/0/49] quit

[Switch] irf-port 1/1

[Switch-irf-port1/1] port group interface gigabitethernet 1/0/49

[Switch-irf-port1/1] quit

[Switch] interface gigabitethernet 1/0/49

[Switch-GigabitEthernet1/0/49] undo shutdown

関連コマンド

irf-port

QX-S5100G シリーズ Ethernet スイッチ

コマンドマニュアル

3. アクセス

本マニュアルは以下に示す章で構成されています。

01-Ethernet インタフェース

02-ループバックインタフェースと Null インタフェース

03-Interface range

04-MAC アドレステーブル

05-MAC Information

06-リンクアグリゲーション

07-Port Isolation

08-STP

09-ループ検出

10-VLAN

11-Private VLAN

12-Voice VLAN

13-QinQ

14-VLAN マッピング

15-LLDP

16-L2PT

目次

このセクションのページは **3-x-x** です。

1 章 Ethernet インタフェース.....1-1
1.1 共通 Ethernet インタフェース設定コマンド.....1-1
1.1.1 broadcast-suppression.....1-1
1.1.2 combo enable.....1-3
1.1.3 description.....1-4
1.1.4 display counters.....1-5
1.1.5 display counters rate.....1-7
1.1.6 display interface.....1-8
1.1.7 duplex.....1-20
1.1.8 eee enable.....1-21
1.1.9 flow-control.....1-22
1.1.10 flow-control receive enable.....1-23
1.1.11 flow-interval.....1-24
1.1.12 ifmonitor crc-error.....1-25
1.1.13 ifmonitor input-error.....1-26
1.1.14 ifmonitor output-error.....1-28
1.1.15 interface.....1-29
1.1.16 jumboframe enable.....1-30
1.1.17 link-delay.....1-31
1.1.18 loopback.....1-32
1.1.19 multicast-suppression.....1-34
1.1.20 port auto-power-down.....1-36
1.1.21 port link-mode.....1-37
1.1.22 reset counters interface.....1-37
1.1.23 shutdown.....1-38
1.1.24 speed.....1-39
1.1.25 unicast-suppression.....1-40
1.1.26 unknown-unicast block outbound.....1-42
1.2 レイヤ 2 Ethernet インタフェース設定コマンド.....1-43
1.2.1 display storm-constrain.....1-43
1.2.2 mdix-mode.....1-45
1.2.3 speed auto.....1-46
1.2.4 storm-constrain.....1-47
1.2.5 storm-constrain control.....1-49
1.2.6 storm-constrain enable log.....1-50
1.2.7 storm-constrain enable trap.....1-51

1.2.8 storm-constrain interval.....1-52
1.2.9 virtual-cable-test 1-53

1章 Ethernet インタフェース

1.1 共通Ethernetインタフェース設定コマンド

1.1.1 broadcast-suppression

⚠ **注意**：

suppression 機能を Ethernet インタフェースもしくはポートグループに複数設定した場合、設定値は以下の優先度で有効化されます。
ブロードキャスト＞不明なユニキャスト＞マルチキャスト
たとえば、**broadcast-suppression** コマンド、**multicast-suppression** コマンド、**unicast-suppression** コマンドをそれぞれ抑制比率 10/20/30 で設定した場合、ブロードキャストの値が反映され、ブロードキャスト、マルチキャスト、不明なユニキャストの合計が 10%まで疎通可能となります。
suppression 機能を **pps** で使用する場合、標準の 10/100/1000BASE-T ポートでは 65 の倍数、SFP/SFP+ポートでは 650 の倍数で制御します。

Syntax

broadcast-suppression { **ratio** | **pps** *max-pps* | **kbps** *max-kbps* }

undo broadcast-suppression

デフォルト

設定なし

View

Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

ratio: イーサネットポートの総伝送能力に対するブロードキャストトラフィックの最大比率です。設定範囲は 1～100%です。この比率が小さいほど、ポートを通過できるブロードキャストトラフィックは少なくなります。

pps *max-pps*: イーサネットポートごとに毎秒のブロードキャストパケットの最大数を指定します。単位は pps（パケット/秒）です。*max-pps* の設定範囲は 1～1.4881×最大インタフェースレートです。

kbps *max-kbps*: イーサネットポートごとに毎秒のブロードキャストトラフィックの最大数を指定します。単位は kbps（キロビット/秒）です。*max-kbps* の設定範囲は、1～最大インタフェースレートです。

説明

broadcast-suppression コマンドはブロードキャストパケットの転送を抑制することを有効にし、しきい値を設定します。

undo broadcast-suppression コマンドは無効にします。

インタフェースでブロードキャストトラフィックのサイズを制限するため、ブロードキャストストーム抑制機能を使用することができます。インタフェースのブロードキャストトラフィックがしきい値を超過したとき、システムはトラフィックがしきい値を下回るまでパケットを廃棄します。

storm-constrain コマンドと **broadcast-suppression** コマンドの両方はポートでブロードキャストストームを抑制することができます。

- **storm-constrain** コマンドはブロードキャストトラフィックを抑制するためにソフトウェアを使用します。ある程度まで装置の性能に影響を及ぼします。
- **broadcast-suppression** コマンドはブロードキャストトラフィックを抑制するためにハードウェアのチップを使用します。装置の性能への影響は **storm-constrain** コマンドよりも小さくなります。

storm-constrain コマンドと **broadcast-suppression** コマンドを同時に設定しないでください。そうでなければ設定した機能が正常に動作しません。

抑制するしきい値を kbps で設定するとき、正確な抑制しきい値は、設定する値と異なります。

- 設定された値が 64 よりも小さい場合、64 の値が適用されます。
- 設定された値が 64 の整数倍より大きく、64 の整数倍でない場合、設定された 64 の整数倍にもっとも近い値が適用されます。

適用される抑制しきい値は、装置の表示画面を参照してください。

例

GigabitEthernet 1/0/1 でブロードキャストストーム抑制のしきい値を 10000kbps に設定します。

<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.
```

出力はしきい値が 10048kbps（64 の 157 倍）に設定されていることを示します。

関連コマンド

- **multicast-suppression**
- **unicast-suppression**

1.1.2 combo enable

🕮 メモ：

- **combo enable** コマンドは QX-S5124GP-4X と QX-S5124GT-4X-PW のみサポートしています。
- コンボポートは使用するポートのみケーブルまたは SFP モジュールを接続してください。

Syntax

combo enable { **copper** | **fiber** | **auto** }

デフォルト

auto

View

Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

copper: RJ-45 コンボポートを有効にします。ポートにツイストペアケーブルを接続します。

fiber: SFP トランシーバモジュールのコンボポートを有効にします。

auto: 自動で RJ-45 コンボポートあるいは SFP トランシーバモジュールのコンボポートを識別します。

- SFP トランシーバモジュールのコンボポートと RJ-45 コンボポートが実装された場合、SFP トランシーバモジュールのコンボポートが優先されます。
- SFP トランシーバモジュールが実装され、RJ-45 ケーブルが接続されていない場合、SFP トランシーバモジュールのコンボポートが有効になります。SFP トランシーバモジュールのコンボポートが実装されたのち、RJ-45 コンボポートに RJ-45 ケーブルを接続してもリンクアップしません。
- RJ-45 コンボポートに RJ-45 ケーブルが接続され、SFP トランシーバモジュールのコンボポートが実装されていない場合、RJ-45 コンボポートが有効になります。RJ-45 コンボポートが接続されリンクアップされていたのち、SFP トランシーバモジュールのコンボポートが実装されても、RJ-45 コンボポートがリンクアップのままとなります。

説明

combo enable コマンドはコンボインタフェースの RJ-45 コンボポートあるいは SFP トランシーバモジュールのコンボポートを有効にします。

コンボインタフェースは装置前面にある 1 ポート SFP トランシーバモジュールのコンボポートと 1 ポート RJ-45 コンボポートの論理インタフェースです。2 つのポートは 1 つの転送インタフェースを共有するため、同時に動作させることはできません。コンボポートでどちらかのモードを有効にした場合、もう一方のモードは自動で無効になります。RJ-45 コンボポートあるいは SFP トランシーバモジュールのコンボポートを選択し、有効にすることができます。

コマンドを実行する前に、装置の前面パネルのマークに従って以下の作業を行ってください。

- 装置のコンボインタフェースを決めてください。
- 各コンボインタフェースに属している 2 つの物理インタフェースを識別してください。

例

GigabitEthernet 1/0/1 のコンボインタフェースを RJ-45 コンボポートに設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] combo enable copper

GigabitEthernet 1/0/1 のコンボインタフェースを SFP トランシーバモジュールのコンボポートに設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] combo enable fiber

1.1.3 description

Syntax

description *text*

undo description

デフォルト

インタフェース名＋Interface です。（たとえば GigabitEthernet1/0/1 Interface です）

View

Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

text: インタフェースの説明を指定します。設定範囲は 1～255 文字です。大文字、小文字を区別します。

説明

description コマンドはインタフェースの説明を変更します。

undo description コマンドはデフォルトに戻します。

例

GigabitEthernet 1/0/1 の説明を lan-interface に変更します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] description lan-interface

1.1.4 display counters

Syntax

display counters { **inbound** | **outbound** } **interface** [*interface-type* [*interface-number*]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

inbound: 受信トラフィックの統計情報を表示します。

outbound: 送信トラフィックの統計情報を表示します。

interface-type: インタフェースのタイプを指定します。

interface-number: インタフェースの番号を指定します。

説明

display counters コマンドはインタフェースのトラフィックの統計情報を表示します。

このコマンドは **flow-interval** コマンドで指定されたポートの統計情報を収集する間隔内のトラフィックの統計情報を表示します。

Ethernet インタフェースのトラフィックの統計情報を削除する場合、**reset counters interface** コマンドを使用します。

インタフェースタイプを指定しない場合、すべてのインタフェースのトラフィックの統計情報を表示します。

インタフェースタイプを指定し、番号を指定しない場合、指定したインタフェースタイプのすべてのインタフェースのトラフィックの統計情報を表示します。

インタフェースタイプと番号を指定した場合、指定したインタフェースのすべてのトラフィックの統計情報を表示します。

例

すべての GigabitEthernet インタフェースの受信トラフィックの統計情報を表示します。

<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.
```

表 1-1 コマンド出力

フィールド	説明
Interface	インタフェース名の省略名です。
Total (pkts)	インタフェースを通して送受信したパケットの総数です。
Broadcast (pkts)	インタフェースを通して送受信したブロードキャストパケットの総数です。
Multicast (pkts)	インタフェースを通して送受信したマルチキャストパケットの総数です。
Err (pkts)	インタフェースを通して送受信したエラーパケットの総数です。
Overflow: More than 14 digits (7 digits for column "Err")	以下のときに**Overflow**と表示します。 • エラーフィールド値のデータ長が10進数で7桁を超えました。 • 非エラーフィールド値のデータ長が10進数で14桁を超えました。
--: Not supported	統計情報をサポートしていません。

関連コマンド

- **flow-interval**

- **reset counters interface**

1.1.5 display counters rate

Syntax

display counters rate { **inbound** | **outbound** } **interface** [*interface-type* [*interface-number*]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

inbound: 受信トラフィックレートの統計情報を表示します。

outbound: 送信トラフィックレートの統計情報を表示します。

interface-type: インタフェースのタイプを指定します。

interface-number: インタフェースの番号を指定します。

説明

display counters rate コマンドは最後のサンプリング間隔からの up 状態のインタフェースのトラフィックレートの統計情報を表示します。

統計情報は up 状態のインタフェースのみ適用されます。

インタフェースタイプを指定しない場合、すべてのインタフェースのトラフィックレートの統計情報を表示します。

インタフェースタイプを指定し、インタフェースの番号を指定しない場合、指定されたタイプのすべての up 状態のインタフェースのトラフィックレートの統計情報を表示します。

インタフェースタイプ、インタフェースの番号を指定した場合、指定したインタフェースのトラフィックレートの統計情報を表示します。

down 状態のインタフェースが指定されている場合、システムはコマンドをサポートしていないと表示されます。

最後のサンプリングの間隔を設定する場合、**flow-interval** コマンドを使用することができます。

例

すべての GigabitEthernet の受信トラフィックレートの統計情報を表示します。

<Switch> display counters rate inbound interface

```
Usage: Bandwidth utilization in percentage
Interface          Usage (%)   Total (pps)   Broadcast (pps)   Multicast (pps)
GE1/0/1                  3          --             --              --

 Overflow: More than 14 digits.
      --: Not supported.
```

表 1-2 コマンド出力

フィールド	説明
Interface	インタフェース名の省略名です。
Usage (%)	最後のサンプリング間隔中にインタフェースで送受信したパケットの平均レートです。単位は%です。
Total (pkts/sec)	最後のサンプリング間隔中に送受信したユニキャストパケットの平均レートです。単位はppsです。
Broadcast (pkts/sec)	最後のサンプリング間隔中に送受信したブロードキャストパケットの平均レートです。単位はppsです。
Multicast (pkts/sec)	最後のサンプリング間隔中に送受信したマルチキャストパケットの平均レートです。単位はppsです。
Overflow: more than 14 decimal digits	データ長が10進数で14桁を超えたときに、**Overflow**と表示します。
--: not supported	統計情報をサポートしていません。

関連コマンド

- **flow-interval**
- **reset counters interface**

1.1.6 display interface

Syntax

display interface [*interface-type* [*interface-number*]] [**brief** [**description** | **down**]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface-type: インタフェースタイプを指定します。

interface-number: インタフェース番号を指定します。

brief: 概要情報を表示します。指定しない場合、コマンドは詳細なインタフェース情報を表示します。

description: インタフェースの説明をすべて表示します。指定しない場合、インタフェースの説明の最初の 27 文字のみ表示します。

down: down 状態のインタフェースの情報と原因を表示します。指定しない場合、すべての状態のインタフェース情報を表示します。

説明

display interface コマンドは Ethernet インタフェースの情報を表示します。

インタフェースタイプを指定しない場合、すべてのインタフェースの情報を表示します。

インタフェースタイプを指定し、番号を指定しない場合、指定したタイプのすべてのインタフェースの情報を表示します。

インタフェースタイプと番号を指定した場合、指定したインタフェースの情報を表示します。

例

GigabitEthernet 1/0/1 の動作状態と情報を表示します。

<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
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
```

```
The maximum frame length is 9416
Last link flapping: 6 hours 39 minutes 28 seconds
Last clearing of counters: Never
Current system time:2019-02-10 14:56:12
Last time when physical state changed to up:-
Last time when physical state changed to down:2019-02-10 14:55:25
```

表 1-3 コマンド出力

フィールド	説明
Current state	Ethernetインタフェースの状態です。 ● **Administratively DOWN**—**shutdown**コマンドでインタフェースがシャットダウンしています。インタフェースは運用上においてdownしています。 ● **DOWN**—**shutdown**コマンドでシャットダウンしていませんが、物理的にdownしています。（イーサネットケーブルが物理的に接続されていない、あるいはリンクに失敗している可能性があります） ● **DOWN (Link-Aggregation interface down)**— **shutdown**コマンドでアグリゲートインタフェースがシャットダウンしています。 ● **mac-address moving down**—MACアドレスの移動の抑制機能によりインタフェースがシャットダウンしています。 ● **MAD ShutDown**—IRFスタックの分裂によりインタフェースがシャットダウンしています。IRFスタックが分裂したのち、IRFスタックユニットのインタフェースがRecovery状態になった場合に、シャットダウンします。 ● **Storm-Constrain**—ストーム抑止機能が不明なユニキャストトラフィック、マルチキャストトラフィック、ブロードキャストトラフィックの上限に到達したことを検出したため、インタフェースがシャットダウンしています。 ● **STP DOWN**—BPDUガード機能によりインタフェースがシャットダウンしています。 ● **UP**—インタフェースが運用上も物理的にも起動している状態です。

フィールド	説明

Line protocol state	インタフェースのリンクレイヤの状態です。リンクレイヤのパラメータのネゴシエーションによって決まります。
	• **UP**—インタフェースがリンクレイヤでupしています。
	• **UP (spoofing)**—インタフェースがリンクレイヤでupしていますが、オンデマンドのリンクあるいは準備ができていない状態です。この属性はNullインタフェースとループバックインタフェースの一般的な状態です。
	• **DOWN**—インタフェースがリンクレイヤでdownしています。
	• **DOWN (*protocols*)**—インタフェースが括弧内のプロトコルにより、リンクレイヤでdownしています。
	  • **DLDP**—リンクが片方向であるとDLDPが検出したため、インタフェースがリンクレイヤでdownしています。
	  • **LAGG**—アグリゲートインタフェースがSelectedポートでないため、インタフェースがリンクレイヤでdownしています。
	  • **BFD**—リンク障害を検出したためインタフェースがリンクレイヤでdownしています。

Bandwidth	インタフェースの予期された帯域幅です。
Maximum transmission unit	インタフェースのMTUです。
Internet protocol processing: Disabled	インタフェースにIPアドレスが設定されておらず、IPパケットを処理できません。
Internet address	インタフェースのIPアドレスを表示します。**primary**はIPアドレスがプライマリIPアドレスであることを示します。
IP packet frame type	IPv4パケットのフレームタイプです。
hardware address	インタフェースのMACアドレスです。
IPv6 packet frame type	IPv6パケットのフレームタイプです。
Port priority	インタフェースのプライオリティです。
Loopback is set internal	インタフェースで内部ループバックテストが動作しています。このフィールドは内部ループバックテストの設定が行われた場合に表示されます。
Loopback is set external	インタフェースで外部ループバックテストが動作しています。このフィールドは外部ループバックテストの設定が行われた場合に表示されます。

フィールド	説明
Loopback is not set	インタフェースでループバックテストが動作していません。このフィールドはループバックテストの設定が行われていない場合に表示されます。
10Mbps-speed mode	インタフェースが10Mbpsで動作しています。このフィールドは通信速度の設定とリンクパラメータのネゴシエーションの結果によって異なります。
100Mbps-speed mode	インタフェースが100Mbpsで動作しています。このフィールドは通信速度の設定とリンクパラメータのネゴシエーションの結果によって異なります。
1000Mbps-speed mode	インタフェースが1000Mbpsで動作しています。このフィールドは通信速度の設定とリンクパラメータのネゴシエーションの結果によって異なります。
10Gbps-speed mode	インタフェースが10Gbpsで動作しています。このフィールドは通信速度の設定とリンクパラメータのネゴシエーションの結果によって異なります。
25Gbps-speed mode	インタフェースが25Gbpsで動作しています。このフィールドは通信速度の設定とリンクパラメータのネゴシエーションの結果によって異なります。
Unknown-speed mode	通信速度のネゴシエーションに失敗あるいはインタフェースが物理的に切断しているため、インタフェースの速度が不明です。
half-duplex mode	インタフェースがhalfの動作モードで動作しています。このフィールドは通信速度の設定とリンクパラメータのネゴシエーションの結果によって異なります。
full-duplex mode	インタフェースがfullの動作モードで動作しています。このフィールドは通信速度の設定とリンクパラメータのネゴシエーションの結果によって異なります。
unknown-duplex mode	通信モードのネゴシエーションに失敗あるいはインタフェースが物理的に切断しているため、インタフェースの通信モードが不明です。
Link speed type is autonegotiation	**speed auto**コマンドでインタフェースに設定されています。
Link speed type is force link	**speed**コマンドで通信速度がインタフェースに設定されています。たとえば100Mbpsです。
link duplex type is autonegotiation	**duplex auto**コマンドでインタフェースに設定されています。
link duplex type is force link	**duplex**コマンドで通信モードがインタフェースに設定されています。たとえばhalfあるいはfullです。
Flow-control is not enabled	インタフェースでフローコントロールが無効です。このフィールドは設定とリンクパラメータのネゴシエーションの結果によって異なります。

フィールド	説明
Maximum frame length	インタフェースの最大フレーム長です。
Allow jumbo frame to pass	インタフェースがジャンボフレームをサポートしています。
Broadcast max-	ブロードキャストストーム抑制のしきい値です。単位はratio、pps、kbpsです。しきい値のユニットは設定に依存します。
Multicast max-	マルチキャストストーム抑制のしきい値です。単位はratio、pps、kbpsです。しきい値のユニットは設定に依存します。
Unicast max-	ユニキャストストーム抑制のしきい値です。単位はratio、pps、kbpsです。しきい値のユニットは設定に依存します。
PVID	インタフェースのポートVLANのID（PVID）です。
MDI type	インタフェースのMDIXタイプです。 ● automdixです。 ● mdiです。 ● mdixです。
Port link-type	インタフェースのリンクタイプです。 ● accessです。 ● trunkです。 ● hybridです。
Tagged VLANs	VLANタグを削除しないでパケット送信するVLANです。
Untagged VLANs	VLANタグを削除したのち、パケット送信するVLANです。
VLAN Passing	パケットがポートで転送することができるVLANです。VLANはすでに作成されている必要があります。
VLAN permitted	パケットがポートで許可されたVLANです。
Trunk port encapsulation	トランクポートのカプセル化のプロトコルタイプです。
Last link flapping	リンクがフラッピングしてからの経過時間です。 **Never**は装置が起動してから一度もリンクのフラッピングが発生していないことを示します。
Last clearing of counters	インタフェースで**reset counters interface**コマンドを最後に使用した時間です。 **Never**は装置が起動してから**reset counters interface**コマンドを一度も使用していないことを示します。
Last 300 second input: 0 packets/sec 0 bytes/sec 0% Last 300 second output: 0 packets/sec 0 bytes/sec 0%	過去300秒以内の平均送受信トラフィックです。単位はpps、bpsです。最大インタフェース速度に対する実際の速度の比率です。ハイフン（-）はサポートしてないことを示します。

フィールド	説明
Input(total):　0 packets, 0 bytes 0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses	フィールドの1行目はインタフェースの受信トラフィックの統計情報（パケット、バイト数）です。すべての正常な受信パケット、異常なパケット、正常なpauseフレームがカウントされます。 2行目の4つのフィールドを示します。 ● ユニキャストパケットの受信数です。 ● ブロードキャストの受信数です。 ● マルチキャストの受信数です。 ● pauseフレームの受信数です。 ハイフン（-）はサポートしてないことを示します。
Input(normal):　0 packets, 0 bytes 0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses	フィールドの1行目はインタフェースの正常な受信トラフィックとの統計情報（パケット、バイト数）です。すべての正常な受信パケット、正常なpauseフレームがカウントされます。 2行目の4つのフィールドを示します。 ● 正常なユニキャストパケットの受信数です。 ● 正常なブロードキャストの受信数です。 ● 正常なマルチキャストの受信数です。 ● 正常なpauseフレームの受信数です。 ハイフン（-）はサポートしてないことを示します。
input errors	受信エラーパケットの統計情報です。
runts	以下の状況にある受信フレーム数です。 ● 64バイト長未満のフレームです。 ● 不正なフォーマットのフレームです。 ● 有効なCRCが含まれるフレームです。
giants	インタフェースでサポートされるフレーム長よりも長い受信フレーム数です。 ジャンボフレームをサポートしていないインタフェースでは、最大フレーム長は以下です。 ● 1518バイト（VLANタグなし）。 ● 1522バイト（VLANタグつき）。 ジャンボフレームをサポートしているインタフェースでは、giantsはインタフェースを通過することを許可されたフレームの最大長より長いフレームを示します。
throttles	整数倍バイト長でない入力フレームの数です。
CRC	正常なフレーム長ですが、CRCエラーが含まれている受信フレームの総数です。

フィールド	説明
frame	CRCエラーが含まれ、整数バイトでない受信フレームの総数です。
overruns	ポートの受信レートがキューの容量を超過したため、廃棄されたパケット数です。
aborts	不正な受信パケットの総数です。 • **Fragment frames**—64バイトよりも短いフレームのCRCエラーフレームです。フレーム長は整数あるいは非整数の値です。 • **Jabber frames**—インタフェースでサポートされている最大フレーム長よりも長いフレームのCRCエラーフレームです。フレーム長は整数あるいは非整数の値です。 • ジャンボフレームを許可しない場合、最大フレーム長は1518バイト（VLANタグなし）あるいは1540バイト（VLANタグつき）よりも長いCRCエラーフレームを示します。 • ジャンボフレームを許可する場合、jabberフレームはインタフェースを通過することを許可されたフレームの最大長より長いフレームを示します。 • **Symbol error frames**—少なくとも1つ以上の定義されていないシンボルを含むフレームです。 • **Unknown operation code frames**—MAC制御フレームでpauseフレームでないフレームです。 • **Length error frames**—802.3のレングスフィールドが実際のフレーム長に合致していないフレームです。（46～1500バイトです）
ignored	ポートの受信バッファの能力不足により、インタフェースに廃棄された受信フレームの数です。
parity errors	パリティエラーのフレームの総数です。

フィールド	説明
Output(total): 0 packets, 0 bytes 0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses	フィールドの1行目はインタフェースの送信トラフィックの統計情報（パケット、バイト数）です。すべての正常な送信パケット、異常なパケット、正常なpauseフレームがカウントされます。 2行目の4つのフィールドを示します。 ● ユニキャストパケットの送信数です。 ● ブロードキャストの送信数です。 ● マルチキャストの送信数です。 ● pauseフレームの送信数です。 ハイフン（-）はサポートしてないことを示します。
Output(normal): 0 packets, 0 bytes 0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses	フィールドの1行目はインタフェースの正常な送信トラフィックとの統計情報（パケット、バイト数）です。すべての正常な送信パケット、正常なpauseフレームがカウントされます。 2行目の4つのフィールドを示します。 ● 正常なユニキャストパケットの送信数です。 ● 正常なブロードキャストの送信数です。 ● 正常なマルチキャストの送信数です。 ● 正常なpauseフレームの送信数です。 ハイフン（-）はサポートしてないことを示します。
output errors	送信エラーパケットの統計情報です。
underruns	ポートの送信レートがキューの容量を超過したため、廃棄されたパケット数です。これは低確率でハードウェアの異常を示します。
buffer failures	ポートの送信バッファの能力不足により、インタフェースに廃棄されたパケットの数です。
aborts	Ethernetコリジョンなどにより、転送に失敗したパケット数です。
deferred	検出したコリジョンにより、フレームを遅延させた数です。
collisions	フレームの送信中にEthernetコリジョンが検出されたため、転送を停止したフレーム数です。
late collisions	最初の512ビットをネットワークに送信した後にコリジョンが検出され、フレームの送信が遅延した回数です。
lost carrier	送信中にキャリアが失われた回数です。このカウンタは、キャリアが失われたときに増加し、シリアルWANインタフェースに適用されます。

フィールド	説明
no carrier	フレームを送信しようとしたときポートがキャリアの検出に失敗した回数です。このカウンタは、ポートがキャリアの検出に失敗したときに増加し、シリアルWANインタフェースに適用されます。
Peak input rate	受信トラフィックレートのピークレートと受信トラフィックのピークが発生したときの時間です。ピークレートの単位はbpsです。
Peak output rate	送信トラフィックレートのピークレートと送信トラフィックのピークが発生したときの時間です。ピークレートの単位はbpsです。

すべてのインタフェースの概要情報を表示します。

<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   100M(a) F(a)   A    1    aaaaaaaaaaaaaaaaaaaaaaaaaa
```

インタフェースの完全な説明を含む GigabitEthernet 1/0/3 の概要情報を表示します。

<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   100M(a) F(a)   A    1    aaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

down 状態のインタフェースの情報と原因を表示します。

<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
```

表 1-4 コマンド出力

フィールド	説明
Brief information on interfaces in route mode:	レイヤ3インタフェースの概要情報です。
Interface	インタフェース名です。
Link	インタフェースの物理リンク状態です。 ● **UP**—リンクがupです。 ● **DOWN**—リンクが物理的にdownしています。 ● **ADM**—リンクが運用上、**shutdown**コマンドでシャットダウンしています。物理状態を回復する場合、**undo shutdown**コマンドを実行します。 ● **Stby**—インタフェースがバックアップインタフェースとして動作します。
Protocol	インタフェースのリンクレイヤの状態です。 ● **UP**－インタフェースのリンクがupです。 ● **DOWN**－インタフェースのリンクがdownです。 ● **UP(s)**—インタフェースのリンクがオンデマンドリンクあるいは準備ができていない状態です。ここで（**s**）はスプーフィングのフラグを示します。Nullインタフェース、ループバックインタフェースで表示されます。
Primary IP	インタフェースのプライマリIPアドレスです。ハイフン（**--**）はIPアドレスが設定されていないことを示します。
Description	インタフェースの説明です。

フィールド	説明
Brief information of interfaces in bridge mode:	レイヤ2インタフェースの概要情報です。
Type: A - access; T - trunk; H – hybrid	インタフェースのリンクタイプのオプションです。
Speed	インタフェースの通信速度です。 インタフェースが自動でネゴシエーションされる場合、(**a**)で示されたオートネゴシエーションのフラグが含まれます。インタフェースにオートネゴシエーションが設定されているがオートネゴシエーションが開始していない場合、**auto**と表示されます。
Duplex	インタフェースの通信モードです。 ● **A**—オートネゴシエーションです。インタフェースのオートネゴシエーションの通信モードがautoに設定されているがオートネゴシエーションが開始していません。 ● **F**—通信モードがfullです。 ● **F(a)**— 通信モードがfullでオートネゴシエートされています。 ● **H**—通信モードがhalfです。 ● **H(a)**—通信モードがhalfでオートネゴシエートされています。
Type	インタフェースのリンクタイプです。 ● **A**—アクセスです。 ● **H**—ハイブリッドです。 ● **T**—トランクです。
PVID	ポートVLANのIDです。

フィールド	説明
Cause	インタフェースの物理リンク状態がDOWNとなった原因です。 ● **Administratively**—**shutdown**コマンドでインタフェースがシャットダウンしています。インタフェースは運用上においてdownしています。物理状態を回復する場合、**undo shutdown**コマンドを実行します。 ● **DOWN (Link-Aggregation interface down)**—アグリゲートインタフェースがシャットダウンしているとき、アグリゲートインタフェースのすべてのメンバポートの物理状態がdownです。 ● **DOWN (Loopback detection down)**—ループバック検出モジュールがループバックを検出したため、ポートがシャットダウンしています。 ● **DOWN (Monitor-Link uplink down)**—モニタリンクモジュールがアップリンクのダウンを検出したため、ポートがシャットダウンしています。 ● **MAD ShutDown**—IRFスタックの分裂後、IRFスタックの除外ポートを除くすべてのインタフェースがdownになりました。 ● **Not connected**—物理接続がありません。（ネットワークが切断された、あるいは故障している可能性があります） ● **Storm-Constrain**—不明なユニキャストトラフィック、マルチキャストトラフィック、ブロードキャストトラフィックが上限を超過したため、ポートがシャットダウンしています。 ● **STP DOWN**—STP BPDUガード機能によってポートがシャットダウンしています。 ● **Standby**—インタフェースがstandby状態です。

関連コマンド

reset counters interface

1.1.7 duplex

Syntax

duplex { **auto** | **full** | **half** }

undo duplex

デフォルト

auto

View

Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

auto: ピアとの動作モードをオートネゴシエーションに設定します。

full: インタフェースが同時にパケットの送受信を行えるように通信モードを full（全 2 重モード）に設定します。

half: インタフェースが受信時にパケットの送信あるいは受信のみを行えるように動作モードを half（半 2 重モード）に設定します。1000BASE-T SFP/SFP+を含む SFP/SFP+トランシーバモジュールで動作するポート、1000Mbps で動作する RJ-45 ポートは、未サポートです。

説明

duplex コマンドはインタフェースの通信モードを設定します。

undo duplex コマンドはインタフェースの通信モードをデフォルトに戻します。

例

GigabitEthernet 1/0/1 の通信モードを full に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] duplex full

1.1.8 eee enable

⚠ **重要:**

ファイバポートでは、このコマンドはサポートされていません。

Syntax

eee enable

undo eee enable

デフォルト

無効

View

Ethernet interface view

定義済みユーザロール

network-admin

説明

eee enable コマンドはインタフェースで EEE 省電力機能を有効にします。

undo eee enable コマンドはインタフェースで EEE 省電力機能を無効にします。

EEE 省電力機能が有効の場合、リンクアップインタフェースは一定期間パケットを受信しないと、低電力状態に遷移します。この期間はチップの仕様に依存し、設定を変更することができません。パケットが到着した後、インタフェースは通常の状態に遷移します。

例

GigabitEthernet 1/0/1 で EEE 省電力機能を有効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] eee enable

1.1.9 flow-control

Syntax

flow-control

undo flow-control

デフォルト

無効

View

Ethernet interface view

定義済みユーザロール

network-admin

説明

flow-control コマンドは Ethernet インタフェースの TxRx モードのフローコントロールを有効にします。

undo flow-control コマンドは Ethernet インタフェースの TxRx モードのフローコントロールを無効にします。

TxRx モードのフローコントロールをインタフェースで有効にするとインタフェースはフローコントロールのフレームを送受信します。

- ピアが混雑したとき、インタフェースは送信停止を対向に知らせるため、送信するフロー制御(pause)フレームに送信停止を要求するパラメータを含めます。
- ピアから送信停止を要求するパラメータを持つフロー制御(pause)フレームを受信したとき、インタフェースはパケットの送信を中断します。

リンクのフローコントロールを実装するため、リンクの両端でフローコントロール機能を有効にしてください。

例

GigabitEthernet 1/0/1 で TxRx モードのフローコントロールを有効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] flow-control

1.1.10 flow-control receive enable

Syntax

flow-control receive enable

undo flow-control

デフォルト

無効

View

Ethernet interface view

定義済みユーザロール

network-admin

説明

flow-control receive enable コマンドは Ethernet ポートで Rx モードのフローコントロールを有効にします。

undo flow-control コマンドは Ethernet ポートで Rx モードのフローコントロールを無効にします。

Rx モード flow-control を有効にすると、インタフェースはフローコントロールフレームを受信できますが、送信できません。

- インタフェースは、ピアからフローコントロールフレームを受信すると、ピアへのパケットの送信を中断します。
- インタフェースでトラフィックの輻輳が発生した場合、インタフェースにフローコントロールフレームを送信できません。

リンクで片方向トラフィック輻輳を処理するには、一方で **flow-control receive enable** コマンドを設定し、もう一方で **flow-control** コマンドを設定します。リンクの両端でトラフィック輻輳の処理を有効にするには、両端で **flow-control** コマンドを設定します。

例

GigabitEthernet 1/0/1 で Rx モードのフローコントロールを有効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-gigabitethernet 1/0/1] flow-control receive enable

関連コマンド

flow-control

1.1.11 flow-interval

Syntax

flow-interval *interval*

undo flow-interval

デフォルト

300 秒

View

Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

interval: ポートの統計情報を収集する間隔を設定します。設定範囲は 5～300 で、5 の倍数にする必要があります。

説明

flow-interval コマンドはポートの統計情報を収集する間隔を設定します。

undo flow-interval コマンドはデフォルトに戻します。

例

GigabitEthernet 1/0/1 の統計情報を収集する間隔を 100 秒に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] flow-interval 100

1.1.12 ifmonitor crc-error

🕮 **メモ:**

Ifmonitor 機能は Version7.1.11 を含む以降のソフトウェアからサポートしています。

Syntax

ifmonitor crc-error slot *slot-number* **high-threshold** *high-value* **low-threshold** *low-value* **interval** *interval* [**shutdown**]

undo ifmonitor crc-error slot *slot-number*

デフォルト

上限しきい値は 1000 です。下限しきい値は 100 です。統計情報収集および比較間隔は 30 秒です。

View

System view

定義済みユーザロール

network-admin

パラメータ

high-value: CRC エラーパケットアラームの上限しきい値を設定します。設定範囲は 1～4294967295 パケットです。

low-value: CRC エラーパケットアラームの下限しきい値を設定します。設定範囲は 1～4294967295 パケットです。

interval: CRC エラーパケットの統計情報収集および比較間隔を設定します。設定範囲は 1～65535 です。

shutdown: インタフェースに受信した CRC エラーパケット数が上限しきい値を超えた場合に、インタフェースをシャットダウンします。その後、インタフェースはすべてのパケットの転送を停止します。インタフェースを回復するには、インタフェースで undo shutdown コマンドを実行します。このキーワードを指定しない場合、CRC エラーパケット受信数がインタフェース上の上限しきい値を超えると、上限しきい値超過アラームが生成され、インタフェースはアラーム状態になります。

slot-number: IRF スタックメンバデバイスをメンバ ID で指定します。

説明

ifmonitor crc-error コマンドは CRC エラーパケットアラームを有効にします。

undo ifmonitor crc-error コマンドは CRC エラーパケットアラームを無効にします。

指定した間隔内で正常状態のインタフェースに受信した CRC エラーパケット数が上限しきい値を超えると、インタフェースは上限しきい値超過アラームを生成し、アラーム状態になります。指定した間隔内でアラーム状態のインタフェースに受信した CRC エラーパケット数が下限しきい値を下回ると、インタフェースは回復アラームを生成し、正常状態に戻ります。

アラーム対象のインタフェースは、物理インタフェースと、アグリゲートインタフェースです。

VLAN インタフェースは対象外です。

例

#CRC エラーパケットアラームの上限しきい値を 5000、下限しきい値を 400、統計情報収集および比較間隔を 6 秒に設定します。

<Switch> system-view

[Switch] ifmonitor crc-error slot 1 high-threshold 5000 low-threshold 400 interval 6

1.1.13 ifmonitor input-error

🕮 メモ:

Ifmonitor 機能は Version7.1.11 を含む以降のソフトウェアからサポートしています。

Syntax

ifmonitor input-error slot *slot-number* **high-threshold** *high-value* **low-threshold** *low-value* **interval** *interval* [**shutdown**]

undo ifmonitor input-error slot *slot-number*

デフォルト

上限しきい値は 1000 です。下限しきい値は 100 です。統計情報収集および比較間隔は 30 秒です。

View

System view

定義済みユーザロール

network-admin

パラメータ

high-value: 入力エラーパケットアラームの上限しきい値を設定します。設定範囲は 1～4294967295 パケットです。

low-value: 入力エラーパケットアラームの下限しきい値を設定します。設定範囲は 1～4294967295 パケットです。

interval: 入力エラーパケットの統計情報収集および比較間隔を設定します。設定範囲は 1～65535 です。

shutdown: インタフェースに受信した入力エラーパケット数が上限しきい値を超えた場合に、インタフェースをシャットダウンします。その後、インタフェースはすべてのパケットの転送を停止します。インタフェースを回復するには、インタフェースで undo shutdown コマンドを実行します。このキーワードを指定しない場合、入力エラーパケット受信数がインタフェース上の上限しきい値を超えると、上限しきい値超過アラームが生成され、インタフェースはアラーム状態になります。

slot-number: IRF スタックメンバデバイスをメンバ ID で指定します。

説明

ifmonitor input-error コマンドは入力エラーパケットアラームを有効にします。

undo ifmonitor input-error コマンドは入力エラーパケットアラームを無効にします。

指定した間隔内で正常状態のインタフェースに受信した入力エラーパケット数が上限しきい値を超えると、インタフェースは上限しきい値超過アラームを生成し、アラーム状態になります。指定した間隔内でアラーム状態のインタフェースに受信した入力エラーパケット数が下限しきい値を下回ると、インタフェースは回復アラームを生成し、正常状態に戻ります。

アラーム対象のインタフェースは、物理インタフェースと、アグリゲートインタフェースです。

VLAN インタフェースは対象外です。

例

#入力エラーパケットアラームの上限しきい値を 5000、下限しきい値を 400、統計情報収集および比較間隔を 6 秒に設定します。

<Switch> system-view

[Switch] ifmonitor input-error slot 1 high-threshold 5000 low-threshold 400 interval 6

1.1.14 ifmonitor output-error

🕮 メモ:

Ifmonitor 機能は Version7.1.11 を含む以降のソフトウェアからサポートしています。

Syntax

ifmonitor output-error slot *slot-number* **high-threshold** *high-value* **low-threshold** *low-value* **interval** *interval* [**shutdown**]

undo ifmonitor output-error slot *slot-number*

デフォルト

上限しきい値は 1000 です。下限しきい値は 100 です。統計情報収集および比較間隔は 30 秒です。

View

System view

定義済みユーザロール

network-admin

パラメータ

high-value: 入力エラーパケットアラームの上限しきい値を設定します。設定範囲は 1～4294967295 パケットです。

low-value: 入力エラーパケットアラームの下限しきい値を設定します。設定範囲は 1～4294967295 パケットです。

interval: 入力エラーパケットの統計情報収集および比較間隔を設定します。設定範囲は 1～65535 です。

shutdown: インタフェースに受信した入力エラーパケット数が上限しきい値を超えた場合に、インタフェースをシャットダウンします。その後、インタフェースはすべてのパケットの転送を停止します。インタフェースを回復するには、インタフェースで undo shutdown コマンドを実行します。このキーワードを指定しない場合、入力エラーパケット受信数がインタフェース上の上限しきい値を超えると、上限しきい値超過アラームが生成され、インタフェースはアラーム状態になります。

slot-number: IRF スタックメンバデバイスをメンバ ID で指定します。

説明

ifmonitor output-error コマンドは出力エラーパケットアラームを有効にします。

undo ifmonitor output-error コマンドは出力エラーパケットアラームを無効にします。

指定した間隔内で正常状態のインタフェースに受信した出力エラーパケット数が上限しきい値を超えると、インタフェースは上限しきい値超過アラームを生成し、アラーム状態になります。指定した間隔内でアラーム状態のインタフェースに受信した出力エラーパケット数が下限しきい値を下回ると、インタフェースは回復アラームを生成し、正常状態に戻ります。

アラーム対象のインタフェースは、物理インタフェースと、アグリゲートインタフェースです。

VLAN インタフェースは対象外です。

例

#出力エラーパケットアラームの上限しきい値を 5000、下限しきい値を 400、統計情報収集および比較間隔を 6 秒に設定します。

<Switch> system-view

[Switch] ifmonitor output-error slot 1 high-threshold 5000 low-threshold 400 interval 6

1.1.15 interface

Syntax

interface *interface-type interface-number*

View

System view

定義済みユーザロール

network-admin

パラメータ

interface-type: インタフェースタイプを指定します。

interface-number: インタフェース番号を指定します。

説明

interface コマンドは interface view に移行します。

例

GigabitEthernet 1/0/1 の interface view に移行します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1]

1.1.16 jumboframe enable

Syntax

jumboframe enable [*value*]

undo jumboframe enable

デフォルト

10000 バイトまでのジャンボフレームを許可します。

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

value: Ethernet フレームの通過を許可する最大フレーム長を設定します。設定範囲は 1536～10000 バイトです。

説明

jumboframe enable コマンドは指定したフレーム長以内のジャンボフレームの通過を許可します。

undo jumboframe enable コマンドはジャンボフレームの通過を拒否します。

value が複数設定されている場合、最後に指定された設定が適用されます。

例

GigabitEthernet 1/0/1 でジャンボフレームの通過を許可します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] jumboframe enable

1.1.17 link-delay

Syntax

link-delay { **down** | **up** } [**msec**] *delay-time*

undo link-delay { **down** | **up** }

デフォルト

0 秒

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

down:リンクダウンのイベントを抑制します。

up:リンクアップのイベントを抑制します。

msec: 本オプションを有効にすると、ミリ秒単位で抑制時間を設定することが出来ます。本オプションを指定しない場合は秒単位での設定となります。

delay-time:イーサネットインタフェースのリンク状態の変化を抑制する間隔を設定します。0 に設定した場合はリンク状態の変化を直ちに CPU に報告します。

- **msec** オプションを指定しない場合、0～30 秒の範囲で指定可能です。
- **msec** オプションを指定した場合、0～10000 ミリ秒で指定が可能です。なお、設定値は 100 の倍数でなければなりません。

説明

link-delay コマンドはインタフェースで物理状態の変更を CPU に通知するまでの時間を設定します。

undo link-delay コマンドでデフォルトに戻します。

リンクダウンイベントのみか、リンクアップイベントのみ、または両方の抑制を設定することができます。遅延タイマが期限切れになる時に、指定したイベントがまだ継続しているならば、システムはイベントを CPU に報告します。

ガイドライン:

- リンクダウンイベントの抑制には、**link-delay down** コマンドを設定してください。
- リンクアップイベントの抑制には、**link-delay up** コマンドを設定してください。
- インタフェースで、リンクアップとリンクダウンで違う遅延タイマを設定することができます。

- 複数回 **link-delay** コマンドを設定した場合、最後に入力したコンフィギュレーションのみ有効になります。
- RRPP、STP、Smart Link が有効なインタフェースでは、本コマンドを実行しないでください。

例

GigabitEthernet 1/0/1 のリンクダウンを CPU に通知するまでの時間を 8 秒に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] link-delay down 8

GigabitEthernet 1/0/1 のリンクアップを CPU に通知するまでの時間を 800 ミリ秒に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] link-delay up msec 800

1.1.18 loopback

注意:

インタフェースでループバックテストを有効にした場合、インタフェースはトラフィックデータを転送しません。

Syntax

loopback { **external** | **internal** }

undo loopback

デフォルト

無効

View

Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

external: Ethernet インタフェースの外部ループバックテストを有効にします。

internal: Ethernet インタフェースの内部ループバックテストを有効にします。

説明

loopback コマンドは Ethernet インタフェースのループバックテストを有効にします。

undo loopback コマンドは Ethernet インタフェースのループバックテストを無効にします。

Ethernet インタフェースでループバックテストを有効にしたのち、Ethernet インタフェースは通信モードを full に切り替わります。Ethernet インタフェースでループバックテストを無効にしたのち、Ethernet インタフェースの通信モードテスト終了後はもとの設定で動作します。

ループバックテストの Ethernet インタフェースはデータのトラフィックを転送しません。

インタフェースがシャットダウンされている場合（インタフェースのステータスは ADM あるいは Administratively DOWN と表示されます）は、内部/外部ループバックテストともに実行できません。

ループバックテストの間、**speed**、**duplex**、**mdix-mode**、**shutdown** コマンドは適用できません。

例

GigabitEthernet 1/0/1 の内部ループバックテストを有効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] loopback internal

1.1.19 multicast-suppression

注意：

suppression 機能を Ethernet インタフェースもしくはポートグループに複数設定した場合、設定値は以下の優先度で有効化されます。
ブロードキャスト＞不明なユニキャスト＞マルチキャスト
たとえば、**broadcast-suppression** コマンド、**multicast-suppression** コマンド、**unicast-suppression** コマンドをそれぞれ抑制比率 10/20/30 で設定した場合、ブロードキャストの値が反映され、ブロードキャスト、マルチキャスト、不明なユニキャストの合計が 10%まで疎通可能となります。
suppression 機能を pps で使用する場合、標準の 10/100/1000BASE-T ポートでは 65 の倍数、SFP/SFP+ポートでは 650 の倍数で制御します。

Syntax

multicast-suppression { *ratio* | **pps** *max-pps* | **kbps** *max-kbps* }

undo multicast-suppression

デフォルト

設定なし

View

Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

ratio: イーサネットポートの総伝送能力に対するマルチキャストトラフィックの最大比率です。設定範囲は 1～100%です。この比率が小さいほど、ポートを通過できるマルチキャストトラフィックは少なくなります。

pps *max-pps*: イーサネットポートごとに毎秒のマルチキャストパケットの最大数を指定します。単位は pps（パケット/秒）です。*max-pps* の設定範囲は 1～1.4881×最大インタフェースレートです。

kbps *max-kbps*: イーサネットポートごとに毎秒のマルチキャストトラフィックの最大数を指定します。単位は kbps（キロビット/秒）です。*max-kbps* の設定範囲は、1～最大インタフェースレートです。

説明

multicast-suppression コマンドはマルチキャストパケットの転送を抑制することを有効にし、しきい値を設定します。

undo multicast-suppression コマンドはデフォルトに戻します。

インタフェースでマルチキャストトラフィックのサイズを制限するため、マルチキャストストーム抑制機能を使用することができます。インタフェースのマルチキャストトラフィックがしきい値を超過したとき、システムはトラフィックがしきい値を下回るまでパケットを廃棄します。

storm-constrain コマンドと **multicast-suppression** コマンドの両方はポートでマルチキャストストームを抑制することができます。

- **storm-constrain** コマンドはマルチキャストトラフィックを抑制するためにソフトウェアを使用します。ある程度まで装置の性能に影響を及ぼします。
- **multicast-suppression** コマンドはマルチキャストトラフィックを抑制するためにハードウェアのチップを使用します。装置の性能への影響は **storm-constrain** コマンドよりも小さくなります。

storm-constrain コマンドと **multicast-suppression** コマンドを同時に設定しないでください。そうでなければ設定した機能が正常に動作しません。

抑制するしきい値を kbps で設定するとき、正確な抑制しきい値は、設定する値と異なります。

- 設定された値が 64 よりも小さい場合、64 の値が適用されます。
- 設定された値が 64 の整数倍より大きく、64 の整数倍でない場合、設定された 64 の整数倍にもっとも近い値が適用されます。

適用される抑制しきい値は、装置の表示画面を参照してください。

例

GigabitEthernet 1/0/1 でマルチキャストストーム抑制のしきい値を 10000kbps に設定します。

<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.
```

出力はしきい値が 10048kbps（64 の 157 倍）に設定されていることを示します。

関連コマンド

- **broadcast-suppression**
- **unicast-suppression**

1.1.20 port auto-power-down

⚠ **重要:**

port auto-power-down コマンドは SFP/SFP+ポートで未サポートです。

Syntax

port auto-power-down

undo port auto-power-down

デフォルト

無効

View

Ethernet interface view

定義済みユーザロール

network-admin

説明

port auto-power-down コマンドはインタフェースの自動パワーダウン機能を有効にします。

undo port auto-power-down コマンドはデフォルトに戻します。

自動パワーダウン機能がインタフェースで有効でインタフェースが一定期間ダウンしているとき、以下のイベントが発生します。

- 装置は自動的にインタフェースへの電源供給を停止します。
- インタフェースが電源セーブモードに移行します。

ダウンする一定期間はインタフェースのチップの仕様に依存します。変更することはできません。

インタフェースが up になると、以下のイベントが発生します。

- 装置は自動的にインタフェースへの電源供給を回復します。
- インタフェースが正常モードに移行します。

例

GigabitEthernet 1/0/1 の自動パワーダウン機能を有効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] port auto-power-down

1.1.21 port link-mode

Syntax

port link-mode { **bridge** | **route** }

undo port link-mode

デフォルト

ブリッジモード

View

Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

bridge: レイヤ 2 モードを指定します。

route: レイヤ 3 モードを指定します。

説明

port link-mode コマンドは、Ethernet インタフェースのリンクモードを変更します。

undo port link-mode コマンドは 、設定をデフォルトに戻します。

インタフェースは、レイヤ 2 とレイヤ 3 のいずれも動作可能です。

コマンドでリンクモードをレイヤ 2 またはレイヤ 3 に設定できます。

Ethernet インタフェースのリンクモードを変更後、**shutdown** コマンドを除いて Ethernet インタフェースのすべてのコマンドは新しいリンクモードの初期状態に戻ります。

例

GigabitEthernet 1/0/1 をレイヤ 2 モードに設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] port link-mode bridge

1.1.22 reset counters interface

Syntax

reset counters interface [*interface-type* [*interface-number*]]

View

User view

定義済みユーザロール

network-admin

パラメータ

interface-type: インタフェースタイプを指定します。

interface-number: インタフェース番号を指定します。

説明

reset counters interface コマンドはインタフェースの統計情報を削除します。

一定期間、トラフィックの統計情報を収集する場合、以前に収集された統計情報の履歴を削除し、このコマンドを使用します。

インタフェースタイプを指定しない場合、すべてのインタフェースの統計情報を削除します。

インタフェースタイプのみを使用する場合、インタフェースタイプのすべてのインタフェースの統計情報を削除します。

インタフェースタイプとインタフェース番号を指定した場合、指定したインタフェースの統計情報を削除します。

例

GigabitEthernet 1/0/1 の統計情報を削除します。

<Switch> reset counters interface gigabitethernet 1/0/1

関連コマンド

- **display counters interface**
- **display counters rate interface**
- **display interface**

1.1.23 shutdown

Syntax

shutdown

undo shutdown

デフォルト

インタフェースはアップ状態です。

View

Ethernet interface view

定義済みユーザロール

network-admin

説明

shutdown コマンドはインタフェースをシャットダウンします。

undo shutdown コマンドはインタフェースをアップ状態にします。

あるインタフェースの設定が適用されていることを確認するため、インタフェースをシャットダウンし、その後アップ状態にする必要があることがあります。

shutdown コマンドと **loopback** コマンドを同時に設定することはできません。

例

GigabitEthernet 1/0/1 をシャットダウンし、その後アップ状態にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] shutdown

[Switch-GigabitEthernet1/0/1] undo shutdown

1.1.24 speed

Syntax

speed { **10** | **100** | **1000** | **auto** }

undo speed

デフォルト

auto

View

Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

10: インタフェースの通信速度を 10Mbps に設定します。

100: インタフェースの通信速度を 100Mbps に設定します。

1000: インタフェースの通信速度を 1000Mbps に設定します。

auto: ピアとの通信速度をオートネゴシエーションに設定します。

説明

speed コマンドはインタフェースの通信速度を設定します。

undo speed コマンドはデフォルトに戻します。

RJ-45 ポートでは、ピアのインタフェースの通信速度に一致するように **speed** コマンドを使用します。1000BASE-T SFP/SFP+を含む SFP/SFP+トランシーバモジュールで動作するポートでは **speed 10** と **100** は未サポートです。

パラメータはインタフェースタイプに依存します。詳細は interface view で **speed ?**コマンドを使用してください。

例

GigabitEthernet 1/0/1 の通信速度を auto に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] speed auto

関連コマンド

speed auto

1.1.25 unicast-suppression

注意：

suppression 機能を Ethernet インタフェースもしくはポートグループに複数設定した場合、設定値は以下の優先度で有効化されます。
ブロードキャスト＞不明なユニキャスト＞マルチキャスト
たとえば、**broadcast-suppression** コマンド、**multicast-suppression** コマンド、**unicast-suppression** コマンドをそれぞれ抑制比率 10/20/30 で設定した場合、ブロードキャストの値が反映され、ブロードキャスト、マルチキャスト、不明なユニキャストの合計が 10%まで疎通可能となります。
suppression 機能を pps で使用する場合、標準の 10/100/1000BASE-T ポートでは 65 の倍数、SFP/SFP+ポートでは 650 の倍数で制御します。

Syntax

unicast-suppression { *ratio* | **pps** *max-pps* | **kbps** *max-kbps* }

undo unicast-suppression

デフォルト

設定なし

View

Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

ratio: イーサネットポートの総伝送能力に対する不明なユニキャストトラフィックの最大比率です。設定範囲は 1～100%です。この比率が小さいほど、ポートを通過できる不明なユニキャストトラフィックは少なくなります。

pps *max-pps*: イーサネットポートごとに毎秒の不明なユニキャストパケットの最大数を指定します。単位は pps（パケット/秒）です。*max-pps* の設定範囲は 1～1.4881×最大インタフェースレートです。

kbps *max-kbps*: イーサネットポートごとに毎秒の不明なユニキャストトラフィックの最大数を指定します。単位は kbps（キロビット/秒）です。*max-kbps* の設定範囲は、1～最大インタフェースレートです。

説明

unicast-suppression コマンドは不明なユニキャストパケットの転送を抑制することを有効にし、しきい値を設定します。

undo unicast-suppression コマンドは不明なユニキャストパケットの転送を抑制することを無効にします。

インタフェースで不明なユニキャストトラフィックのサイズを制限するため、不明なユニキャストストーム抑制機能を使用することができます。インタフェースの不明なユニキャストトラフィックがしきい値を超過したとき、システムはトラフィックがしきい値を下回るまでパケットを廃棄します。

storm-constrain コマンドと **unicast-suppression** コマンドの両方はポートで不明なユニキャストストームを抑制することができます。

- **storm-constrain** コマンドは不明なユニキャストトラフィックを抑制するためにソフトウェアを使用します。ある程度まで装置の性能に影響を及ぼします。
- **unicast-suppression** コマンドは不明なユニキャストトラフィックを抑制するためにハードウェアのチップを使用します。装置の性能への影響は **storm-constrain** コマンドよりも小さくなります。

storm-constrain コマンドと **unicast-suppression** コマンドを同時に設定しないでください。そうでなければ設定した機能が正常に動作しません。

抑制するしきい値を kbps で設定するとき、正確な抑制しきい値は、設定する値と異なります。

- 設定された値が 64 よりも小さい場合、64 の値が適用されます。
- 設定された値が 64 の整数倍より大きく、64 の整数倍でない場合、設定された 64 の整数倍にもっとも近い値が適用されます。

適用される抑制しきい値は、装置の表示画面を参照してください。

例

GigabitEthernet 1/0/1 で不明なユニキャストストーム抑制のしきい値を 10000kbps に設定します。

<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.
```

出力はしきい値が 10048kbps（64 の 157 倍）に設定されていることを示します。

関連コマンド

- **broadcast-suppression**
- **multicast-suppression**

1.1.26 unknown-unicast block outbound

Syntax

unknown-unicast block outbound

undo unknown-unicast block outbound

デフォルト

設定なし

View

Ethernet interface view

定義済みユーザロール

network-admin

説明

unknown-multicast block outbound を使用すると、 インタフェース で発信元の不明なマルチキャストパケットを廃棄できます。

undo unknown-multicast block outboun で、デフォルトに戻ります。

例

GigabitEthernet 1/0/1 を有効にして、不明なユニキャストパケットをドロップします。。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] unknown-unicast block outbound

1.2 レイヤ2 Ethernetインタフェース設定コマンド

1.2.1 display storm-constrain

Syntax

display storm-constrain [**broadcast** | **multicast** | **unicast**] [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

broadcast: ブロードキャスト抑止機能の設定と統計情報を表示します。

multicast: マルチキャスト抑止機能の設定と統計情報を表示します。

unicast: 不明なユニキャスト抑止機能の設定と統計情報を表示します。

interface *interface-type interface-number*: インタフェースのタイプと番号を指定します。パラメータを指定しない場合、ストーム抑止機能が有効なすべてのインタフェースの設定と統計情報を表示します。

説明

display storm-constrain コマンドはストーム抑止機能の設定と統計情報を表示します。

パラメータを指定しない場合、有効なストーム抑止機能のすべての設定と統計情報を表示します。

例

有効なストーム抑止機能のすべての設定と統計情報を表示します。

<Switch> display storm-constrain

```
Abbreviation: BC - broadcast; MC - multicast; UC - 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
```

表 1-5 コマンド出力

フィールド	説明
Flow Statistic Interval	ストーム抑止モジュールのトラフィックポーリング間隔です。単位は秒です。
Port	省略されたポート名です。
Type	ストーム抑止機能が有効なトラフィックタイプです。 ● **BC**—ブロードキャストパケットです。 ● **MC**—マルチキャストパケットです。 ● **UC**—不明なユニキャストパケットです。
Lower	ストーム抑止の下限値です。単位はpps、kbps、%です。
Upper	ストーム抑止の上限値です。単位はpps、kbps、%です。
Unit	ストーム抑止のしきい値の単位です。 ● ppsです。 ● kbpsです。 ● %です。
CtrlMode	上限に到達したときの保護動作です。(blockあるいはshutdownがあります) N/Aは保護動作が設定されていないことを示します。
Status	パケットの転送状態です。 ● **forwarding** —ポートが正常にトラフィックを転送しています。 ● **shutdown**—ポートがシャットダウンです。 ● **block**—ポートがトラフィックのタイプを廃棄します。
Trap	ストーム抑止がしきい値に到達した際のトラップの状態です。 ● **on**—ポートはしきい値イベントをトラップします。 ● **off**—ポートはしきい値イベントをトラップしません。
Log	ストーム抑止がしきい値に到達した際のログの状態です。 ● **on**—ポートはしきい値イベントをログに保存します。 ● **off**—ポートはしきい値イベントをログに保存しません。
SwitchNum	インタフェースの転送状態の変更回数です。 カウントが65535に到達したとき、自動でリセットされます。

1.2.2 mdix-mode

重要:

このコマンドは SFP/SFP+ポートで未サポートです。

Syntax

mdix-mode { **automdix** | **mdi** | **mdix** }

undo mdix-mode

デフォルト

automdix

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

automdix: ピアのピンの役割をネゴシエートするインタフェースを指定します。

mdi: ピン 1、ピン 2 が送信、ピン 3、ピン 6 が受信に指定します。

mdix: ピン 1、ピン 2 が受信、ピン 3、ピン 6 が送信に指定します。

説明

mdix-mode コマンドは Ethernet インタフェースの MDIX（Medium Dependent Interface Cross-Over）モードを設定します。

undo mdix-mode コマンドはデフォルトに戻します。

例

GigabitEthernet 1/0/1 を automdix モードで動作するように設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] mdix-mode automdix

1.2.3 speed auto

Syntax

speed auto { **10** | **100** | **1000** } *

undo speed

デフォルト

設定なし

View

100Mbps あるいは 1000Mbps の Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

10: ポートのオートネゴシエーションの通信速度を 10Mbps に指定します。

100: ポートのオートネゴシエーションの通信速度を 100Mbps に指定します。

1000: ポートのオートネゴシエーションの通信速度を 1000Mbps に指定します。

説明

speed auto コマンドはオートネゴシエーションの通信速度を設定します。

undo speed コマンドはデフォルトに戻します。

speed コマンドと **speed auto** コマンドはどちらか一方のコマンドのみ適用します。

speed コマンドと **speed auto** コマンドを両方設定した場合、最後に設定されたコマンドが適用されます。

- ポート上で **speed auto 100 1000** コマンドを設定した後、**speed 100** コマンドを設定した場合、ネゴシエーションされることなく 100Mbps 固定になります。
- ポート上で **speed 100** コマンドを設定した後で、**speed auto 100 1000** コマンドを設定した場合、ネゴシエーションを行い 100 Mbps または 1000 Mbps のどちらかになります。

speed auto コマンドは接続装置間でインタフェースがサポートする最速の通信速度を設定します。ネゴシエーションするため、パラメータを絞り込むことができます。ネゴシエーションの失敗を避けるため、接続装置で少なくとも 1 つは速度設定を一致させてください。

例

GigabitEthernet 1/0/1 のオートネゴシエーションの通信速度を 10 Mbps あるいは 1000 Mbps に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] speed auto 10 1000

関連コマンド

speed

1.2.4 storm-constrain

Syntax

storm-constrain { **broadcast** | **multicast** | **unicast** } { **pps** | **kbps** | **ratio** } *upperlimit lowerlimit*

undo storm-constrain { **all** | **broadcast** | **multicast** | **unicast** }

デフォルト

無効

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

all: パケットのすべてのタイプ（ブロードキャスト、マルチキャスト、不明なユニキャスト）のストーム抑止を無効にします。

broadcast: ブロードキャストストーム抑止を有効あるいは無効にします。

multicast: マルチキャストストーム抑止を有効あるいは無効にします。

unicast:不明なユニキャストストーム抑止を有効あるいは無効にします。

pps: ストーム抑止のしきい値の単位を pps で指定します。

kbps: ストーム抑止のしきい値の単位を kbps で指定します。

ratio: ストーム抑止のしきい値をインタフェースの転送能力の割合で指定します。

upperlimit: 上限のしきい値を指定します。単位は pps、kbps、%です。

- **pps** パラメータを指定した場合、上限のしきい値は 0～1.4881×インタフェースレートです。
- **kbps** パラメータを指定した場合､上限のしきい値は 0～インタフェースレートです。
- **ratio** パラメータを指定した場合、上限のしきい値は 0～100%です。

lowerlimit: 下限のしきい値を指定します。単位は pps、kbps、%です。

- **pps** パラメータを指定した場合、下限のしきい値は 0～1.4881×インタフェースレートです。

- **kbps** パラメータを指定した場合、下限のしきい値は 0～インタフェースレートです。
- **ratio** パラメータを指定した場合、下限のしきい値は 0～100%です。

説明

storm-constrain コマンドはポートでブロードキャスト、マルチキャスト、不明なユニキャストのストーム抑止を有効にします。

undo storm-constrain コマンドはストーム抑止を無効にします。

このコマンドを設定した後、装置は指定したポーリングサイクルでトラフィックの特定タイプの統計情報を収集します。ポーリングサイクルは **storm-constrain interval** コマンドで設定することができます。トラフィックの特定のタイプが上限を超過した場合、インタフェースは **storm-constrain control** コマンドで設定されたアクションを実行します。

storm-constrain コマンド、**broadcast-suppression** コマンド、**multicast-suppression** コマンド、**unicast-suppression** コマンドはポートでストームを抑制することができます。

- **storm-constrain** コマンドはブロードキャストトラフィックを抑制するためにソフトウェアを使用します。ある程度まで装置の性能に影響を及ぼします。
- **broadcast-suppression** コマンド、**multicast-suppression** コマンド、**unicast-suppression** コマンドはブロードキャストトラフィックを抑制するためにハードウェアのチップを使用します。装置の性能への影響は **storm-constrain** コマンドよりも小さくなります。

トラフィックの同じタイプに **storm constrain** コマンドと、**broadcast-suppression** コマンド、**multicast-suppression** コマンド、**unicast-suppression** コマンドのいずれかの設定を一緒に設定しないでください。そうでないとトラフィックの抑止は正しく動作しません。

この設定を行うとき、*upperlimit* は *lowerlimit* よりも大きい値にしてください。

例

GigabitEthernet 1/0/1 で不明なユニキャストのストーム抑止を有効にし、上限のしきい値を 150pps、下限のしきい値を 200pps に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] storm-constrain unicast pps 200 150

GigabitEthernet 1/0/2 でブロードキャストのストーム抑止を有効にし、上限のしきい値を 2000kbps、下限のしきい値を 1500kbps に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/2

[Switch-GigabitEthernet1/0/2] storm-constrain broadcast kbps 2000 1500

GigabitEthernet 1/0/3 でマルチキャストのストーム抑止を有効にし、上限のしきい値を 80%、下限のしきい値を 15%に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/3

[Switch-GigabitEthernet1/0/3] storm-constrain multicast ratio 80 15

関連コマンド

- **storm-constrain control**
- **storm-constrain interval**

🕮 **メモ：**

- suppression(パケット転送抑制機能)で指定しているタイプと同じパケットタイプを、storm-constrain(ストーム抑止機能)で指定した場合は正しく動作しません。たとえば、broadcast-suppression と storm-constrain broadcast を同じポートに設定しないでください。
- しきい値の上限値は、下限値より小さい値を設定できません。また、しきい値の上限値と下限値を同じ値に設定しないことを推奨します。
- storm-constrain unicast コマンドを設定した場合、Unknown ユニキャストと Known ユニキャストを区別せず、両方のユニキャストパケットが制御されます。
- Unknown ユニキャストのみストーム抑止を行いたい場合には、同様の機能であるストーム抑制機能(unicast-suppression)を使用してください。

1.2.5 storm-constrain control

Syntax

storm-constrain control { **block** | **shutdown** }

undo storm-constrain control

デフォルト

設定なし

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

block: 該当タイプのトラフィック転送を停止します。該当以外のトラフィックは転送します。インタフェースはブロックされたトラフィックを転送しませんが、トラフィック

をカウントします。ブロックされたトラフィックが下限のしきい値を下回ったと検出したとき、ポートはトラフィックを転送し始めます。

shutdown: 自動的にシャットダウンします。インタフェースは自動的にシャットダウンし、すべてのトラフィックの転送を停止します。ブロックされたトラフィックが下限のしきい値を下回ったと検出したとき、ポートはトラフィックを転送しません。インタフェースを up にするため、**undo shutdown** コマンドを実行するか、ストーム抑止を無効にする必要があります。

説明

storm-constrain control コマンドはトラフィックのタイプ（不明なユニキャスト、マルチキャスト、あるいはブロードキャスト）がストーム抑止の上限のしきい値を超過したとき、インタフェースで実行するアクションを設定します。

undo storm-constrain control コマンドはデフォルトに戻します。

例

トラフィックがストーム抑止の上限のしきい値を超過したと検出したとき、トラフィックをブロックするように GigabitEthernet 1/0/1 を設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] storm-constrain control block

関連コマンド

- **storm-constrain**
- **storm-constrain control**

1.2.6 storm-constrain enable log

Syntax

storm-constrain enable log

undo storm-constrain enable log

デフォルト

モニタされたトラフィックが上限のしきい値を超過あるいは下限のしきい値を下回ったとき、インタフェースはログの送信を有効にします。

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

説明

storm-constrain enable log コマンドはインタフェースでストーム抑止のしきい値イベントのログの送信を有効にします。

undo storm-constrain enable log コマンドはログの送信を無効にします。

例

ストーム抑止のしきい値イベントを検出したとき、GigabitEthernet 1/0/1 でログの送信を有効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] storm-constrain enable log

1.2.7 storm-constrain enable trap

Syntax

storm-constrain enable trap

undo storm-constrain enable trap

デフォルト

モニタされたトラフィックが上限のしきい値を超過あるいは下限のしきい値を下回ったとき、インタフェースはトラップの送信を有効にします。

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

説明

storm-constrain enable trap コマンドはインタフェースでストーム抑止のしきい値イベントのトラップの送信を有効にします。

undo storm-constrain enable trap コマンドはトラップの送信を無効にします。

例

ストーム抑止のしきい値イベントを検出したとき、GigabitEthernet 1/0/1 でトラップの送信を有効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] storm-constrain enable trap

1.2.8 storm-constrain interval

Syntax

storm-constrain interval *interval*

undo storm-constrain interval

デフォルト

10 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

interval: ストーム抑止のトラフィックを計測するポーリング間隔を設定します。設定範囲は 1～300 秒です。ネットワークの信頼性のため、デフォルト値以上の値を使用してください。

説明

storm-constrain interval コマンドはストーム抑止のトラフィックを計測するポーリング間隔を設定します。

undo storm-constrain interval コマンドはデフォルトに戻します。

storm-constrain interval コマンドによって設定された間隔は、ストーム抑止機能の間隔です。インタフェースのポーリング間隔の統計情報を設定する場合、**flow-interval** コマンドを使用します。

例

ストーム抑止のトラフィックを計測するポーリング間隔を 60 秒に設定します。

<Switch> system-view

[Switch] storm-constrain interval 60

関連コマンド

- **storm-constrain**
- **storm-constrain control**

1.2.9 virtual-cable-test

重要：

このコマンドは SFP/SFP+ポートで未サポートです。
リンクアップしていないポートでは動作しません。

Syntax

virtual-cable-test

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

説明

virtual-cable-test コマンドは Ethernet インタフェースのケーブル接続をテストし、テスト結果を表示します。

テスト結果は参考情報です。ケーブル長の最大誤差は 10mです。

テストが有効でない場合、ハイフン（-）が表示されます。

例

GigabitEthernet 1/0/1 のケーブル接続のテストを行います。

<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
```

表 1-6 コマンド出力

フィールド	説明
Cable status	ケーブルの状態です。 ● **Normal**—ケーブルが良好です。 ● **Abnormal**—ケーブルが異常です。 ● **Abnormal (open)**—断線が検出されました。 ● **Abnormal (short)**—ショートが検出されました。 ● **Failure**—テストが失敗しました。
n metre(s)	ケーブル接続が正常に行われている場合、このフィールドはケーブルの長さが表示されます。

目次

このセクションのページは **3-x-x** です。

2 章 ループバックインタフェースと Null インタフェース 2-1
2.1 ループバックインタフェースと Null インタフェース設定コマンド 2-1
2.1.1 description 2-1
2.1.2 display interface loopback 2-2
2.1.3 display interface null 2-5
2.1.4 interface loopback 2-7
2.1.5 interface null 2-8
2.1.6 reset counters interface loopback 2-8
2.1.7 reset counters interface null 2-9
2.1.8 shutdown 2-10

2章 ループバックインタフェースと Null インタフェース

2.1 ループバックインタフェースとNullインタフェース設定コマンド

2.1.1 description

Syntax

description *text*

undo description

デフォルト

インタフェース名＋Interface です。（たとえば、LoopBack1 Interface です）

View

Loopback interface view

Null interface view

定義済みユーザロール

network-admin

パラメータ

text: インタフェースの説明を記載します。設定範囲は 1～255 文字です。大文字、小文字を区別します。

説明

description コマンドはインタフェースの説明を設定します。

undo description コマンドはデフォルトに戻します。

インタフェースの説明を設定することで、インタフェースの識別、管理しやすさを向上させることができます。

設定された説明を表示する場合、**display interface** コマンドを使用します。

例

ループバック 1 の説明を RouterID に設定します。

<Switch> system-view

[Switch] interface loopback 1

[Switch-LoopBack1] description for RouterID

2.1.2 display interface loopback

Syntax

display interface loopback [*interface-number*] [**brief** [**description** | **down**]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface-number: ループバックインタフェースの番号を指定します。番号は存在するループバックのインタフェースの番号です。番号を指定しない場合、装置のすべての既存のループバックインタフェースの情報を表示します。

brief: インタフェースの概要を表示します。指定しない場合、詳細なインタフェースの情報を表示します。

description: 完全なインタフェースの説明を表示します。指定しない場合、説明の最初の 27 文字のみを表示します。

down: down 状態のインタフェースの情報と原因を表示します。指定しない場合、すべての状態のインタフェースの情報を表示します。

説明

display interface loopback コマンドは指定した、あるいはすべての既存のループバックインタフェースの情報を表示します。

ループバックインタフェースが作成されたのち、適用されます。

例

ループバック 0 のインタフェースの詳細情報を表示します。

<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
```

表 2-1 コマンド出力

フィールド	説明
Current state	ループバックインタフェースの物理レイヤの状態です。 ● **UP**—ループバックインタフェースがパケットの送受信を行うことができます。 ● **Administratively DOWN**—インタフェースが**shutdown**コマンドにより手動でシャットダウンしています。
Line protocol state	インタフェースのリンクレイヤプロトコルの状態です。**UP (spoofing)**はインタフェースのリンクレイヤプロトコルですが、オンデマンドのリンクあるいは準備ができていない状態です。この属性はNullインタフェースとループバックインタフェースの一般的な状態です。
Description	インタフェースの説明です。
Bandwidth	インタフェースの帯域幅です。値が0の場合、このフィールドは表示されません。
Maximum transmission unit	インタフェースのMTUです。
Internet protocol processing: Disabled	インタフェースにIPアドレスが設定されていないため、IPパケットを処理できません。
Internet address: 1.1.1.1/32 (primary)	インタフェースのIPアドレスです。primaryはIPアドレスがプライマリIPアドレスであることを示します。
Physical: Loopback	インタフェースの物理タイプがループバックです。
Last clearing of counters	インタフェースで**reset counters interface**コマンドを最後に使用した時間です。 **Never**は装置が起動してから**reset counters interface**コマンドを一度も使用していないことを示します。
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec	最新の300秒の平均受信レートです。 ● **bytes/sec**—1秒間に受信した平均バイト数です。 ● **bits/sec**—1秒間に受信した平均ビット数です。 ● **packets/sec**—1秒間に受信した平均パケット数です。

フィールド	説明
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec	最新の300秒の平均送信レートです。 ● **bytes/sec**—1秒間に送信した平均バイト数です。 ● **bits/sec**—1秒間に送信した平均ビット数です。 ● **packets/sec**—1秒間に送信した平均パケット数です。
Input: 0 packets, 0 bytes, 0 drops	インタフェースの受信パケットの総数とサイズ（単位はバイトです）と廃棄したパケット数です。
Output: 0 packets, 0 bytes, 0 drops	インタフェースの送信パケットの総数とサイズ（単位はバイトです）と廃棄したパケット数です。

すべてのループバックインタフェースの概要情報を表示します。

<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
```

down 状態のすべてのループバックインタフェースの情報と原因を表示します。

<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
```

表 2-2 コマンド出力

フィールド	説明
Link	インタフェースの物理リンク状態です。 ● **UP**—リンクがupです。 ● **DOWN**—リンクが物理的にdownしています。 ● **ADM**—リンクが運用上でシャットダウンしています。物理状態を回復するために、**undo shutdown**コマンドを実行します。 ● **Stby**—インタフェースがstandbyインタフェースです。

フィールド	説明
Protocol	インタフェースのデータリンクレイヤプロトコルフィールドの説明です。このフィールドは**UP(s)**と表示されます。**UP(s)**はインタフェースがリンクレイヤでupしていますが、オンデマンドのリンクあるいは準備ができていない状態です。（**s**）はスプーフィングを示します。この属性はインタフェースNull 0、ループバックインタフェースの一般的な状態です。
Primary IP	インタフェースのプライマリIPアドレスです。
Description	インタフェースの説明です。
Cause	インタフェースの物理リンク状態がDOWNとなった原因です。**shutdown**コマンドでインタフェースがシャットダウン状態であるとき、このフィールドは**Administratively**と表示されます。物理状態を回復するために、**undo shutdown**コマンドを実行します。

関連コマンド

- **interface loopback**
- **reset counters interface loopback**

2.1.3 display interface null

Syntax

display interface null [**0**] [**brief** [**description** | **down**]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

0: Null 0 インタフェースを指定します。

brief: インタフェースの概要情報を表示します。指定しない場合、詳細なインタフェースの情報を表示します。

description: 完全なインタフェースの説明を表示します。指定しない場合、説明の最初の 27 文字のみを表示します。

down: down 状態のインタフェースの情報と原因を表示します。指定しない場合、すべての状態のインタフェースの情報を表示します。

説明

display interface null コマンドは Null インタフェースの情報を表示します。

装置は 1 つの Null 0 インタフェースのみがあります。

null を指定した場合、0 パラメータの指定にかかわらず、Null 0 インタフェースの情報を表示します。

例

Null 0 インタフェースの詳細情報を表示します。

<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
```

Null 0 インタフェースの概要情報を表示します。

<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)    --
```

コマンド出力は表 2-1、表 2-2 を参照してください。

関連コマンド

- **interface null**
- **reset counters interface null**

2.1.4 interface loopback

Syntax

interface loopback *interface-number*

undo interface loopback *interface-number*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

*interface-numbe*r: ループバックインタフェースを指定します。設定範囲は 0～127 です。

説明

interface loopback コマンドはループバックインタフェースを作成し、loopback interface view に移行します。すでにループバックインタフェースが存在する場合、loopback interface view に移行します。

undo interface loopback コマンドはループバックインタフェースを削除します。

ループバックインタフェースの物理レイヤの状態とリンクレイヤプロトコルは手動でシャットダウンしない限り、常に up 状態です。このため、以下の目的に使用することができます。

- インタフェースの物理状態に影響されることなく、接続状態となります。
- 接続の信頼性を改善します。

たとえば、FTP 接続を確立するために送信元インタフェースとしてループバックインタフェースを設定することができます。

例

インタフェースループバック 1 を作成します。

<Switch> system-view

[Switch] interface loopback 1

[Switch-LoopBack1]

2.1.5 interface null

Syntax

interface null 0

デフォルト

装置は 1 つの Null インタフェース(Null 0)があります。作成あるいは削除することができません。

View

System view

定義済みユーザロール

network-admin

パラメータ

0: Null 0 インタフェースを指定します。Null インタフェースの番号は常に 0 です。

説明

interface null コマンドは null interface view に移行します。

例

null 0 interface view に移行します。

<Switch> system-view

[Switch] interface null 0

[Switch-NULL0]

2.1.6 reset counters interface loopback

Syntax

reset counters interface loopback [*interface-number*]

View

User view

定義済みユーザロール

network-admin

パラメータ

interface-number: ループバックインタフェースの番号を指定します。番号は存在するループバックのインタフェースの番号です。番号を指定しない場合、装置のすべての既存のループバックインタフェースの統計情報を削除します。

説明

reset counters interface loopback コマンドは指定した、あるいはすべての既存のループバックインタフェースの統計情報を削除します。

一定期間、ループバックインタフェースのトラフィックの統計情報を収集する場合、以前に収集された統計情報の履歴を削除するために **reset counters interface** [**loopback** [*interface-number*]]コマンドを使用します。その後、自動で統計情報を収集します。

このコマンドは少なくとも 1 つのループバックインタフェースが作成されている場合のみ有効です。

例

ループバックインタフェース 1 の統計情報を削除します。

<Switch> reset counters interface loopback 1

関連コマンド

display interface loopback

2.1.7 reset counters interface null

Syntax

reset counters interface null [**0**]

View

User view

定義済みユーザロール

network-admin

パラメータ

0: Null 0 インタフェースを指定します。Null インタフェースの番号は常に 0 です。

説明

reset counters interface null コマンドは Null インタフェースの統計情報を削除します。

一定期間、Null インタフェースのトラフィックの統計情報を収集する場合、以前に収集された統計情報の履歴を削除するために **reset counters interface** [**null** [**0**]]コマンドを使用します。その後、自動で統計情報を収集します。

例

Null 0 インタフェースの統計情報を削除します。

<Switch> reset counters interface null 0

関連コマンド

display interface null

2.1.8 shutdown

Syntax

shutdown

undo shutdown

デフォルト

up

View

Loopback interface view

定義済みユーザロール

network-admin

説明

shutdown コマンドはループバックインタフェースをシャットダウンします。

undo shutdown コマンドはループバックインタフェースを up にします。

このコマンドはインタフェースの接続を切断し、通信を行うためのインタフェースを無効にするため、**shutdown** コマンドを使用する際には影響を考慮してください。

例

ループバックインタフェース Loopback 1 をシャットダウンします。

<Switch> system-view

[Switch] interface loopback 1

[Switch-LoopBack1] shutdown

目次

このセクションのページは **3-x-x** です。

3 章 Interface range 3-1
3.1 Interface range 設定コマンド 3-1
3.1.1 display interface range 3-1
3.1.2 interface range 3-2
3.1.3 interface range name 3-3

3章 Interface range

3.1 Interface range設定コマンド

3.1.1 display interface range

Syntax

display interface range [**name** *name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

name *name*: インタフェースレンジの名前を指定します。設定範囲は 1～32 文字です。大文字、小文字を区別します。指定しない場合、**interface range name** コマンドで作成されたすべてのインタフェースレンジの情報を表示します。

説明

display interface range コマンドは **interface range name** コマンドを使用して作成されたインタフェースレンジの情報を表示します。

例

interface range name コマンドを使用して作成されたすべての既存のインタフェースレンジの情報を表示します。

<Switch> display interface range

```
Interface range name t2 GigabitEthernet1/0/1 GigabitEthernet1/0/2
Interface range name test GigabitEthernet1/0/3 GigabitEthernet1/0/4
```

出力は以下のことを示します。

- インタフェースレンジ **t2** に GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 が追加されました。
- インタフェースレンジ **test** に GigabitEthernet 1/0/3 と GigabitEthernet 1/0/4 が追加されました。

関連コマンド

interface range name

3.1.2 interface range

Syntax

interface range *interface-list*

View

System view

定義済みユーザロール

network-admin

パラメータ

interface-list: インタフェースを指定します。半角スペースで区切り、24 までインタフェースを指定するか、インタフェースの範囲を指定します。インタフェースの範囲の形式は *interface-type interface-number* **to** *interface-type interface-number* です。*interface-type interface-number1* **to** *interface-type interface-number2* を指定したとき、*interface-number2* は *interface-number1* 以上の値にしてください。

説明

interface range コマンドはインタフェースレンジを作成し、interface range view に移行します。

同じ機能を 1 つずつインタフェースに設定する代わりに、interface range view に移行して、複数のインタフェースをまとめて実行することができます。たとえば、インタフェースの範囲をシャットダウンするため、interface range view で **shutdown** コマンドを実行します。

interface range コマンドで作成されたインタフェースレンジはカレントコンフィグレーションに保存されません。インタフェースレンジは繰り返し使用することができません。使用したインタフェースレンジを繰り返し使用する場合、**interface range name** コマンドを使用します。

interface range view では、最初に指定したインタフェースでサポートされるコマンドのみが有効です。最初に指定するインタフェースは **interface range** コマンドで指定されます。インタフェースレンジのコマンドを表示する場合、interface range view に移行し、インタフェースのコマンドラインでクエスチョン（**?**）を入力します。

interface range view でコマンドを実行した後、以下のいずれかの状態が起こる可能性があります。

- システムは、エラーメッセージを表示し interface range view にとどまります。それは、メンバインタフェースで実行が失敗したことを意味します。
  - □ 最初のメンバインタフェースで失敗した場合、コマンドはどのメンバインタフェースでも実行されません。

- □ 最初のメンバインタフェース以外で失敗した場合、コマンドは他のメンバインタフェースでは有効となります。
- システムは system view に戻ります。それは、以下を意味します。
  - □ コマンドは system view と interface view のいずれでもサポートされています。
  - □ interface range view において、メンバインタフェースでの実行に失敗しましたが、system view で成功しました。
  - □ コマンドは、それ以降のメンバインタフェースで実行されませんでした。

display this コマンドで、それぞれのメンバインタフェースの interface view における設定を確認することができます。また、system view での設定が不要な場合、設定を取り消すために **undo** コマンドを使用してください。

インタフェースレンジの最初に指定したインタフェースの設定を確認する場合、interface range view で **display this** コマンドを実行します。

インタフェースレンジの設定を行う場合、以下のガイドラインに従ってください。

- インタフェースレンジで最初に指定するインタフェースを設定する前に、**interface** *interface-type interface-number* コマンドを使用してインタフェースの view に移行できることを確認してください。
- インタフェースレンジにアグリゲートインタフェースとアグリゲートインタフェースのメンバインタフェースの両方を割り当てないでください。アグリゲートインタフェースとアグリゲートインタフェースのメンバインタフェースの両方で実行すると、コマンドはアグリゲーションに失敗します。
- インタフェースレンジのインタフェースの最大数の制限の設定はありません。インタフェースレンジで多くのインタフェースを設定する場合、実行時間が長くなります。

例

GigabitEthernet 1/0/1～GigabitEthernet 1/0/5 をシャットダウンします。

```
<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

Syntax

interface range name *name* [**interface** *interface-list*]

undo interface range name *name*

View

System view

定義済みユーザロール

network-admin

パラメータ

name: インタフェースレンジの名前を指定します。設定範囲は 1～32 文字です。大文字、小文字を区別します。

interface-list: インタフェースを指定します。半角スペースで区切り、24 までインタフェースを指定するか、インタフェースの範囲を指定します。インタフェースの範囲の形式は *interface-type interface-number* **to** *interface-type interface-number* です。*interface-type interface-number1* **to** *interface-type interface-number2* を指定したとき、*interface-number2* は *interface-number1* 以上の値にしてください。

説明

interface range name *name* **interface** *interface-list* コマンドはインタフェースレンジを作成し、インタフェースレンジの名前を設定し、interface range view に移行します。

interface パラメータを指定しない場合、指定された名前のインタフェースレンジの view に移行します。

undo interface range name コマンドは指定された名前のインタフェースレンジを削除します。

インタフェースレンジに名前を割り当てるために、コマンドを使用することができます。インタフェースレンジではなくインタフェースの名前を指定して interface range view に移行することができます。

interface range name コマンドで作成されたインタフェースレンジはカレントコンフィグレーションに保存され、メンバインタフェースを繰り返し使用することができます。

interface range view では、最初に指定したインタフェースでサポートされているコマンドのみ有効ですインタフェースレンジの最初に指定したインタフェースでサポートされるコマンドを表示する場合、interface range view に移行し、インタフェースのコマンドラインでクエスチョン（**?**）を入力します。

interface range view でコマンドを実行した後、以下のいずれかの状態が起こる可能性があります。

- システムは、エラーメッセージを表示し interface range view にとどまります。それは、メンバインタフェースで実行が失敗したことを意味します。
  - □ 最初のメンバインタフェースで失敗した場合、コマンドはどのメンバインタフェースでも実行されません。
  - □ 最初のメンバインタフェース以外で失敗した場合、コマンドは他のメンバインタフェースでは有効となります。
- システムは、system view に戻ります。それは、以下を意味します。
  - □ コマンドは system view と interface view のいずれでもサポートされています。
  - □ interface range view において、メンバインタフェースでの実行に失敗しましたが、system view で成功しました。
  - □ コマンドは、それ以降のメンバインタフェースで実行されませんでした。

display this コマンドで、それぞれのメンバインタフェースの interface view における設定を確認することができます。また、system view での設定が不要な場合、設定を取り消すために **undo** コマンドを使用してください。

インタフェースレンジの最初に指定したインタフェースの設定を確認する場合、interface range view で **display this** コマンドを実行します。

インタフェースレンジのメンバインタフェースを表示する場合、**display interface range** コマンドを使用します。

インタフェースレンジの設定を行う場合、以下のガイドラインに従ってください。

- インタフェースレンジで最初に指定するインタフェースを設定する前に、**interface** *interface-type interface-number* コマンドを使用してインタフェースの view に移行できることを確認してください。
- インタフェースレンジにアグリゲートインタフェースとアグリゲートインタフェースのメンバインタフェースの両方を割り当てないでください。アグリゲートインタフェースとアグリゲートインタフェースのメンバインタフェースの両方で実行すると、コマンドはアグリゲーションに失敗します。
- インタフェースレンジのインタフェースの最大数の制限の設定はありません。インタフェースレンジで多くのインタフェースを設定する場合、実行時間が長くなります。
- インタフェースレンジの名前の最大数はシステムリソースによってのみ制限されます。インタフェースレンジの設定を保証するため、1000 個のインタフェースレンジの名前より少ない数にしてください。

例

インタフェースレンジ **myEthPort** に GigabitEthernet 1/0/1～GigabitEthernet 1/0/5 を追加し、interface range view に移行します。

<Switch> system-view

[Switch] interface range name myEthPort interface gigabitethernet 1/0/1 to gigabitethernet 1/0/5

[Switch-if-range-myEthPort]

インタフェースレンジ **myEthPort** の view に移行します。

<Switch> system-view

[Switch] interface range name myEthPort

[Switch-if-range-myEthPort]

関連コマンド

display interface range

目次

このセクションのページは **3-x-x** です。

4 章 MAC アドレステーブル 4-1
4.1 MAC アドレステーブル設定コマンド 4-1
4.1.1 display mac-address 4-1
4.1.2 display mac-address aging-time 4-3
4.1.3 display mac-address hash-bucket-size 4-4
4.1.4 display mac-address mac-learning 4-4
4.1.5 display mac-address mac-move 4-6
4.1.6 display mac-address statistics 4-7
4.1.7 mac-address (interface view) 4-8
4.1.8 mac-address (system view) 4-10
4.1.9 mac-address hash-bucket-size 4-13
4.1.10 mac-address mac-learning enable 4-14
4.1.11 mac-address mac-move fast-update 4-16
4.1.12 mac-address mac-roaming enable 4-16
4.1.13 mac-address max-mac-count 4-17
4.1.14 mac-address max-mac-count enable-forwarding 4-18
4.1.15 mac-address notification mac-move 4-19
4.1.16 mac-address notification mac-move suppression (interface view) 4-21
4.1.17 mac-address notification mac-move suppression (system view) 4-22
4.1.18 mac-address timer 4-23
4.1.19 mac-learn-mode 4-24
4.1.20 snmp-agent trap enable mac-address 4-25

4章 MAC アドレステーブル

4.1 MACアドレステーブル設定コマンド

4.1.1 display mac-address

Syntax

display mac-address [*mac-address* [**vlan** *vlan-id*] | [[**dynamic** | **static**] [**interface** *interface-type interface-number*] | **blackhole** | **multiport**] [**vlan** *vlan-id*] [**count**]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

mac-address: MAC アドレスを指定します。形式は H-H-H です。H の先頭から 0 が続く場合は省略できます。たとえば、000f-00e2-0001 は、f-e2-1 と省略できます。

vlan *vlan-id*: VLAN ID を指定します。設定範囲は 1～4094 です。

dynamic: ダイナミック MAC アドレスエントリを表示します。

static: スタティック MAC アドレスエントリを表示します。

interface *interface-type interface-number*: インタフェースのタイプと番号を指定します。

blackhole: ブラックホール MAC アドレスエントリを表示します。

multiport:マルチポートユニキャスト MAC アドレスエントリを表示します。

count: コマンドで指定したすべてのエントリに一致する MAC アドレスエントリ数のみを表示します。MAC アドレスエントリの詳細は表示されません。たとえば、VLAN 20 のダイナミックエントリ数を表示する場合、**display mac-address vlan** *20* **dynamic count** コマンドを使用します。エントリの属性が指定されない場合、MAC アドレステーブルのエントリ数を表示します。**count** を指定しない場合、指定された MAC アドレスエントリの詳細情報を表示します。

説明

display mac-address コマンドは MAC アドレスエントリを表示します。

MAC アドレスエントリは宛先 MAC アドレス、出力インタフェース、VLAN ID が含まれます。

パラメータを指定しない場合、すべての MAC アドレスエントリを表示します。

アグリゲートインタフェースに少なくとも 1 つの Selected メンバポートがある場合、アグリゲートインタフェースのダイナミック MAC アドレスエントリのみ表示します。

マルチポートユニキャスト MAC アドレスエントリは、MAC アドレス学習に影響しません。送信元 MAC アドレスがマルチポートユニキャストエントリと一致するフレームを受信しても、装置はそのフレームの MAC アドレスを学習し、ダイナミックエントリを生成できます。ただし、生成されたダイナミックエントリの優先度は低くなります。装置は、エントリの MAC アドレスを宛先とするフレームの転送にマルチポートユニキャストエントリを使用することを選択します。

例

VLAN 100 の MAC アドレスエントリを表示します。

<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
```

MAC アドレスエントリ数を表示します。

<Switch> display mac-address count

```
1 mac address(es) found.
```

表 4-1 コマンド出力

フィールド	説明
VLAN ID	MACアドレスエントリが所属する出力インタフェースのVLAN IDです。
State	MACアドレスエントリの状態です。 ● **Static**—スタティックMACアドレスエントリです。 ● **Learned**—ダイナミックMACアドレスエントリです。ダイナミックエントリは自動あるいは手動で設定されたものがあります。 ● **Blackhole**—ブラックホールMACアドレスエントリです。 ● **Multiport**—マルチポートユニキャストMACアドレスエントリです。
Port/NickName	MACアドレスに関連づけられるパケットの出力インタフェースです。ブラックホールMACアドレスエントリの場合、**N/A**と表示されます。

フィールド	説明
Aging	エントリがエージングアウト可能かどうかを示します。 • **Y**—エントリはエージングアウト可能です。 • **N**—エントリはエージングアウトできません。但しMAC認証によるエントリは例外です。
mac address(es) found	MACアドレスエントリに一致する数です。

関連コマンド

- **mac-address**
- **mac-address timer**

4.1.2 display mac-address aging-time

Syntax

display mac-address aging-time

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display mac-address aging-time コマンドはダイナミック MAC アドレスエントリのエージングタイマを表示します。

例

ダイナミック MAC アドレスエントリのエージングタイマを表示します。

<Switch> display mac-address aging-time

```
MAC address aging time: 300s.
```

関連コマンド

mac-address timer

4.1.3 display mac-address hash-bucket-size

Syntax

display mac-address hash-bucket-size

View

すべての view

定義済みユーザロール

network-admin

説明

display mac-address hash-bucket-size コマンドは MAC アドレステーブルのハッシュバケットサイズを表示します。

例

MAC アドレステーブルのハッシュバケットサイズを表示します。

<Switch> display mac-address hash-bucket-size

```
Hash-bucket-size in use: 4
Hash-bucket-size at the next reboot: 8
```

表 4-2 コマンド出力

フィールド	説明
Hash-bucket-size in use	現在のハッシュバケットサイズです。
Hash-bucket-size at the next reboot	次回の起動時に適用されるハッシュバケットサイズです。

関連コマンド

mac-address hash-bucket-size

4.1.4 display mac-address mac-learning

Syntax

display mac-address mac-learning [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: インタフェースのタイプと番号を指定します。

インタフェースを指定しない場合、グローバル MAC アドレスの学習状態とすべてのインタフェースの MAC アドレスの学習状態を表示します。

説明

display mac-address mac-learning コマンドはグローバル MAC アドレスの学習状態と指定された、あるいはすべてのインタフェースの MAC アドレスの学習状態を表示します。

例

グローバル MAC アドレスの学習状態とすべてのインタフェースの MAC アドレスの学習状態を表示します。

<Switch> display mac-address mac-learning

```
Global MAC address learning status: Enabled.

Port                    Learning Status
GE1/0/1                  Enabled
GE1/0/2                  Enabled
```

表 4-3 コマンド出力

フィールド	説明
Global MAC address learning status	グローバルMACアドレスの学習状態です。 • 有効です。 • 無効です。
Learning Status	インタフェースのMACアドレスの学習状態を表示します。 • 有効です。 • 無効です。

関連コマンド

mac-address mac-learning enable

4.1.5 display mac-address mac-move

Syntax

display mac-address mac-move [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

slot *slot-number*: IRF スタックのメンバ装置を ID で指定します。メンバ装置を指定しない場合、すべての IRF スタックメンバ装置の MAC アドレスの移動記録を表示します。

説明

display mac-address mac-move コマンドは装置が起動した後、MAC アドレスの移動記録を表示します。

指定された 2 つのインタフェース間で MAC アドレスの移動が発生したとき、ネットワークでレイヤ 2 でのループが発生する可能性があります。ループを検出し、位置を特定するために MAC アドレスの移動記録を表示することができます。

MAC アドレスの移動記録では、同一 MAC アドレス、VLAN、送信元ポート、現在のポートの記録が 1 つの記録として認識されます。

IRF スタックメンバ装置は 200 の MAC アドレスの移動記録を保存することができます。

例

IRF スタックメンバ装置 1 の MAC アドレスの移動記録を表示します。

<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  ---
```

すべての IRF スタックメンバ装置の MAC アドレスの移動記録を表示します。

<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  ---
```

表 4-4 コマンド出力

フィールド	説明
VLAN	MACアドレスエントリが属している出力インタフェースのVLANです。
Current port	MACアドレスが移動したインタフェースです。
Source port	MACアドレスが移動する前のインタフェースです。
Last time	最後にMACアドレスが移動したときの時間です。
Times	装置が起動したのち、MACアドレスが移動した数です。 新しいMACアドレスの移動が、MACアドレスの記録として、同じMACアドレス、VLAN、現在のポート、送信元ポートのフィールドを持っていたとき、MACアドレスを記録するため、MACアドレスの移動した数は1つずつ増加します。

関連コマンド

mac-address notification mac-move

4.1.6 display mac-address statistics

Syntax

display mac-address statistics

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display mac-address statistics コマンドは MAC アドレステーブルの統計情報を表示します。

このコマンドはタイプごとの MAC アドレスエントリ数と各タイプの最大 MAC アドレスエントリ数を表示します。

例

MAC アドレステーブルの統計情報を表示します。

<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:                        16384
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
```

表 4-5 コマンド出力

フィールド	説明
Dynamic Unicast Address (Learned) Count	パケットによって発生したダイナミックユニキャストMACアドレスエントリ数です。
Dynamic Unicast Address (Security-service-defined) Count	セキュリティサービスによって発生したダイナミックユニキャストMACアドレスエントリ数です。
Static Unicast Address (User-defined) Count	ユーザによって追加されたスタティックユニキャストMACアドレスエントリ数です。
Static Unicast Address (System-defined) Count	システムによって追加されたスタティックユニキャストMACアドレスエントリ数です。
Total Unicast MAC Addresses In Use	ユニキャストMACアドレスエントリ数です。
Total Unicast MAC Addresses Available	ユニキャストMACアドレスエントリの最大数です。
Multicast and Multiport MAC Address Count	マルチキャストとマルチポートユニキャストMACアドレスエントリ数です。
Static Multicast and Multiport MAC Address (User-defined) Count	ユーザによって追加されたスタティックマルチキャストとマルチポートユニキャストMACアドレスエントリ数です。
Total Multicast and Multiport MAC Addresses Available	マルチキャストとマルチポートユニキャストMACアドレスエントリの最大数です。

4.1.7 mac-address (interface view)

Syntax

mac-address { **dynamic** | **multiport** | **static** } *mac-address* **vlan** *vlan-id*

undo mac-address { **dynamic** | **multiport** | **static** } *mac-address* **vlan** *vlan-id*

デフォルト

設定なし

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

dynamic: ダイナミック MAC アドレスエントリを指定します。

static: スタティック MAC アドレスエントリを指定します。

multiport:マルチポートユニキャスト MAC アドレスエントリを指定します。宛先 MAC アドレスがマルチポートユニキャスト MAC アドレスエントリと一致するフレームは、複数のポートから送信されます。

mac-address: MAC アドレスを指定します。マルチキャスト MAC アドレスとすべてが 0 の MAC アドレスを除きます。形式は H-H-H です。H の先頭から 0 が続く場合は省略できます。たとえば、000f-00e2-0001 は、f-e2-1 と省略できます。

vlan *vlan-id*: 指定されたインタフェースが所属する既存の VLAN ID を指定します。設定範囲は 1～4094 です。

説明

mac-address コマンドはインタフェースの MAC アドレスエントリを追加あるいは修正します。

undo mac-address コマンドはインタフェースの MAC アドレスエントリを削除します。

一般的に、装置は自動で各インタフェースの受信フレームの送信元 MAC アドレスによって学習された MAC アドレステーブルを構築します。しかし、手動でスタティック MAC アドレスエントリを設定することができます。手動で設定されたスタティック MAC アドレスエントリはダイナミック MAC アドレスエントリよりも優先されます。インタフェースに接続されたユーザの装置のセキュリティを向上するため、ユーザの装置をインタフェースに関連づけるため、スタティックエントリを設定します。ユーザの装置（たとえばホスト A）のフレームは常にインタフェースから送信されます。ホスト A の偽の MAC アドレスを使用するほかのホストはホスト A からのフレームを取得することができません。

MAC アドレスエントリの設定は、設定を保存しないと、再起動により削除されます。ただしダイナミック MAC アドレスエントリは設定の保存に関わらず、再起動により削除されます。

例

VLAN 2 に所属する GigabitEthernet 1/0/1 に MAC アドレス 000f-e201-0101 のスタティック MAC アドレスエントリを追加します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] mac-address static 000f-e201-0101 vlan 2

VLAN 1 に所属するアグリゲートインタフェース Bridge-Aggregation 1 に MAC アドレス 000f-e201-0101 のスタティック MAC アドレスエントリを追加します。

<Switch> system-view

[Switch] interface bridge-aggregation 1

[Switch-Bridge-Aggregation1] mac-address static 000f-e201-0102 vlan 1

VLAN2 に属する GigabitEthernet1 / 0/1 および GigabitEthernet1 / 0/2 の MAC アドレス 0001-0001-0101 のマルチポートユニキャスト MAC アドレスエントリを追加します。

<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

関連コマンド

- **display mac-address**
- **mac-address (system view)**

4.1.8 mac-address (system view)

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*]

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

dynamic: ダイナミック MAC アドレスエントリを指定します。

static: スタティック MAC アドレスエントリを指定します。

blackhole: ブラックホール MAC アドレスエントリを指定します。パケットの送信元 MAC アドレスあるいは宛先 MAC アドレスがブラックホール MAC アドレスに一致している場合、パケットは廃棄されます。

multiport:マルチポートユニキャスト MAC アドレスエントリを指定します。宛先 MAC アドレスがマルチポートユニキャスト MAC アドレスエントリと一致するフレームは、複数のポートから送信されます。

mac-address: MAC アドレスを指定します。マルチキャスト MAC アドレスとすべてが 0 の MAC アドレスを除きます。形式は H-H-H です。H の先頭から 0 が続く場合は省略できます。たとえば、000f-00e2-0001 は、f-e2-1 と省略できます。

vlan *vlan-id*: 指定されたインタフェースが所属する既存の VLAN ID を指定します。設定範囲は 1～4094 です。

interface *interface-type interface-number*: 出力インタフェースのタイプと番号を指定します。

interface *interface-list*: インタフェースの範囲を指定します。形式は{ *interface-type interface-number1* [**to** *interface-type interface-number2*] } &<1-4>です。*interface-type interface-number* はインタフェースのタイプと番号を指定します。インタフェースは Ethernet インタフェースあるいはアグリゲートインタフェースのみ指定することができます。*interface-number2* は *interface-number1* より大きい値にする必要があります。はインタフェースあるいはインタフェースの範囲を最大 4 つまで設定できることを示します。

説明

mac-address コマンドは MAC アドレスエントリを追加あるいは修正します。

undo mac-address コマンドは 1 つあるいはすべての MAC アドレスエントリを削除します。

以下のタイプの MAC アドレスエントリを設定することができます。

- ダイナミックエントリ
  ダイナミックエントリは手動で設定されたダイナミックエントリと自動で学習されたダイナミックエントリが含まれます。
- スタティックエントリ

手動で設定されたスタティックエントリはダイナミックエントリよりも優先します。インタフェースに接続された装置のセキュリティを向上するため、インタフェースに割り当てる装置のスタティックエントリを手動で設定します。装置宛て（たとえば、Host A）のフレームは常にインタフェースに送信されます。Host A の MAC アドレスに偽造させた MAC アドレスを使用するほかのホストは Host A 宛てのフレームを受信することができません。

- ブラックホールエントリ
  指定された送信元 MAC アドレスあるいは宛先 MAC アドレスのフレームを廃棄するため、ブラックホールエントリを設定することができます。
- マルチポートユニキャストエントリ
  特定の宛先 MAC アドレスを持つフレームを複数のポートから送信するには、マルチポートユニキャストエントリを設定します。このコマンドを初めて実行する場合は、エントリが追加されます。同じ MAC アドレスと VLAN を使用し、インタフェースが異なるコマンドを再実行すると、このコマンドはこのエントリに指定されたインタフェースを追加します。

スタティックあるいはブラックホール MAC アドレスエントリはダイナミック MAC アドレスエントリに上書きすることができます。ダイナミック MAC アドレスエントリはスタティックあるいはブラックホール MAC アドレスエントリに上書きすることはできません。

パラメータを指定しないで **undo mac-address** コマンドを実行した場合、すべてのユニキャスト MAC アドレスエントリとスタティックマルチキャスト MAC アドレスエントリを削除します。

指定した VLAN のすべての MAC アドレスエントリ（ユニキャスト MAC アドレスエントリとスタティックマルチキャスト MAC アドレスエントリを含みます）を削除することができます。また特定のタイプ（ダイナミック、スタティック、ブラックホール、またはマルチポートユニキャスト）の MAC アドレスエントリのみを削除することができます。1 つのインタフェースのみを選択することで、スタティックマルチキャスト MAC アドレスエントリではなく、対応するユニキャスト MAC アドレスエントリを削除します。

MAC アドレスエントリの設定は、設定を保存しないと、再起動により削除されます。ただしダイナミック MAC アドレスエントリは設定の保存に関わらず、再起動により削除されます。

例

MAC アドレス 000f-e201-0101 のスタティックエントリを追加します。MAC アドレスに関連づけられたすべてのフレームは VLAN 2 に所属する GigabitEthernet 1/0/1 から送信します。

<Switch> system-view

[Switch] mac-address static 000f-e201-0101 interface gigabitethernet 1/0/1 vlan 2

MAC アドレス 000f-e201-0101 のマルチポートユニキャスト MAC アドレスエントリを追加します。MAC アドレスに関連づけられたすべてのフレームが、VLAN2 に所属する GigabitEthernet1 / 0/1 から GigabitEthernet1 / 0/3 を介して送信されます。

<Switch> system-view

[Switch] mac-address multiport 000f-e201-0101 interface gigabitethernet 1/0/1 to gigabitethernet 1/0/3 vlan 2

関連コマンド

- **display mac-address**
- **mac-address (interface view)**

4.1.9 mac-address hash-bucket-size

Syntax

mac-address hash-bucket-size *size*

undo mac-address hash-bucket-size

デフォルト

4

View

System view

定義済みユーザロール

network-admin

パラメータ

size: ハッシュバケットサイズを指定します。設定可能な値は 4、8 です。

説明

mac-address hash-bucket-size コマンドは MAC アドレステーブルのハッシュバケットサイズを設定します。

undo mac-address hash-bucket-size コマンドはデフォルトに戻します。

装置はハッシュチェーンを通じて MAC アドレステーブルを保存します。複数の MAC アドレスがハッシュによって同じハッシュキーを取得する場合、MAC アドレスハッシュの競合が発生し、装置はこれらの MAC アドレスの一部を学習できません。装置は、未知の MAC アドレス宛てにトラフィックをブロードキャストします。この MAC アドレスは、帯域幅とリソースを消費します。

MAC アドレステーブルのハッシュバケットサイズを大きくすると、MAC アドレスハッシュの競合を減らすことができます。ハッシュバケットサイズが大きいほど、より多くのシステムリソースが必要になります。システムリソースに応じて、ハッシュバケットのサイズを適切に設定してください。

設定されたハッシュバケットサイズは、次回の起動時に有効になります。

例

MAC アドレステーブルのハッシュバケットサイズを 8 に設定します。

<Switch> system-view

[Switch] mac-address hash-bucket-size 8

```
The configuration will take effect at the next reboot. Continue? [Y/N]:y
Reboot device to make the configuration take effect.
```

関連コマンド

display mac-address hash-bucket-size

4.1.10 mac-address mac-learning enable

Syntax

mac-address mac-learning enable

undo mac-address mac-learning enable

デフォルト

有効

View

System view

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

VLAN view

定義済みユーザロール

network-admin

説明

mac-address mac-learning enable コマンドはグローバル、インタフェース、VLAN で MAC アドレスの学習を有効にします。

undo mac-address mac-learning enable コマンドはグローバル、インタフェース、VLAN で MAC アドレスの学習を無効にします。

MAC アドレステーブルが一杯になることを防ぐため、MAC アドレステーブルの学習を無効にすることができます。

たとえば、攻撃者からの異なる送信元 MAC アドレスの大量のパケットを学習しないように、以下のガイドラインに従い、装置で MAC アドレスの学習を無効にすることができます。

- インタフェースごとに MAC アドレスの学習を無効にすることができます。グローバルで MAC アドレスの学習を無効にした場合、すべてのインタフェースで MAC アドレスの学習が無効になります。装置は MAC アドレスの学習を停止し、ダイナミックに MAC アドレステーブルのアップデートを行うことができません。
- MAC アドレスの学習を無効にすると、ブロードキャストストームが発生する可能性あるため、インタフェースで MAC アドレスの学習を無効にしたのち、ブロードキャストストームの抑制を行ってください。ブロードキャストストームの抑制の詳細は、オペレーションマニュアルのセクション 3 *アクセス* “*Ethernet インタフェース*” を参照してください。
- グローバルで MAC アドレスの学習を有効にし、インタフェースあるいは VLAN で MAC アドレスの学習を無効にすることができます。
- MAC アドレスの学習を無効にしたとき、装置はインタフェースにある既存のダイナミック MAC アドレスエントリを即座に削除します。

例

グローバルで MAC アドレスの学習を無効にします。

<Switch> system-view

[Switch] undo mac-address mac-learning enable

VLAN 10 で MAC アドレスの学習を無効にします。

<Switch> system-view

[Switch] vlan 10

[Switch-vlan10] undo mac-address mac-learning enable

GigabitEthernet 1/0/1 で MAC アドレスの学習を無効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] undo mac-address mac-learning enable

アグリゲートインタフェース Bridge-Aggregation 1 で MAC アドレスの学習を無効にします。

<Switch> system-view

[Switch] interface bridge-aggregation 1

[Switch-Bridge-Aggregation1] undo mac-address mac-learning enable

関連コマンド

display mac-address mac-learning

4.1.11 mac-address mac-move fast-update

Syntax

mac-address mac-move fast-update

undo mac-address mac-move fast-update

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

mac-address mac-move fast-update コマンドは MAC アドレスの移動による ARP クイックアップデートを有効にします。

undo mac-address mac-move fast-update コマンドはデフォルトに戻します。

例

MAC アドレスの移動による ARP クイックアップデートを有効にします。

<Switch> system-view

[Switch] mac-address mac-move fast-update

4.1.12 mac-address mac-roaming enable

Syntax

mac-address mac-roaming enable

undo mac-address mac-roaming enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

mac-address mac-roaming enable コマンドは MAC アドレスの同期化（ローミング）を有効にします。

undo mac-address mac-roaming enable コマンドはデフォルトに戻します。

異なる IRF スタックメンバ装置のポートが、同じアグリゲーショングループの Selected ポートである場合、MAC アドレスエントリは IRF スタックメンバ装置間で MAC アドレスの同期化を行います。同期化を行うことで MAC アドレスのアドレスローミングを行います。IRF スタックユニットで MAC アドレスの同期化が有効かどうかにかかわらず、MAC アドレスの同期化を行います。アグリゲーショングループの詳細は、オペレーションマニュアルのセクション 3 *アクセス“リンクアグリゲーション”*を参照してください。

MAC アドレステーブルのサイズは IRF スタックメンバ装置によって異なります。MAC アドレスの同期化が有効である場合、IRF スタックメンバ装置の MAC アドレスのテーブルサイズが超過すると、MAC アドレステーブルの同期化は行うことができません。

例

MAC アドレスの同期化を有効にします。

<Switch> system-view

[Switch] mac-address mac-roaming enable

4.1.13 mac-address max-mac-count

Syntax

mac-address max-mac-count *count*

undo mac-address max-mac-count

デフォルト

設定なし

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

count: インタフェースで学習できる MAC アドレスの最大数を指定します。設定範囲は 0～4096 です。0 が指定された場合、インタフェースで MAC アドレスの学習が行われません。

説明

mac-address max-mac-count コマンドはインタフェースで学習できる MAC アドレスの最大数を設定します。

undo mac-address max-mac-count コマンドはデフォルトに戻します。

mac-address max-mac-count コマンドは MAC アドレステーブルのサイズを制限するため、MAC アドレスエントリ数を制限します。

MAC アドレステーブルが大きくなるとフォワーディングの性能に影響します。インタフェースで学習した MAC アドレスの数が上限に達した場合、インタフェースは MAC アドレスエントリの学習を停止します。

例

GigabitEthernet 1/0/1 で学習できる MAC アドレスエントリの最大数を 600 に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] mac-address max-mac-count 600

関連コマンド

mac-address

4.1.14 mac-address max-mac-count enable-forwarding

Syntax

mac-address max-mac-count enable-forwarding

undo mac-address max-mac-count enable-forwarding

デフォルト

有効

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

説明

mac-address max-mac-count enable-forwarding コマンドはインタフェースで学習できる MAC アドレスの数が制限に到達したのち、インタフェースで受信された未知のフレームを装置が転送することを有効にします。

undo mac-address max-mac-count enable-forwarding コマンドはインタフェースで学習できる MAC アドレスの数が制限に到達したのち、インタフェースで受信された未知のフレームを装置が転送することを無効にします。

例

MAC アドレスエントリを最大 600 まで学習できるように GigabitEthernet 1/0/1 を設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] mac-address max-mac-count 600

GigabitEthernet 1/0/1 で学習できる MAC アドレスの数が制限に到達したのち、GigabitEthernet 1/0/1 で受信された未知のフレームを装置が転送することを無効にします。

[Switch-GigabitEthernet1/0/1] undo mac-address max-mac-count enable-forwarding

関連コマンド

- **mac-address**
- **mac-address max-mac-count**

4.1.15 mac-address notification mac-move

Syntax

mac-address notification mac-move [**interval** *interval-value*]

undo mac-address notification mac-move

デフォルト

MAC アドレスの検出は無効です。MAC アドレスの移動の検出間隔は 1 分です。

View

System view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: MAC アドレスの移動の検出間隔を指定します。設定範囲は 1～60 分です。パラメータを指定しない場合、デフォルトで 1 分が指定されます。

説明

mac-address notification mac-move コマンドは MAC アドレスの移動を通知することを有効にし、MAC アドレスの検出間隔を指定します。

undo mac-address notification mac-move コマンドは MAC アドレスの移動を通知することを無効にします。

MAC アドレスの移動の通知を有効にした際、システムが MAC アドレスの移動を検出したとき、MAC アドレスが移動したログを表示します。各 MAC アドレスの移動ログは以下の情報が含まれます。

- MAC アドレス
- MAC アドレスエントリの VLAN ID
- MAC アドレスの移動元のポートと移動先のポート
- MAC アドレスの検出間隔以内に MAC アドレスが移動した数

MAC アドレスは 1 つの MAC アドレスの移動記録のみ保持することができます。1 つの MAC アドレスを複数回移動した場合、最新の移動記録のみ保持します。

検出間隔以内に、IRF スタックメンバ装置は最大 20 の MAC アドレスの移動を記録することができます。

記録は MAC アドレス移動カウントの下降順にランク付けされます。新しい記録の MAC アドレスの移動カウントが既存の記録の MAC 移動カウント数より高い場合、装置は以下の処理を行います。

- もっとも低い MAC アドレス移動カウントの記録を廃棄します。
- MAC アドレス移動記録を、MAC アドレス移動カウントの下降順にランク付けます。

そして次の検出間隔で、装置は以前の検出間隔内に作成されたすべての MAC アドレス移動記録を廃棄し、別の MAC アドレス移動記録の収集を開始します。

このコマンドを実行した後、システムは Information Center に syslog メッセージのみを送信します。**snmp-agent trap enable mac-address** コマンドが有効である場合、装置の SNMP モジュールに SNMP 情報を送信します。

例

MAC アドレスの移動を通知することを有効にします。

<Switch> system-view

[Switch] mac-address notification mac-move

[Switch]

```
%May 14 17:16:45:688 2013 MAC/4/MAC_NOTIFICATION: MAC address 0000-0012-0034 in
VLAN 500 has moved from port GE1/0/1 to port GE1/0/2 for 1 times
```

出力は以下のこと示します。

- MAC アドレス 0000-0012-0034 の VLAN ID は 500 です。
- MAC アドレスは GigabitEthernet 1/0/1 から GigabitEthernet 1/0/2 に移動しました。
- MAC アドレスは最新の 1 分以内に 1 回移動しました。

関連コマンド

display mac-address mac-move

4.1.16 mac-address notification mac-move suppression (interface view)

Syntax

mac-address notification mac-move suppression

undo mac-address notification mac-move suppression

デフォルト

無効

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

mac-address notification mac-move suppression コマンドは MAC アドレスの移動の抑制機能を有効にします。

undo mac-address notification mac-move suppression コマンドはデフォルトに戻します。

説明

MAC アドレスの検出期間以内に、指定した抑制しきい値より多くの MAC アドレスがインタフェースから移動したとき、インタフェースをシャットダウンします。インタフェースを UP 状態にする場合、手動で **shutdown** コマンドを実行し、**undo shutdown** コマンドを実行する必要があります。抑制間隔後、インタフェースは自動で UP 状態となります。

MAC アドレスの移動の抑制機能がインタフェースをシャットダウンするとき、システムは Information Center モジュールに syslog メッセージのみを送信します。**snmp-agent trap enable mac-address** コマンドが有効である場合、装置の SNMP モジュールに SNMP 情報を送信します。

例

GigabitEthernet 1/0/1 で MAC アドレスの移動の抑制機能を有効にします。

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] mac-address notification mac-move suppression

関連コマンド

mac-address notification mac-move suppression (system view)

4.1.17 mac-address notification mac-move suppression (system view)

Syntax

mac-address notification mac-move suppression { **interval** *interval* | **threshold** *threshold* }

undo mac-address notification mac-move suppression { **interval** | **threshold** }

デフォルト

MAC アドレスの抑制間隔は 30 秒です。MAC アドレスのしきい値は 3 です。

View

System view

定義済みユーザロール

network-admin

パラメータ

interval *interval*: MAC アドレスの抑制間隔を指定します。設定範囲は 30～86400 秒です。パラメータを指定しない場合、30 秒が指定されます。

threshold *threshold*: 検出間隔内に送信元のインタフェースから移動する MAC アドレスのしきい値を設定します。設定範囲は 0～1024 です。パラメータを指定しない場合、3 が指定されます。

説明

mac-address notification mac-move suppression コマンドは MAC アドレスの抑制間隔、あるいは MAC アドレス移動のしきい値を設定します。

undo mac-address notification mac-move suppression コマンドはデフォルトに戻します。

インタフェースでコマンドを適用する場合、MAC アドレスの移動の抑制機能を有効にする必要があります。

MAC アドレスの抑制間隔あるいは MAC アドレスのしきい値を複数回設定した場合、最後に行った設定が適用されます。抑制間隔の設定は MAC アドレス移動のしきい値の設定と独立しています。

例

MAC アドレスの抑制間隔を 40 秒に設定し、MAC アドレス移動のしきい値を 1 に設定します。

<Switch> system-view

[Switch] mac-address notification mac-move suppression interval 40

[Switch] mac-address notification mac-move suppression threshold 1

関連コマンド

mac-address notification mac-move suppression (interface view)

4.1.18 mac-address timer

Syntax

mac-address timer { **aging** *seconds* | **no-aging** }

undo mac-address timer

デフォルト

300 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

aging *seconds*: ダイナミック MAC アドレスエントリのエージングタイマを設定します。設定範囲は 10～100000 秒です。

no-aging: ダイナミック MAC アドレスエントリをエージアウトしないように設定します。

説明

mac-address timer コマンドはダイナミック MAC アドレスエントリのエージングタイマを設定します。

undo mac-address timer コマンドはデフォルトに戻します。

適切にエージングタイマを設定するために、以下のガイドラインに従ってください。

- エージング間隔が長いと、エージング時間が終了したエントリを MAC アドレステーブルに残す可能性があり、最新のネットワークの変化に対応できなくなる可能性があります。
- エージング間隔が短いと、有効なエントリを削除してしまい、装置のパフォーマンスに影響を及ぼす不要なブロードキャストを送信する結果になる可能性があります。

例

ダイナミック MAC アドレスエントリのエージングタイマを 500 秒に設定します。

<Switch> system-view

[Switch] mac-address timer aging 500

関連コマンド

display mac-address aging-time

4.1.19 mac-learn-mode

Syntax

mac-learn-mode { **hardware** | **software** }

undo mac-learn-mode

デフォルト

ソフトウェア学習モード

View

System view

定義済みユーザロール

network-admin

パラメータ

hardware: MAC アドレスの学習モードをハードウェアに設定します。

software: MAC アドレスの学習モードをソフトウェアに設定します。

説明

mac-learn-mode hardware コマンドは、MAC アドレスの学習モードをハードウェアに設定します。

mac-learn-mode software コマンドは、MAC アドレスの学習モードをソフトウェアに設定します。

undo mac-learn-mode コマンドは、MAC アドレスの学習モードをデフォルトに戻します。

例

MAC アドレスの学習モードをハードウェアに変更します。

<Switch> system-view

[Switch] mac-learn-mode hardware

注意:

- 学習モードを変更した場合は装置を再起動してください。
- MAC アドレスの学習モードを”hardware”モードに設定した場合、すべてのインタフェースで MAC アドレスの学習モードが”hardware モードになります。
- MAC アドレスの学習モードを”hardware”モードに設定しても、802.1X 認証機能、または **mac-address max-mac-count** 設定を行ったポートでは、内部的に”software”モードでの動作となる為、ワイヤーレートでの MAC アドレス学習はできません。
- データがバースト転送される環境において、ハードウェアモードを使用している装置で **undo mac-address** コマンドを実行すると、**display mac-address** に表示される MAC アドレス情報が実際に学習されている MAC アドレスと異なる結果となる場合があります。本仕様によるパケット転送への影響はありません。この状態を復旧する場合は、データ転送が少なくなった状況で再度 **undo mac-address** を実行してください。

4.1.20 snmp-agent trap enable mac-address

Syntax

snmp-agent trap enable mac-address

undo snmp-agent trap enable mac-address

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

snmp-agent trap enable mac-address コマンドは MAC アドレステーブルの SNMP notification の送信を有効にします。

undo snmp-agent trap enable mac-address コマンドは MAC アドレステーブルの SNMP notification の送信を無効にします。

NMS に重大な MAC アドレスの移動を通知するため、MAC アドレステーブルの SNMP notification の送信を有効にします。正しく MAC アドレス移動の通知を行うため、装置で SNMP を設定する必要があります。

MAC アドレステーブルの SNMP notification の送信が無効であるとき、MAC アドレスが移動した場合、information center モジュールに作成されたログメッセージを通知します。ログメッセージを表示する場合、information center でログの宛先と出力ルールを設定します。

SNMP と information center の詳細は、オペレーションマニュアルのセクション 11 *システム管理* “*SNMP*”、“*Information Center*”を参照してください。

MAC アドレステーブルは、MAC アドレスの移動に関する SNMP notification の送信のみをサポートします。

MAC アドレスの移動に関する SNMP notification の送信が有効であるとき、MAC アドレステーブルの SNMP notification のすべてのタイプを有効にします。MAC アドレスの移動に関する SNMP notification の送信が無効であるとき、MAC アドレステーブルの SNMP notification のすべてのタイプを無効にします。

例

MAC アドレステーブルで MAC アドレスが移動した場合 SNMP notification の送信を無効にします。

<Switch> system-view

[Switch] undo snmp-agent trap enable mac-address mac-move

関連コマンド

mac-address notification mac-move

目次

このセクションのページは **3-x-x** です。

5 章 MAC Information 5-1
5.1 MAC Information 設定コマンド 5-1
5.1.1 mac-address information enable (interface view) 5-1
5.1.2 mac-address information enable (system view) 5-2
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 5-4

5章 MAC Information

5.1 MAC Information設定コマンド

5.1.1 mac-address information enable (interface view)

Syntax

mac-address information enable { **added** | **deleted** }

undo mac-address information enable { **added** | **deleted** }

デフォルト

無効

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

added: インタフェースで新しい MAC アドレスが学習されたとき、装置が MAC アドレスの変更情報を記録することを有効にします。

deleted: 既存の MAC アドレスが削除されたとき、装置が MAC アドレスの変更情報を記録することを有効にします。

説明

mac-address information enable コマンドは MAC Information 機能をインタフェースで有効にします。

undo mac-address information enable コマンドは MAC Information 機能をインタフェースで無効にします。

インタフェースで MAC Information 機能を有効にするまえに、グローバルで MAC Information 機能を有効にしてください。

例

新しい MAC アドレスを学習したとき、MAC アドレスの変更情報を記録するため、GigabitEthernet 1/0/1 で MAC Information 機能を有効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] mac-address information enable added

関連コマンド

mac-address information enable (system view)

5.1.2 mac-address information enable (system view)

Syntax

mac-address information enable

undo mac-address information enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

mac-address information enable コマンドは MAC Information 機能をグローバルで有効にします。

undo mac-address information enable コマンドは MAC Information 機能をグローバルで無効にします。

インタフェースで MAC Information 機能を有効にするまえに、グローバルで MAC Information 機能を有効にしてください。

例

MAC Information 機能をグローバルで有効にします。

<Switch> system-view

[Switch] mac-address information enable

関連コマンド

mac-address information enable (interface view)

5.1.3 mac-address information interval

Syntax

mac-address information interval *interval*

undo mac-address information interval

デフォルト

1 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

interval: SNMP notification メッセージで MAC アドレスの変更を通知する送信間隔を指定します。設定範囲は 1～20000 秒です。

説明

mac-address information interval コマンドは Syslog あるいは SNMP トラップメッセージで MAC アドレスの変更を通知する送信間隔を指定します。

undo mac-address information interval コマンドはデフォルトに戻します。

Syslog あるいは SNMP トラップメッセージが頻繁に送信されることがないように、通知する送信間隔を長い値にしてください。

例

Syslog あるいは SNMP トラップメッセージで MAC アドレスの変更を通知する送信間隔を 200 秒に設定します。

<Switch> system-view

[Switch] mac-address information interval 200

5.1.4 mac-address information mode

Syntax

mac-address information mode { **syslog** | **trap** }

undo mac-address information mode

デフォルト

trap

View

System view

定義済みユーザロール

network-admin

パラメータ

syslog: MAC アドレスの変更を Syslog で通知するように指定します。

trap: MAC アドレスの変更を SNMP トラップメッセージで通知するように指定します。

説明

mac-address information mode コマンドは MAC Information のモードを設定します。MAC Information のモードは、MAC アドレスの変更を通知するメッセージのタイプ（Syslog あるいは SNMP トラップメッセージ）を指定します。

undo mac-address information mode コマンドはデフォルトに戻します。

例

MAC Information のモードを SNMP トラップメッセージに設定します。

<Switch> system-view

[Switch] mac-address information mode trap

5.1.5 mac-address information queue-length

Syntax

mac-address information queue-length *value*

undo mac-address information queue-length

デフォルト

50

View

System view

定義済みユーザロール

network-admin

パラメータ

value: MAC Information のキューの長さを指定します。設定範囲は 0～1000 です。MAC Information のキュー長は、MAC アドレスの変更メッセージの数を示します。

説明

mac-address information queue-length コマンドは MAC アドレスの変更を記録する MAC Information のキューの長さを指定します。

undo mac-address information queue-length コマンドはデフォルトに戻します。

MAC Information のキューの長さが 0 である場合、装置は MAC アドレスが学習あるいは削除されたのち、すぐに Syslog メッセージあるいは SNMP トラップメッセージを送信します。

MAC Information のキューの長さが 0 でない場合、キューの MAC アドレスの変更を記録します。

- 以下の状況のとき、装置は最新の MAC アドレスの変更をもっとも古い MAC アドレスの変更に上書きします。
  - □ MAC アドレスの変更を通知する送信間隔が終了していません。
  - □ キューが一杯になりました。
- MAC アドレスの変更を通知する送信間隔が終了した場合、装置は Syslog メッセージあるいは SNMP トラップメッセージを送信します。

例

MAC アドレスの変更を記録する MAC Information のキューの長さを 600 に指定します。

<Switch> system-view

[Switch] mac-address information queue-length 600

目次

このセクションのページは **3-x-x** です。

6 章 リンクアグリゲーション 6-1
6.1 リンクアグリゲーション設定コマンド 6-1
6.1.1 description 6-1
6.1.2 display interface 6-2
6.1.3 display lacp system-id 6-6
6.1.4 display link-aggregation load-sharing mode 6-7
6.1.5 display link-aggregation member-port 6-9
6.1.6 display link-aggregation summary 6-12
6.1.7 display link-aggregation verbose 6-13
6.1.8 interface bridge-aggregation 6-17
6.1.9 lacp period short 6-18
6.1.10 lacp system-priority 6-19
6.1.11 link-aggregation global load-sharing mode 6-20
6.1.12 link-aggregation load-sharing mode local-first 6-21
6.1.13 link-aggregation mode 6-22
6.1.14 link-aggregation port-priority 6-23
6.1.15 link-aggregation selected-port maximum 6-23
6.1.16 link-aggregation selected-port minimum 6-25
6.1.17 port link-aggregation group 6-26
6.1.18 reset counters interface 6-27
6.1.19 reset lacp statistics 6-27
6.1.20 shutdown 6-28

6章 リンクアグリゲーション

6.1 リンクアグリゲーション設定コマンド

6.1.1 description

Syntax

description *text*

undo description

デフォルト

インタフェース名＋Interface です。（たとえばアグリゲートインタフェース Bridge-Aggregation1 のデフォルトは Bridge-Aggregation1 Interface です）

View

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

text: インタフェースの説明を指定します。設定範囲は 1～255 文字です。大文字、小文字を区別します。

説明

description コマンドはインタフェースの説明を設定します。

undo description コマンドはデフォルトに戻します。

例

アグリゲートインタフェース Bridge-Aggregation 1 の説明を connect to the lab に設定します。

<Switch> system-view

[Switch] interface bridge-aggregation 1

[Switch-Bridge-Aggregation1] description connect to the lab

6.1.2 display interface

Syntax

display interface [**bridge-aggregation** [*interface-number*]] [**brief** [**description** | **down**]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

bridge-aggregation: レイヤ 2 アグリゲートインタフェースを指定します。

interface-number: 既存のアグリゲートインタフェース番号を指定します。設定範囲は、すべての既存のアグリゲートインタフェース番号の範囲です。

brief: インタフェースの概要情報を表示します。指定されない場合、コマンドは詳細なインタフェース情報を表示します。

description: インタフェースの説明をすべて表示します。指定しない場合、インタフェースの説明の最初の 27 文字のみ表示します。

down: down 状態のインタフェースの情報と原因を表示します。指定しない場合、すべての状態のインタフェース情報を表示します。

説明

display interface コマンドはアグリゲートインタフェースの情報を表示します。

bridge-aggregation パラメータを指定しない場合、すべてのインタフェースの情報を表示します。

bridge-aggregation パラメータを指定し、インタフェース番号を指定しない場合、指定したタイプのすべてのアグリゲートインタフェースの情報を表示します。

bridge-aggregation パラメータとインタフェース番号を指定した場合、指定したアグリゲートインタフェースの情報を表示します。

例

レイヤ 2 アグリゲートインタフェース Bridge-Aggregation 1 の詳細情報を表示します。

<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
```

レイヤ 2 アグリゲートインタフェース Bridge-Aggregation 1 の概要情報を表示します。

<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
```

表 6-1 コマンド出力

フィールド	説明
Bridge-Aggregation1	レイヤ2アグリゲートインタフェース名です。

フィールド	説明
Current state	アグリゲートインタフェースの状態です。 ● **Administratively DOWN**–**shutdown**コマンドでインタフェースがシャットダウンしています。 ● **DOWN**–**shutdown**コマンドでシャットダウンしていませんが、物理的にdownしています。（イーサネットケーブルが物理的に接続されていない、あるいはリンクに失敗している可能性があります） ● **UP**–インタフェースが運用上も物理的にも起動している状態です。
IP packet frame type	IPv4パケットのフレームフォーマットです。
Description	インタフェースの説明です。
Bandwidth	インタフェースの予期された帯域幅です。帯域幅が0kbpsの場合、フィールドは表示されません。
Port priority	インタフェースのポートプライオリティです。
Output queue - Urgent queuing: Size/Length/Discards	緊急の出力キューの情報です。 ● **Size**—キューのパケット数です。 ● **Length**—キューに含めることができるパケットの最大数です。 ● **Discards**—廃棄したパケット数です。
Output queue - Protocol queuing: Size/Length/Discards	プロトコル出力キューの情報です。 ● **Size**—キューのパケット数です。 ● **Length**—キューに含めることができるパケットの最大数です。 ● **Discards**—廃棄したパケット数です。
Output queue - FIFO queuing: Size/Length/Discards	FIFO出力キューの情報です。 ● **Size**—キューのパケット数です。 ● **Length**—キューに含めることができるパケットの最大数です。 ● **Discards**—廃棄したパケット数です。
Unknown-speed mode, unknown-duplex mode	インタフェースの通信速度と通信モードが不明です。
Port link-type	インタフェースのリンクタイプです。 ● accessです。 ● trunkです。 ● hybridです。
Tagged VLANs	パケットがVLANタグをつけてインタフェースに送信されるVLANです。

フィールド	説明
Untagged VLANs	パケットがVLANタグなしでインタフェースに送信されるVLANです。
Last clearing of counters	インタフェースで**reset counters interface**コマンドを最後に使用してからの総時間です。 **Never**は装置が起動してから**reset counters interface**コマンドを一度も使用していないことを示します。
Last 300 seconds input/output rate	過去300秒以内の平均送受信のトラフィックレートです。
Input/Output (total)	インタフェースで送受信されたすべてのパケットの統計情報です。
Input/Output (normal)	インタフェースで送受信されたすべての正常なパケットの統計情報です。
Line protocol state	インタフェースのリンクレイヤの状態です。 ● UP ● DOWN
Maximum transmission unit	インタフェースのMTUです。
Internet protocol processing: Disabled	インタフェースにIPアドレスが設定されておらず、IPパケットを処理できません。
Internet address	インタフェースのIPアドレスを表示します。primaryはIPアドレスがプライマリIPアドレスであることを示します。
Brief information on interfaces in bridge mode	レイヤ2インタフェースの概要情報です。
Interface	省略したインタフェース名です。
Link	インタフェースの物理状態です。 ● **UP**—インタフェースが物理的にupしています。 ● **DOWN**—インタフェースが物理的にdownしています。 ● **ADM**— **shutdown**コマンドでインタフェースがシャットダウンしています。物理状態を回復する場合、**undo shutdown**コマンドを実行します。 ● **Stby**—インタフェースがバックアップインタフェースとして動作します。
Speed	インタフェースの通信速度です。単位はbpsです。 インタフェースが自動でネゴシエーションされる場合、(**a**)で示されたオートネゴシエーションのフラグが含まれます。インタフェースにオートネゴシエーションが設定されているがオートネゴシエーションが開始していない場合、**auto**と表示されます。

フィールド	説明
Duplex	インタフェースの通信モードです。 ● **A**—オートネゴシエーションです。インタフェースのオートネゴシエーションの通信モードがautoに設定されているがオートネゴシエーションが開始していません。 ● **F**—通信モードがfullです。 ● **F(a)**—通信モードがfullでオートネゴシエートされています。 ● **H**—通信モードがhalfです。 ● **H(a)**—通信モードがhalfでオートネゴシエートされています。
Type	インタフェースのリンクタイプです。 ● **A**－accessです。 ● **H**－hybridです。 ● **T**－trunkです。
Protocol	インタフェースのリンクレイヤの状態です。 ● **UP**－インタフェースのリンクがupです。 ● **DOWN**－インタフェースのリンクがdownです。 ● **UP(s)**—インタフェースのリンクがオンデマンドリンクあるいは準備ができていない状態です。ここで（**s**）はスプーフィングのフラグを示します。Nullインタフェース、ループバックインタフェースで表示されます。
Primary IP	インタフェースのプライマリIPアドレスです。ハイフン（**--**）はIPアドレスが設定されていないことを示します。
Cause	物理リンクがダウンした原因です。

6.1.3 display lacp system-id

Syntax

display lacp system-id

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display lacp system-id コマンドはローカルシステムのシステム ID を表示します。

ローカルシステムの LACP プライオリティを変更するために **lacp system-priority** コマンドを使用することができます。LACP プライオリティ値は 10 進数で指定しますが、**display lacp system-id** コマンドは、16 進数で表示されます。

例

ローカルシステムのシステム ID を表示します。

<Switch> display lacp system-id

```
Actor System ID: 0x8000, 0000-fc00-6504
```

表 6-2 コマンド出力

フィールド	説明
Actor System ID: 0x8000, 0000-fc00-6504	ローカルシステムIDです。LACPプライオリティ（例 0x8000）およびシステムのMACアドレス（例 0000-fc00-6504）で構成されます。

関連コマンド

lacp system-priority

6.1.4 display link-aggregation load-sharing mode

Syntax

display link-aggregation load-sharing mode [**interface** [**bridge-aggregation** *interface-number*]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

bridge-aggregation: レイヤ 2 アグリゲートインタフェースを指定します。

interface-number: 既存のアグリゲートインタフェース番号を指定します。

説明

display link-aggregation load-sharing mode コマンドはリンクアグリゲーションロードシェアリングモードを表示します。

interface パラメータを指定しない場合、グローバルのリンクアグリゲーションロードシェアリングモードを表示します。

interface パラメータを指定し、*interface-number* を指定しない場合、すべてのアグリゲーショングループのリンクアグリゲーションロードシェアリングモードを表示します。

bridge-aggregation パラメータは装置でアグリゲートインタフェースが存在するときのみ有効です。

例

デフォルトのグローバルのリンクアグリゲーションロードシェアリングモードを表示します。

<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
```

設定したグローバルのリンクアグリゲーションロードシェアリングモードを表示します。

<Switch> display link-aggregation load-sharing mode

```
Link-aggregation load-sharing mode:
destination-mac address, source-mac address
```

レイヤ 2 アグリゲートインタフェースに対応するアグリゲーショングループ 10 のデフォルトのリンクアグリゲーションロードシェアリングモードを表示します。

<Switch> display link-aggregation load-sharing mode interface bridge-aggregation 10

```
Bridge-Aggregation10 load-sharing mode:
Layer 2 traffic: packet type-based sharing
Layer 3 traffic: packet type-based sharing
```

レイヤ 2 アグリゲートインタフェースに対応するアグリゲーショングループ 10 の設定したリンクアグリゲーションロードシェアリングモードを表示します。

<Switch> display link-aggregation load-sharing mode interface bridge-aggregation 10

```
Bridge-Aggregation10 load-sharing mode:
destination-mac address, source-mac address
```

表 6-3 コマンド出力

フィールド	説明
Link-aggregation load-sharing mode	グローバルのリンクアグリゲーションのロードシェアリングモードを表示します。 デフォルトでは、レイヤ2、レイヤ3のリンクアグリゲーションのロードシェアリングモードが表示されます。 グローバルのロードシェアリングモードを設定した場合、設定されたモードが表示されます。
Bridge-Aggregation10 load-sharing mode	アグリゲートインタフェースBridge-Aggregation 10に対応するアグリゲーショングループのリンクアグリゲーションのロードシェアリングモードです。 デフォルトでは、グローバルのリンクアグリゲーションのロードシェアリングモードが表示されます。 特にこのアグリゲーショングループのリンクアグリゲーションのロードシェアリングモードを設定した場合、設定されたモードが表示されます。
Layer 2 traffic: packet type-based sharing	レイヤ2のデフォルトのロードシェアリングモードを示します。この出力のモードはパケットタイプです。
Layer 3 traffic: packet type-based sharing	レイヤ3のデフォルトのロードシェアリングモードを示します。この出力のモードはパケットタイプです。
destination-mac address, source-mac address	設定されたリンクアグリゲーションロードシェアリングモードを示します。この出力例では、トラフィックは送信元と宛先のMACアドレスにもとづいています。

6.1.5 display link-aggregation member-port

Syntax

display link-aggregation member-port [*interface-list*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface-list: リンクアグリゲーションメンバポートを指定します。形式は *interface-type interface-number1* [**to** *interface-type interface-number2*]です。*interface-number2* は *interface-number1* 以上の値にしてください。

説明

display link-aggregation member-port コマンドは指定されたメンバポートのリンクアグリゲーションの詳細情報を表示します。

スタティックアグリゲーショングループのメンバポートはピアグループの情報は知りません。スタティックのアグリゲーショングループは、ローカルインタフェースのポート番号、ポートプライオリティ、使用可能なキーのみ表示されます。

例

GigabitEthernet 1/0/1 のリンクアグリゲーションの詳細情報を表示します。そのポートは、スタティックのアグリゲーショングループのメンバポートです。

<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
```

GigabitEthernet 1/0/2 のリンクアグリゲーションの詳細情報を表示します。そのポートは、ダイナミックのアグリゲーショングループのメンバポートです。

<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)
```

表 6-4 コマンド出力

フィールド	説明
Flags	1バイトのLACPの状態フラグです。最下位から最上位のビットまで、以下のようにA～Hで表示されます。1が真、0が偽で示します。 ● **A**－LACPが有効か無効かを示します。1が有効、0が無効です。 ● **B**－LACPのタイムアウトの長さを示します。1がショートタイムアウト、0がロングタイムアウトです。 ● **C**－送信システムがこのリンクを集約可能とみなすかどうかを示します。1は可能、0が不可能です。 ● **D**－送信システムがこのリンクを同期しているとみなすかどうかを示します。1が同期している、0が同期していないです。 ● **E**－送信システムが、受信フレームをアグリゲートしているかどうかを示します。1がアグリゲートしている、0がアグリゲートしていないです。 ● **F**－送信システムが、送信フレームを分配しているかどうかを示します。1が分配している、0が分配していないです。 ● **G**－送信システムがデフォルトのフレームを受信するかどうかを示します。1が受信する、0が受信しないです。 ● **H**－送信システムが期限切れのフレームを受信するかどうかを示します。1が受信する、0が受信しないです。
Aggregate Interface	メンバポートが所属するアグリゲートインタフェースです。
Local	ローカルインタフェースの情報です。
Oper-key	操作キーです。
Flag	LACPプロトコル状態のフラグです。
Remote	ピアエンドの情報です。
System ID	ピアのシステムIDです。システムLACPプライオリティとシステムMACアドレスが含まれます。
Received LACP Packets	受信したLACPパケット数です。
Illegal	異常パケットの総数です。

フィールド	説明
Sent LACP Packets	送信したLACPパケット数です。

6.1.6 display link-aggregation summary

Syntax

display link-aggregation summary

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display link-aggregation summary コマンドはすべてのアグリゲーショングループの概要情報を表示します。

スタティックアグリゲーショングループのメンバポートはピアグループの情報は知りません。スタティックリンクアグリゲーションのパートナーID フィールドは、**None** と表示されるか、なにも表示されません。

例

すべてのアグリゲーショングループの概要情報を表示します。

<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
--------------------------------------------------------------------------------
BAGG20     D     0x8000,f474-88ff-ff01   2         0           0           Shar
```

表 6-5 コマンド出力

フィールド	説明
Aggregate Interface Type	アグリゲートインタフェースのタイプを表示します。**BAGG** はレイヤ2のアグリゲートインタフェースです。
Aggregation Mode	アグリゲーショングループのタイプです。 ● **S**ースタティックリンクアグリゲーションです。 ● **D**ーダイナミックリンクアグリゲーションです。
Loadsharing Type	ロードシェアリングのタイプです。 ● **Shar**—負荷分散を行います。 ● **NonS**—非負荷分散を行いません。
Actor System ID	ローカルシステムのIDです。システムLACPプライオリティ、システムのMACアドレスが含まれます。
AGG Interface	アグリゲートインタフェースのタイプと番号です。
AGG Mode	アグリゲーショングループのタイプです。
Partner ID	ピアシステムのシステムIDです。ピアシステムのLACPプライオリティ、ピアシステムのMACアドレスが含まれます。
Selected Ports	Selectedポートの総数です。
Unselected Ports	Unselectedポートの総数です。
Individual Ports	個々のポートの総数です。
Share Type	ロードシェアリングタイプです。

6.1.7 display link-aggregation verbose

Syntax

display link-aggregation verbose [**bridge-aggregation** [*interface-number*]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

bridge-aggregation:アグリゲートインタフェースを指定します。

interface-number: 既存のアグリゲートインタフェース番号を指定します。

説明

display link-aggregation verbose コマンドは指定されたアグリゲートインタフェースに対応するアグリゲーショングループの詳細情報を表示します。

bridge-aggregation パラメータのみを指定した場合、すべてのアグリゲートインタフェースの詳細情報を表示します。

アグリゲートインタフェースタイプを指定しない場合、すべてのアグリゲーショングループの詳細情報を表示します。

bridge-aggregation パラメータは装置でアグリゲートインタフェースが存在するときのみ有効です。

例

レイヤ 2 のアグリゲートインタフェースに対応したアグリゲーショングループ 10 の詳細情報を表示します。アグリゲーショングループはダイナミックのアグリゲーショングループです。

<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}
```

レイヤ 2 のアグリゲートインタフェースに対応したアグリゲーショングループ 20 の詳細情報を表示します。アグリゲーショングループはスタティックのアグリゲーショングループです。

<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         U       32768    1
  GE1/0/2         U       32768    1
  GE1/0/3         U       32768    1
```

表 6-6 コマンド出力

フィールド	説明
Loadsharing Type	ロードシェアリングのタイプです。 ● **Shar**—負荷分散を行います。 ● **NonS**—非負荷分散を行いません。
Port Status	ポートの状態です。 ● Selected ● Unselected ● Individual
Port	ポートタイプです。 ● **Auto port**—ポートは自動リンクアグリゲーションが有効です。このタイプは現在のソフトウェアバージョンでサポートしていません。 ● **Management port**—ポートはマネジメントポートです。このタイプは現在のソフトウェアバージョンでサポートしていません。 ● **Reference port**—このポートは参照ポートです。

フィールド	説明
Flags	1バイトのLACPの状態フラグです。最下位から最上位のビットまで、以下のようにA～Hで表示されます。1が真、0が偽で示します。 ● **A**－LACPが有効か無効かを示します。1が有効、0が無効です。 ● **B**－LACPのタイムアウトの長さを示します。1がショートタイムアウト、0がロングタイムアウトです。 ● **C**－送信システムがこのリンクを集約可能とみなすかどうかを示します。1は可能、0が不可能です。 ● **D**－送信システムがこのリンクを同期しているとみなすかどうかを示します。1が同期している、0が同期していないです。 ● **E**－送信システムが、受信フレームをアグリゲートしているかどうかを示します。1がアグリゲートしている、0がアグリゲートしていないです。 ● **F**－送信システムが、送信フレームを分配しているかどうかを示します。1が分配している、0が分配していないです。 ● **G**－送信システムがデフォルトのフレームを受信するかどうかを示します。1が受信する、0が受信しないです。 ● **H**－送信システムが期限切れのフレームを受信するかどうかを示します。1が受信する、0が受信しないです。
Aggregate Interface	アグリゲートインタフェースの名前です。
Aggregation Mode	アグリゲーショングループのタイプです。 ● **S**－スタティックです。 ● **D**－ダイナミックです。
Management VLANs	マネジメントVLANです。マネジメントVLANが指定されていない場合、**None**と表示されます。 このフィールドは現在のソフトウェアバージョンでサポートしていません。
System ID	ローカルのシステムIDです。ローカルのシステムLACPプライオリティとローカルのシステムMACアドレスが含まれます。

フィールド	説明
Local	ローカルインタフェースの情報です。 ● **Port**–ポートタイプと番号です。 ● **Status**–ポート状態です。Selectedあるいは Unselected、Individualがあります。 ● **Priority**–ポートプライオリティです。 ● **Oper-Key**–操作キーです。 ● **Flag**–LACPの状態フラグです。 🕮 **メモ：** スタティックのアグリゲーショングループでは、Flagは表示されません。
Remote	ピアエンドの情報です。 ● **Actor**–ローカルポートのタイプと番号です。ピアポートが参照ポートである場合、次のポートで（R）フラグを表示します。 ● **Priority**–ピアポートのプライオリティです。 ● **Oper-Key**–ピアポートの操作キーです。 ● **System ID**–ピアエンドのシステムIDです。 ● **Flag**–ピアエンドのLACPの状態フラグです。

6.1.8 interface bridge-aggregation

Syntax

interface bridge-aggregation *interface-number*

undo interface bridge-aggregation *interface-number*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

interface-number: アグリゲートインタフェースの番号を指定します。設定範囲は 1～1024 です。

説明

interface bridge-aggregation コマンドはアグリゲートインタフェースを作成し、aggregate interface view に移行します。すでにアグリゲートインタフェースが存在する場合、aggregate interface view に移行します。

undo interface bridge-aggregation コマンドはアグリゲートインタフェースを削除します。

アグリゲートインタフェースを作成したとき、システムは自動的に同一番号のアグリゲーショングループを作成します。デフォルトのアグリゲーショングループはスタティックのアグリゲーションモードです。

アグリゲートインタフェースを削除するとアグリゲートグループも削除されます。同時にアグリゲーショングループのメンバポートがアグリゲーショングループから除外されます。

例

アグリゲートインタフェース Bridge-Aggregation 1 を作成し、aggregate interface view に移行します。

<Switch> system-view

[Switch] interface bridge-aggregation 1

[Switch-Bridge-Aggregation1]

6.1.9 lacp period short

Syntax

lacp period short

undo lacp period

デフォルト

90 秒

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

説明

lacp period short コマンドはポートの LACP タイムアウト間隔をショート（3 秒）に設定します。ピアエンドは早急に LACPDU を送信することができます。

undo lacp period コマンドはデフォルトに戻します。

例

GigabitEthernet 1/0/1 の LACP タイムアウト間隔をショート（3 秒）に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] lacp period short

6.1.10 lacp system-priority

Syntax

lacp system-priority *priority*

undo lacp system-priority

デフォルト

32768

View

System view

定義済みユーザロール

network-admin

パラメータ

priority: システム LACP プライオリティです。設定範囲は 0～65535 です。この値が小さいほど、LACP プライオリティが高くなります。

説明

lacp system-priority コマンドはシステム LACP プライオリティを設定します。

undo lacp system-priority コマンドはデフォルトに戻します。

例

システム LACP プライオリティを 64 に設定します。

<Switch> system-view

[Switch] lacp system-priority 64

関連コマンド

link-aggregation port-priority

6.1.11 link-aggregation global load-sharing mode

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

デフォルト

システムはパケットタイプに従い自動でグローバルのリンクアグリゲーションのロードシェアリングモードを選択します。

装置は以下の組み合わせでロードシェアリングを行います。

- パケットタイプに従った自動ロードシェアリングモードの選択
- 送信元 IP アドレス
- 宛先 IP アドレス
- 送信元 MAC アドレス
- 宛先 MAC アドレス
- 入力ポート
- 送信元 MAC アドレスと宛先 MAC アドレス
- 送信元 IP アドレスと宛先 IP アドレス
- 送信元 IP アドレスと送信元ポート
- 宛先 IP アドレスと宛先ポート
- 送信元 IP アドレス、送信元ポート、宛先 IP アドレス、宛先ポート
- 送信元 MAC アドレス、宛先 MAC アドレス、送信元 IP アドレス、宛先 IP アドレス

View

System view

定義済みユーザロール

network-admin

パラメータ

destination-ip: 宛先 IP アドレスをもとにしてリンクアグリゲーショングループのロードシェアリングを実行します。

destination-mac: 宛先 MAC アドレスをもとにしてリンクアグリゲーショングループのロードシェアリングを実行します。

destination-port: 宛先ポートをもとにしてリンクアグリゲーショングループのロードシェアリングを実行します。

ingress-port: 入力ポートをもとにしてリンクアグリゲーショングループのロードシェアリングを実行します。

source-ip: 送信元 IP アドレスをもとにしてリンクアグリゲーショングループのロードシェアリングを実行します。

source-mac: 送信元 MAC アドレスをもとにしてリンクアグリゲーショングループのロードシェアリングを実行します。

source-port: 送信元ポートをもとにしてリンクアグリゲーショングループのロードシェアリングを実行します。

説明

link-aggregation global load-sharing mode コマンドはグローバルのリンクアグリゲーションのロードシェアリングのモードを設定します。

undo link-aggregation global load-sharing mode コマンドはデフォルトに戻します。

設定したロードシェアリングのモードは前のロードシェアリングのモードに上書きされます。

コマンドを複数回実行した場合、最後に行った設定が適用されます。

サポートされていないリンクアグリゲーションのロードシェアリングモードが設定された場合、エラーが発生します。

例

宛先 MAC アドレスをもとにしてグローバルのリンクアグリゲーショングループのロードシェアリングのモードを設定します。

<Switch> system-view

[Switch] link-aggregation global load-sharing mode destination-mac

関連コマンド

link-aggregation load-sharing mode

6.1.12 link-aggregation load-sharing mode local-first

Syntax

link-aggregation load-sharing mode local-first

undo link-aggregation load-sharing mode local-first

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

link-aggregation load-sharing mode local-first コマンドはリンクアグリゲーションの local-first ロードシェアリングを有効にします。

undo link-aggregation load-sharing mode local-first コマンドはリンクアグリゲーションの local-first ロードシェアリングを無効にします。

local-first ロードシェアリングを無効にすると、すべての IRF スタックメンバ装置のアグリゲートインタフェースのすべての Selected ポート間でパケットのロードシェアリングを行います。

例

リンクアグリゲーションの local-first ロードシェアリングを無効にします。

<Switch> system-view

[Switch] undo link-aggregation load-sharing mode local-first

6.1.13 link-aggregation mode

Syntax

link-aggregation mode dynamic

undo link-aggregation mode

デフォルト

スタティックアグリゲーションモード

View

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

link-aggregation mode dynamic コマンドはダイナミックアグリゲーションモードで動作するようにアグリゲーショングループを設定し、LACP を有効にします。

undo link-aggregation mode コマンドはデフォルトに戻します。

例

ダイナミックアグリゲーションモードで動作するようにアグリゲートインタフェース Bridge-Aggregation 1 に対応するアグリゲーショングループを設定します。

<Switch> system-view

[Switch] interface bridge-aggregation 1

[Switch-Bridge-Aggregation1] link-aggregation mode dynamic

6.1.14 link-aggregation port-priority

Syntax

link-aggregation port-priority *priority*

undo link-aggregation port-priority

デフォルト

32768

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

priority: ポートプライオリティを設定します。設定範囲は 0～65535 です。この値が小さいほど、LACP プライオリティが高くなります。

説明

link-aggregation port-priority コマンドはインタフェースのポートプライオリティを設定します。

undo link-aggregation port-priority コマンドはデフォルトに戻します。

例

GigabitEthernet 1/0/1 のポートプライオリティを 64 に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] link-aggregation port-priority 64

関連コマンド

lacp system-priority

6.1.15 link-aggregation selected-port maximum

Syntax

link-aggregation selected-port maximum *max-number*

undo link-aggregation selected-port maximum

デフォルト

8

View

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

max-number: アグリゲーショングループで使用できる Selected ポートの最大数を設定します。設定範囲は 1～8 です。

説明

link-aggregation selected-port maximum コマンドはアグリゲーショングループで使用できる Selected ポートの最大数を設定します。

undo link-aggregation selected-port maximum コマンドはデフォルトに戻します。

このコマンドを実行すると、アグリゲーショングループのいくつかの Selected ポートは Unselected ポートになる可能性があります。

アグリゲーショングループで使用できる Selected ポートの最大数は、ローカルとピアエンドで同一にする必要があります。

アグリゲーショングループで使用できる Selected ポートの最大数は、以下の値の小さい方に制限されます。

- **link-aggregation selected-port maximum** コマンドで設定された最大数
- ハードウェアの制限

以下の処理を実行することによって 2 つのポート間でバックアップを設定することができます。

- アグリゲーショングループに 2 つのポートを割り当てます。
- アグリゲーショングループで使用できる Selected ポートの最大数を 1 に設定します。

そして、アグリゲーショングループの Selected ポートはすべてのポイントで使用できますが、Unselected ポートはバックアップポートとして動作します。

例

アグリゲートインタフェース Bridge-Aggregation 1 に対応するアグリゲーショングループで使用できる Selected ポートの最大数を 5 に設定します。

<Switch> system-view

[Switch] interface bridge-aggregation 1

[Switch-Bridge-Aggregation1] link-aggregation selected-port maximum 5

関連コマンド

link-aggregation selected-port minimum

6.1.16 link-aggregation selected-port minimum

Syntax

link-aggregation selected-port minimum *min-number*

undo link-aggregation selected-port minimum

デフォルト

設定なし

View

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

min-number: アグリゲートインタフェースを UP にするのに必要なアグリゲーショングループで使用できる Selected ポートの最小数を設定します。設定範囲は 1～8 です。

説明

link-aggregation selected-port minimum コマンドはアグリゲーショングループで使用できる Selected ポートの最小数を設定します。

undo link-aggregation selected-port minimum コマンドはデフォルトに戻します。

このコマンドを実行すると、アグリゲーショングループのすべてのメンバポートは Unselected ポートになる可能性があります。

アグリゲーショングループで使用できる Selected ポートの最小数は、ローカルとピアエンドで同一にする必要があります。

例

アグリゲートインタフェース Bridge-Aggregation 1 に対応するアグリゲーショングループで使用できる Selected ポートの最小数を 3 に設定します。

<Switch> system-view

[Switch] interface bridge-aggregation 1

[Switch-Bridge-Aggregation1] link-aggregation selected-port minimum 3

関連コマンド

link-aggregation selected-port maximum

6.1.17 port link-aggregation group

Syntax

port link-aggregation group *group-id*

undo port link-aggregation group

デフォルト

設定なし

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

group-id: アグリゲーショングループに対応するアグリゲートインタフェースの数を指定します。設定範囲は 1～1024 です。

説明

port link-aggregation group コマンドは指定したアグリゲーショングループにインタフェースを割り当てます。

undo port link-aggregation group コマンドは所属しているアグリゲーショングループからインタフェースを削除します。

インタフェースは 1 つのアグリゲーショングループのみ所属することができます。

例

アグリゲーショングループ 1 に GigabitEthernet 1/0/1 を割り当てます。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] port link-aggregation group 1

6.1.18 reset counters interface

Syntax

reset counters interface [**bridge-aggregation** [*interface-number*]]

View

User view

定義済みユーザロール

network-admin

パラメータ

bridge-aggregation: アグリゲートインタフェースを指定します。

interface-number: アグリゲートインタフェース番号を指定します。

説明

reset counters interface コマンドは指定されたアグリゲートインタフェースの統計情報を削除します。

一定期間、トラフィックの統計情報を収集する場合、以前に収集された統計情報の履歴を削除し、このコマンドを使用します。

パラメータを指定しない場合、システムのすべてのインタフェースの統計情報を削除します。

bridge-aggregation パラメータのみを使用する場合、すべてのレイヤ 2 のアグリゲートインタフェースの統計情報を削除します。

bridge-aggregation *interface-number* パラメータを指定した場合、指定したレイヤ 2 のアグリゲートインタフェースの統計情報を削除します。

bridge-aggregation パラメータは装置でレイヤ 2 のアグリゲートインタフェースが存在するときのみ有効です。

例

アグリゲートインタフェース Bridge-Aggregation 1 の統計情報を削除します。

<Switch> reset counters interface bridge-aggregation 1

6.1.19 reset lacp statistics

Syntax

reset lacp statistics [**interface** *interface-list*]

View

User view

定義済みユーザロール

network-admin

パラメータ

interface *interface-list*: リンクアグリゲーションメンバポートを指定します。形式は *interface-type interface-number1* [**to** *interface-type interface-number2*] です。*interface-number2* は *interface-number1* 以上の値にしてください。メンバポートを指定しない場合、すべてのメンバポートの LACP の統計情報を削除します。

説明

reset lacp statistics コマンドはリンクアグリゲーションメンバポートの LACP の統計情報を削除します。

例

すべてのリンクアグリゲーションメンバポートの LACP の統計情報を削除します。

<Switch> reset lacp statistics

関連コマンド

display link-aggregation member-port

6.1.20 shutdown

Syntax

shutdown

undo shutdown

View

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

shutdown コマンドはアグリゲートインタフェースをシャットダウンします。

undo shutdown コマンドはアグリゲートインタフェースを up にします。

例

アグリゲートインタフェース Bridge-Aggregation 1 を up にします。

<Switch> system-view

[Switch] interface bridge-aggregation 1

[Switch-Bridge-Aggregation1] undo shutdown

目次

このセクションのページは **3-x-x** です。

7 章 Port Isolation 7-1
7.1 Port Isolation 設定コマンド 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 7-3

7章 Port Isolation

🕮 メモ：

QX-S5100G シリーズは、ポートアイソレーションと MLD スヌーピングを同時に使用することができません。

7.1 Port Isolation設定コマンド

7.1.1 display port-isolate group

Syntax

display port-isolate group [*group-id*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

group-id: アイソレーショングループの番号を指定します。設定範囲は 1～8 です。

説明

display port-isolate group コマンドはアイソレーショングループの情報を表示します。

例

すべてのアイソレーショングループの情報を表示します。

<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
```

アイソレーショングループ 1 の情報を表示します。

<Switch> display port-isolate group 1

```
Port isolation group information:
Group ID: 1
Group members:
   GigabitEthernet1/0/1
```

表 7-1 コマンド出力

フィールド	説明
Group ID	アイソレーショングループ番号です。
Group members	アイソレーショングループのアイソレートポートです。 アイソレーショングループにポートがない場合、**No ports**と表示されます。

関連コマンド

port-isolate enable

7.1.2 port-isolate enable

Syntax

port-isolate enable group *group-id*

undo port-isolate enable

デフォルト

設定なし

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

group *group-id*: アイソレーショングループの番号を指定します。設定範囲は 1～8 です。

説明

port-isolate enable コマンドはアイソレーショングループにポートを割り当てます。

undo port-isolate enable コマンドはアイソレーショングループからポートを削除します。

interface view で設定した場合、インタフェースのみ適用されます。

aggregate interface view で設定した場合、アグリゲートインタフェースとアグリゲーションメンバポートに適用されます。装置がアグリゲートインタフェースへの設定が適用できなかった場合、アグリゲーションメンバポートはアイソレーショングループに割り当てられません。アグリゲーションメンバポートで故障が発生した場合、装置はポートをスキップし、アイソレーショングループをほかのアグリゲーションメンバポートに割り当て続けます。

指定されたアイソレーショングループにポートを割り当てるため、アイソレーショングループはすでに作成されている必要があります。

1 つのポートは 1 つのアイソレーショングループにのみ割り当てることができます。

例

アイソレーショングループ 1 に GigabitEthernet 1/0/1、GigabitEthernet 1/0/2 を割り当てます。

<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

関連コマンド

display port-isolate group

7.1.3 port-isolate group

Syntax

port-isolate group *group-id*

undo port-isolate group { *group-id* | **all** }

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

group-id: アイソレーショングループの番号を指定します。設定範囲は 1～8 です。

all: すべてのアイソレーショングループを削除します。

説明

port-isolate group コマンドはアイソレーショングループを作成します。

undo port-isolate group コマンドはアイソレーショングループを削除します。

コマンドを複数回実行した場合、最後に行った設定が適用されます。

例

アイソレーショングループ 1 を作成します。

<Switch> system-view

[Switch] port-isolate group 1

目次

このセクションのページは **3-x-x** です。

8 章 STP 8-1
8.1 STP 設定コマンド 8-1
8.1.1 active region-configuration 8-1
8.1.2 bpdu-drop any 8-2
8.1.3 check region-configuration 8-2
8.1.4 display stp 8-4
8.1.5 display stp abnormal-port 8-12
8.1.6 display stp bpdu-statistics 8-14
8.1.7 display stp down-port 8-17
8.1.8 display stp history 8-18
8.1.9 display stp region-configuration 8-20
8.1.10 display stp root 8-21
8.1.11 display stp tc 8-22
8.1.12 instance 8-24
8.1.13 region-name 8-25
8.1.14 reset stp 8-26
8.1.15 revision-level 8-27
8.1.16 snmp-agent trap enable stp 8-28
8.1.17 stp bpdu-protection 8-29
8.1.18 stp bridge-diameter 8-30
8.1.19 stp compliance 8-31
8.1.20 stp config-digest-snooping 8-32
8.1.21 stp cost 8-33
8.1.22 stp dispute-protection 8-35
8.1.23 stp edged-port 8-36
8.1.24 stp enable 8-37
8.1.25 stp global config-digest-snooping 8-38
8.1.26 stp global enable 8-39
8.1.27 stp global mcheck 8-40
8.1.28 stp ignore-pvid-inconsistency 8-41
8.1.29 stp log enable tc 8-41
8.1.30 stp loop-protection 8-42
8.1.31 stp max-hops 8-43
8.1.32 stp mcheck 8-44
8.1.33 stp mode 8-45
8.1.34 stp no-agreement-check 8-46

8.1.35 stp pathcost-standard 8-47
8.1.36 stp point-to-point 8-48
8.1.37 stp port bpdu-protection 8-49
8.1.38 stp port priority 8-50
8.1.39 stp port shutdown permanent 8-52
8.1.40 stp port-log 8-52
8.1.41 stp priority 8-54
8.1.42 stp pvst-bpdu-protection 8-55
8.1.43 stp region-configuration 8-56
8.1.44 stp role-restriction 8-56
8.1.45 stp root primary 8-57
8.1.46 stp root secondary 8-58
8.1.47 stp root-protection 8-59
8.1.48 stp tc-protection 8-60
8.1.49 stp tc-protection threshold 8-61
8.1.50 stp tc-snooping 8-62
8.1.51 stp timer forward-delay 8-63
8.1.52 stp timer hello 8-64
8.1.53 stp timer max-age 8-65
8.1.54 stp timer-factor 8-67
8.1.55 stp transmit-limit 8-68
8.1.56 stp vlan enable 8-69
8.1.57 vlan-mapping modulo 8-70

8章 STP

8.1 STP設定コマンド

8.1.1 active region-configuration

Syntax

active region-configuration

View

MST region view

定義済みユーザロール

network-admin

説明

active region-configuration コマンドは MST(multiple spanning tree)リージョン設定をアクティブにします。

MST リージョンパラメータを設定するとき、MSTP は新しいスパニングツリーの計算プロセスを行います。スパニングツリーの計算プロセスが実行されるとネットワークが不安定になります。VLAN-インスタンスマッピングテーブルを設定するときに、よく発生します。このため **active region-configuration** コマンドあるいは **stp global enable** コマンドを実行したのち、MSTP を有効にします。

このコマンドを実行する前に、**check region-configuration** コマンドを使用して MST のリージョンの設定が正しいことを確認してください。MST のリージョンの設定が正しいことが確認できたら、このコマンドを実行してください。

例

MSTI 1 に VLAN 2 をマッピングし、MST リージョンの設定を有効にします。

<Switch> system-view

[Switch] stp region-configuration

[Switch-mst-region] instance 1 vlan 2

[Switch-mst-region] active region-configuration

関連コマンド

- **check region-configuration**
- **instance**
- **region-name**
- **revision-level**

- **stp global enable**
- **vlan-mapping modulo**

8.1.2 bpdu-drop any

Syntax

bpdu-drop any

undo bpdu-drop any

デフォルト

無効

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

説明

bpdu-drop any コマンドはポートで BPDU ドロップ機能を有効にします。

undo bpdu-drop any コマンドは BPDU ドロップ機能を無効にします。

装置は STP、RSTP、MSTP、PVST、LACP、イーサネット OAM、GVRP、および LLDP の BPDU をドロップします。本コマンドを設定する場合は、この機能の影響を十分に認識しておく必要があります。

例

GigabitEthernet 1/0/1 で BPDU ドロップ機能を有効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] bpdu-drop any

8.1.3 check region-configuration

Syntax

check region-configuration

View

MST region view

定義済みユーザロール

network-admin

説明

check region-configuration コマンドはリージョン名、リビジョンレベル、VLAN-インスタンスマッピング設定などの、まだアクティブにされていない MST リージョンの設定の情報を表示します。

スパニングツリーの装置は物理リンクを通して接続され、以下の設定が同一であるときのみ、同じ MST リージョンに属します。

- フォーマットセレクタ（デフォルトは 0 で設定できません。）
- MST リージョン名
- MST リージョンリビジョンレベル
- MST リージョンの VLAN-インスタンスマッピングエントリ

MST リージョンの設定をアクティブにする前に、MST のリージョン設定が正しいかどうかをチェックするために、このコマンドを使うことを推奨します。結果が正しいときのみ、MST リージョン設定をアクティブにしてください。

例

MST リージョンのまだアクティブにされていない設定の情報を表示します。

<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
```

表 8-1 コマンド出力

フィールド	説明
Format selector	フォーマットセレクタです。値は0です（設定はできません）
Region name	MST リージョン名です。
Revision level	MSTリージョンのリビジョンレベルです。

フィールド	説明
Instance VLANs Mapped	MSTリージョンのVLAN-インスタンスマッピングエントリです。

関連コマンド

- **active region-configuration**
- **instance**
- **region-name**
- **revision-level**
- **vlan-mapping modulo**

8.1.4 display stp

Syntax

display stp [**instance** *instance-list* | **vlan** *vlan-id-list*] [**interface** *interface-list* | **slot** *slot-number*] [**brief**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

instance *instance-list*: MSTI を指定します。半角スペースで区切り 10 まで設定するか、MSTI の範囲で設定することができます。MSTI を範囲で指定する形式は *instance-id1* [**to** *instance-id2*]です。*instance-id2* は *instance-id1* 以上の値にしてください。設定範囲は 0～4094 です。0 は CIST を示します。

vlan *vlan-id-list*: VLAN を指定します。半角スペースで区切り 10 まで設定するか、VLAN の範囲で設定することができます。VLAN を範囲で指定する形式は *vlan-id1* [**to** *vlan-id2*] です。*vlan-id2* は *vlan-id1* 以上の値にしてください。設定範囲は 1～4094 です。

interface *interface-list*: インタフェースを指定します。半角スペースで区切り 10 まで設定するか、インタフェースの範囲で設定することができます。インタフェースを範囲で指定する形式は *interface-type interface-number1* [**to** *interface-type interface-number2*] です。*interface-number2* は *interface-number1* 以上の値にしてください。

brief: スパニングツリーの状態と統計情報の概要を表示します。指定しない場合、詳細なスパニングツリーの状態と統計情報を表示します。

slot *slot-number*: IRF スタックメンバ装置を指定します。*slot-number* は IRF スタックメンバ装置の ID を示します。指定しない場合、IRF スタックユニットのすべてのメンバ装置に適用されます。

説明

display stp コマンドはスパニングツリーの状態と統計情報を表示します。スパニングツリーの状態および統計情報にもとづいて、ネットワークトポロジの分析および維持、あるいはスパニングツリーが正常に動作しているか確認することができます。

STP あるいは RSTP モード：コマンド出力はポート名の順番で表示されます。

- ポートを指定しない場合、すべてのポートに適用されます。
- ポートリストを指定した場合、指定したポートに適用されます。

PVST モード：コマンド出力はそれぞれの VLAN の VLAN ID とポート名の順番で表示されます。

- VLAN あるいはポートを指定しない場合、すべての VLAN のすべてのポートに適用されます。
- VLAN を指定し、ポートを指定しない場合、すべての VLAN の指定したポートに適用されます。
- ポートリストを指定し、VLAN を指定しない場合、すべての VLAN の指定したポートに適用されます。
- VLAN およびポートリストを指定した場合、指定した VLAN のポートに適用されます。

MSTP モード：コマンド出力はそれぞれの MSTI の MSTI ID とポート名の順番で表示されます。

- MSTI あるいはポートを指定しない場合、すべてのポートの MSTI に適用されます。
- MSTI を指定し、ポートを指定しない場合、指定した MSTI のすべてのポートに適用されます。
- ポートリストを指定し、MSTI を指定しない場合、指定したポートのすべての MSTI に適用されます。
- MSTI およびポートリストを指定した場合、指定した MSTI の指定ポートに適用されます。

例

MSTP モードで、MSTI0 の GigabitEthernet 1/0/1 のスパニングツリーの状態と概要情報を表示します。

<Switch> display stp instance 0 interface GigabitEthernet 1/0/1 brief

```
MST ID     Port                    Role  STP State     Protection
0          GigabitEthernet1/0/1      ALTE  DISCARDING    LOOP
```

PVST モードで、VLAN2 の GigabitEthernet 1/0/1 のスパニングツリーの状態と概要情報を表示します。

<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
```

表 8-2 コマンド出力

フィールド	説明
MST ID	MSTリージョンのMSTI IDです。
Port	各MSTIあるいはVLANに対応するポート名です。
Role	ポートの役割です。 • **ALTE**—代理ポートです。 • **BACK**—バックアップポートです。 • **ROOT**—ルートポートです。 • **DESI**—Designatedポートです。 • **MAST**—マスタポートです。 • **DISA**—ポートが無効です。
STP State	ポートのスパニングツリーの状態です。 • **FORWARDING**—ポートはBPDUを送受信し、ユーザトラフィックを転送します。 • **DISCARDING**—ポートはBPDUを送受信できますが、ユーザトラフィックを転送できません。 • **LEARNING**—ポートは過渡状態です。ポートはBPDUを送受信できますが、ユーザトラフィックを転送できません。
Protection	ポートの保護タイプです。 • **ROOT**—Rootガード（保護）です。 • **LOOP**—Loopガード（保護）です。 • **BPDU**—BPDUガード（保護）です。 スパニングツリーが設定されていない、あるいはスパニングツリーのガード機能が開始されていない場合、**NONE**と表示されます。

MSTP モードで、すべてのポートのすべての MSTI のスパニングツリーの状態と詳細情報を表示します。

<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
```

PVST モードで、すべての VLAN のすべてのポートのスパニングツリーの状態と詳細情報を表示します。

<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
```

MSTP モードで、スパニングツリー機能が無効であるときのスパニングツリーの状態と詳細情報を表示します。

<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
```

PVST モードで、スパニングツリー機能が無効であるときのスパニングツリーの状態と詳細情報を表示します。

<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
```

表 8-3 コマンド出力

フィールド	説明
Bridge ID	ブリッジのIDです。装置のプライオリティとMACアドレスを含みます。たとえば32768.000f-e200-2200において、ピリオド（.）の前の値は装置のプライオリティを示し、ピリオド（.）の前の値は装置のMACアドレスを示します。
Bridge times	ブリッジの主要パラメータです。 • **Hello**—Hello時間です。 • **MaxAge**—最大エージング時間です。 • **FwdDelay**—転送遅延時間です。 • **MaxHops**—MSTリージョンの最大ホップ数です。
Root ID/ERPC	CISTルートIDと外部パスコストです。（装置からCISTルートまでのパスコストです）

フィールド	説明
RegRoot ID/IRPC	CISTリージョナルルートIDと内部パスコストです。（装置からCISTリージョナルルートまでのパスコストです）
VlanRoot ID/RPC	VLANルートIDと内部パスコストです。（装置からVLANルートブリッジまでのパスコストです）
RootPort ID	ルートポートIDです。**0.0**は装置がルートでルートポートがないことを示します。
BPDU-Protection	BPDU保護のグローバル状態を示します。
Bridge Config-Digest-Snooping	Digest Snoopingのグローバル状態を示します。
TC or TCN received	MSTIあるいはVLANで受信されたTC/TCNパケット数です。
Time since last TC	MSTIあるいはVLANで最後にトポロジが変更されてからの経過時間です。
[FORWARDING]	ポートがforwarding状態です。
[DISCARDING]	ポートが廃棄状態です。
[LEARNING]	ポートがlearning状態です。
Port protocol	ポートのスパニングツリーの状態です。
Port role	ポートの役割です。 • **Alternate**—代理ポートです。 • **Backup**—バックアップポートポートです。 • **Root**—ルートポートです。 • **Designated**—Designatedポートです。 • **Master**—マスタポートです。 • **Disabled**—ポートが無効です。
(Boundary)	ポートが境界ポートです。
Port cost(Legacy)	ポートのパスコストです。括弧の中身はポートパスコストの計算で使用される標準（legacy、dot1d-1998、あるいはdot1t）を示します。 • **Config**－設定値です。 • **Active**－実際の値です。
Desg.bridge/port	ポートのDesignated ブリッジIDとポートIDです。 表示されたポートIDは、ポートプライオリティをサポートしないポートであるため、重要ではありません。
Port edged	edgeポートあるいは非edgeポートです。 • **Config**－設定値です。 • **Active**－実際の値です。

フィールド	説明
Point-to-Point	ポートがポイントツーポイントで接続されているかどうかを示します。 • **Config**－設定値です。 • **Active**－実際の値です。
Transmit limit	各Hello時間以内にポートから送信されたBPDU最大数です。
Protection type	スパニングツリーの保護機能がポートで設定されているかどうかを示します。 • **Config**－設定値です。 • **Active**－適用されています。 ポートの保護タイプです。 • **ROOT**—Rootガードです。 • **LOOP**—Loopガードです。 • **BPDU**—BPDUガードです。 • **PVST BPDU**—PVST BPDUガードです。 スパニングツリーが設定されていない、あるいはスパニングツリーのガード機能が開始されていない場合、**NONE**と表示されます。
TC-Restriction	ポートのTC転送の制限の状態です。 TC-Restrictionはサポートしていません。
Role-Restriction	ポートのポート役割の制限の状態です。
MST BPDU format	ポートが送信可能なMST BPDUの形式です。 • **Config**－設定値（legacyあるいは802.1s準拠）です。 • **Active**－実際の値（legacyあるいは802.1s準拠）です。
Port Config-Digest-Snooping	ポートのDigest Snoopingの状態です。
Rapid transition	MSTIあるいはVLANでポートの転送状態が高速状態遷移であるかどうかを示します。
Num of VLANs mapped	MSTIにマッピングされたVLAN数です。
Port times	ポートの主要パラメータです。 • **Hello**—Hello時間です。 • **MaxAge**—最大エージング時間です。 • **FwdDelay**—転送遅延時間です。 • **MsgAge**—メッセージのエージング時間 • **RemHops**—残りのホップ数です。
BPDU sent	送信BPDUの統計情報です。

フィールド	説明
BPDU received	受信BPDUの統計情報です。
RegRoot ID/IRPC	MSTIリージョナルルートと内部パスのコストです。
Root Type	MSTIルートタイプです。 ● **Primary root**－プライマリルートです。 ● **Secondary root**－セカンダリルートです。
Master bridge	MSTIルートブリッジIDです。
Cost to master	MSTIからマスタブリッジへのパスコストです。
TC received	受信TC BPDUの数です。
Protocol status	スパニングツリープロトコルの状態です。
Protocol Std.	スパニングツリープロトコルが標準です。
Version	スパニングツリープロトコルのバージョンです。
Bridge-Prio.	● MSTPモードで、CISTの装置のプライオリティです。 ● PVSTモードで、VLAN1の装置のプライオリティです。
Max age(s)	BPDUのエージング時間です。（単位は秒です。PVSTモードのVLAN1のエージング時間と同一です）
Forward delay(s)	ポートの状態遷移遅延です。（単位は秒です。PVSTモードのVLAN1の状態遷移遅延と同一です）
Hello time(s)	BPDUを送信するルートブリッジの送信間隔です。（単位は秒です。PVSTモードのVLAN1の送信間隔と同一です）
Max hops	MSTIの最大ホップ数です。
TC Snooping	TC snoopingの状態です。 ● **Enabled**－有効です。 ● **Disabled**－無効です。

関連コマンド

reset stp

8.1.5 display stp abnormal-port

Syntax

display stp abnormal-port

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display stp abnormal-port コマンドは、スパニングツリー保護機能によってブロックされたポートに関する情報を表示します。

MSTI あるいはVLAN ではスパニングツリー保護機能によってブロックされたポートで最大 3 つの履歴を表示することができます。

例

MSTI モードでスパニングツリー保護機能によってブロックされたポートに関する情報を表示します。

<Switch> display stp abnormal-port

```
---[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
```

PVST モードでスパニングツリー保護機能によってブロックされたポートに関する情報を表示します。

<Switch> system-view

[Switch] stp mode pvst

[Switch] display stp abnormal-port

```
---[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
```

表 8-4 コマンド出力

フィールド	説明
MST ID	ブロックされたポートのMSTIです。
VLAN ID	ブロックされたポートのVLANです。

フィールド	説明
BlockReason	ポートがブロックされた理由です。 • **Root-Protected**—Rootガード機能です。 • **Loop-Protected**—Loopガード機能です。 • **Loopback-Protected**—自己ループの保護です。MSTIのポートが送信したBPDUを受信しました。 • **Disputed**—Disputeの保護です。ポートは非ブロックのDesignatedポートから低いプライオリティのBPDUを受信しました。 • **InconsistentPortType-Protected**—ポートタイプ不一致保護です。 • **InconsistentPvid-Protected**—PVID不一致保護です。
Time	保護機能の開始時間です。

8.1.6 display stp bpdu-statistics

Syntax

display stp bpdu-statistics [**interface** *interface-type interface-number* [**instance** *instance-list*]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: インタフェースのタイプと番号を指定します。

instance *instance-list*: MSTI を指定します。半角スペースで区切り 10 まで設定するか、MSTI の範囲で設定することができます。MSTI を範囲で指定する形式は *instance-id1* [**to** *instance-id2*]です。*instance-id2* は *instance-id1* 以上の値にしてください。設定範囲は 0～4094 です。0 は CIST を示します。

説明

display stp bpdu-statistics コマンドはポートの BPDU 統計情報を表示します。

MSTP モード：コマンド出力はポート名と MSTI ID の順番で表示されます。

- MSTI あるいはポートを指定しない場合、すべてのポートのすべての MSTI に適用されます。
- ポートを指定し、MSTI を指定しない場合、ポートのすべての MSTI に適用されます。
- MSTI およびポートを指定した場合、指定したポートの指定した MSTI に適用されます。

STP、RSTP あるいは PVST モード：コマンド出力はポート名の順番で表示されます。

- ポートを指定しない場合、すべてのポートに適用されます。
- ポート名を指定した場合、指定したポートに適用されます。

例

MSTP モードで GigabitEthernet 1/0/1 のすべての MSTI の BPDU 統計情報を表示します。

<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
```

PVST モードで GigabitEthernet 1/0/1 の BPDU 統計情報を表示します。

<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
```

表 8-5 コマンド出力

フィールド	説明
Port	ポート名です。
Instance-Independent	特定のMSTIに関係ない統計情報です。
Type	統計項目です。
Looped-back BPDUs	BPDUを送信したのち、同一ポートで受信したBPDUです。
Max-aged BPDUs	最大エージングを超過したBPDUです。
TCN sent	TCN BPDUの送信数です。
TCN received	TCN BPDUの受信数です。

フィールド	説明
TCA sent	TCA BPDUの送信数です。
TCA received	TCA BPDUの受信数です。
Config sent	Configuration BPDUの送信数です。
Config received	Configuration BPDUの受信数です。
RST sent	RSTP BPDUの送信数です。
RST received	RSTP BPDUの受信数です。
MST sent	MSTP BPDUの送信数です。
MST received	MSTP BPDUの受信数です。
Instance	特定のMSTIの統計情報です。
Timeout BPDUs	タイムアウトしたBPDUです。
Max-hoped BPDUs	最大ホップ数が超過したBPDUです。
TC detected	TC BPDUの検出数です。
TC sent	TC BPDUの送信数です。
TC received	TC BPDUの受信数です。
PVID inconsistency BPDUs	入力ポートに一致しないPVSTのPVST BPDU受信数です。

8.1.7 display stp down-port

Syntax

display stp down-port

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display stp down-port コマンドは STP 保護機能によってシャットダウンされたポートに関する情報を表示します。

例

STP 保護機能によってシャットダウンされたポートに関する情報を表示します。

<Switch> display stp down-port

```
Down Port                Reason
GigabitEthernet1/0/1       BPDU protection
```

表 8-6 コマンド出力

フィールド	説明
Down Port	STP保護機能によってシャットダウンされたポート名です。
Reason	ポートがシャットダウンされた理由です。 ● **BPDU-Protected**－BPDUガード機能を示します。 ● **PVST BPDU protection**－PVST BPDUガード機能を示します。

8.1.8 display stp history

Syntax

display stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **history** [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

instance *instance-list*: MSTI を指定します。半角スペースで区切り 10 まで設定するか、MSTI の範囲で設定することができます。MSTI を範囲で指定する形式は *instance-id1* [**to** *instance-id2*]です。*instance-id2* は *instance-id1* 以上の値にしてください。設定範囲は 0～4094 です。0 は CIST を示します。

vlan *vlan-id-list*: VLAN を指定します。半角スペースで区切り 10 まで設定するか、VLAN の範囲で設定することができます。VLAN を範囲で指定する形式は *vlan-id1* [**to** *vlan-id2*] です。*vlan-id2* は *vlan-id1* 以上の値にしてください。設定範囲は 1～4094 です。

slot *slot-number*: IRF スタックメンバ装置を指定します。*slot-number* は IRF スタックメンバ装置の ID を示します。指定しない場合、IRF スタックユニットのすべてのメンバ装置に適用されます。

説明

display stp history コマンドはポートのロール計算の履歴情報を表示します。

STP あるいは RSTP モードではポートのロール計算の時間の順番で表示されます。

PVST モード：コマンド出力は VLAN ID と各 VLAN のポートのロール計算の時間の順番で表示されます。

- VLAN を指定しない場合、すべての VLAN に適用されます。
- VLAN リストを指定した場合、指定した VLAN に適用されます。

MSTP モード：コマンド出力は MSTI ID と各 MSTI のポートのロール計算の時間の順番で表示されます。

- MSTI を指定しない場合、すべての MSTI に適用されます。
- MSTI リストを指定した場合、指定した MSTI に適用されます。

例

MSTP モードで、MSTI 2 の IRF スタックメンバ装置 1 のポートのロール計算の履歴情報を表示します。

<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
```

PVST モードで、VLAN 2 の IRF スタックメンバ装置 1 のポートロール計算の履歴情報を表示します。

<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
```

表 8-7 コマンド出力

フィールド	説明
Port	ポート名です。
Role change	ポートの役割変更です。（**Aged**は設定BPDUのタイムアウトによって変更が起きたことを示します）
Time	ポートロール計算の時間です。

8.1.9 display stp region-configuration

Syntax

display stp region-configuration

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display stp region-configuration コマンドは有効な MST リージョンの設定情報を表示します。

例

MSTP モードで有効な MST リージョンの設定情報を表示します。

<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
```

表 8-8 コマンド出力

フィールド	説明
Format selector	スパニングツリープロトコルで定義されたフォーマットセレクタです。デフォルト値は0です。セレクタは設定できません。
Region name	MSTリージョン名です。
Revision level	MSTリージョンのリビジョンレベルです。**revision-level**コマンドを使って設定できます。デフォルトは0です。
VLANs Mapped	MSTIにマッピングされたVLANです。

関連コマンド

- **instance**
- **region-name**
- **revision-level**
- **vlan-mapping modulo**

8.1.10 display stp root

Syntax

display stp root

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display stp root コマンドはスパニングツリーのルートブリッジ情報を表示します。

例

MSTP モードですべてのスパニングツリーのルートブリッジ情報を表示します。

<Switch> display stp root

```
MST ID  Root Bridge ID       ExtPathCost IntPathCost Root Port
0       0.f474-880e-6554     200200      0           GigabitEthernet1/0/1
```

PVST モードですべてのスパニングツリーのルートブリッジ情報を表示します。

<Switch> display stp root

```
VLAN ID  Root Bridge ID       ExtPathCost IntPathCost Root Port
1        0.f474-880e-6554     200200      0           GigabitEthernet1/0/1
```

表 8-9 コマンド出力

フィールド	説明
ExtPathCost	外部パスコストです。装置は自動的にポートのデフォルトパスコストを計算します。あるいはポートのパスコストを設定するために**stp cost** コマンドを使用することができます。
IntPathCost	内部パスコストです。装置は自動的にポートのデフォルトパスコストを計算します。あるいはポートのパスコストを設定するために**stp cost** コマンドを使用することができます。
Root Port	ルートポート名です。（装置のポートがMSTIのルートポートである場合のみ表示されます）

8.1.11 display stp tc

Syntax

display stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **tc** [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

instance *instance-list*: MSTI を指定します。半角スペースで区切り 10 まで設定するか、MSTI の範囲で設定することができます。MSTI を範囲で指定する形式は *instance-id1* [**to**

instance-id2]です。*instance-id2* は *instance-id1* 以上の値にしてください。設定範囲は 0～4094 です。0 は CIST を示します。

vlan *vlan-id-list*: VLAN を指定します。半角スペースで区切り 10 まで設定するか、VLAN の範囲で設定することができます。VLAN を範囲で指定する形式は *vlan-id1* [**to** *vlan-id2*] です。*vlan-id2* は *vlan-id1* 以上の値にしてください。設定範囲は 1～4094 です。

slot *slot-number*: IRF スタックメンバ装置を指定します。*slot-number* は IRF スタックメンバ装置の ID を示します。指定しない場合、IRF スタックユニットのすべてのメンバ装置に適用されます。

説明

display stp tc コマンドはポートで送受信する TC/TCN BPDU の統計情報を表示します。

STP あるいは RSTP モードでは、出力はポート名の順番で表示されます。

PVST モード：コマンド出力は VLAN ID と各 VLAN のポート名の順番で表示されます。

- VLAN を指定しない場合、すべての VLAN に適用されます。
- VLAN リストを指定した場合、指定した VLAN に適用されます。

MSTP モード：コマンド出力は MSTI ID と各 MSTI のポート名の順番で表示されます。

- MSTI を指定しない場合、すべての MSTI に適用されます。
- MSTI リストを指定した場合、指定した MSTI に適用されます。

例

MSTP モードで MSTI 0 の IRF スタックメンバ装置 1 のすべてのポートで送受信する TC/TCN BPDU の統計情報を表示します。

<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
```

PVST モードで VLAN 2 の IRF スタックメンバ装置 1 のすべてのポートで送受信する TC/TCN BPDU の統計情報を表示します。

<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
```

表 8-10 コマンド出力

フィールド	説明
Port	ポート名です。

フィールド	説明
Receive	各ポートが受信したTC/TCN BPDUの数です。
Send	各ポートが送信したTC/TCN BPDUの数です。

8.1.12 instance

Syntax

instance *instance-id* **vlan** *vlan-id-list*

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

デフォルト

CIST

View

MST region view

定義済みユーザロール

network-admin

パラメータ

instance-list: MSTI ID を指定します。設定範囲は 0～4094 です。0 は CIST を示します。コマンドの設定範囲は 1～4094 です。

vlan *vlan-id-list*: VLAN を指定します。半角スペースで区切り 10 まで設定するか、VLAN の範囲で設定することができます。VLAN を範囲で指定する形式は *vlan-id1* [**to** *vlan-id2*] です。*vlan-id2* は *vlan-id1* 以上の値にしてください。設定範囲は 1～4094 です。

説明

注意：

以下の状況下でグローバル Digest Snooping を使用する場合、注意してください。

- VLAN-インスタンスマッピングを修正します。
- デフォルトの MST リージョンの設定に戻します。

もしローカル装置が隣接装置と異なる VLAN-インスタンスマッピングを持っている場合、ループあるいはトラフィックの中断が発生します。

instance コマンドは VLAN のリストを MSTI にマッピングします。

undo instance コマンドは指定した VLAN あるいはすべての VLAN を CIST（MSTI 0）に再マッピングします。

undo instance コマンドで VLAN を指定しない場合、指定された MSTI にマッピングされたすべての VLAN は CIST に再マッピングされます。

同一の VLAN を異なる MSTI にマッピングすることはできません。インスタンスにマッピングされている VLAN を新たなインスタンスにマッピングすると、古いマッピングは自動的に削除されます。

VLAN-インスタンスマッピングを最大 65 の MSTI にマッピングすることができます。

このコマンドを設定した後、VLAN-インスタンスマッピングをアクティブにするため、**active region-configuration** コマンドを実行します。

例

VLAN 2 を MSTI 1 にマッピングします。

<Switch> system-view

[Switch] stp region-configuration

[Switch-mst-region] instance 1 vlan 2

関連コマンド

- **active region-configuration**
- **check region-configuration**
- **display stp region-configuration**

8.1.13 region-name

Syntax

region-name *name*

undo region-name

デフォルト

装置の MST リージョン名は MAC アドレスです。

View

MST region view

定義済みユーザロール

network-admin

パラメータ

name: MST リージョン名を指定します。設定範囲は 1～32 です。

説明

region-name コマンドは MST リージョン名を設定します。

undo region-name コマンドはデフォルトに戻します。

装置の MST リージョンは、装置の MST リージョン名、VLAN-インスタンスマッピングテーブルおよび MSTP リビジョンレベルによって決まります。

このコマンドを設定した後、MST リージョン名をアクティブにするため、**active region-configuration** コマンドを実行します。

例

装置の MST リージョン名を hello に設定します。

<Switch> system-view

[Switch] stp region-configuration

[Switch-mst-region] region-name hello

関連コマンド

- **active region-configuration**
- **check region-configuration**
- **display stp region-configuration**
- **instance**
- **revision-level**
- **vlan-mapping modulo**

8.1.14 reset stp

Syntax

reset stp [**interface** *interface-list*]

View

User view

定義済みユーザロール

network-admin

パラメータ

interface *interface-list*: インタフェースを指定します。半角スペースで区切り 10 まで設定するか、インタフェースの範囲で設定することができます。インタフェースを範囲で指定する形式は *interface-type interface-number1* [**to** *interface-type interface-number2*] です。*interface-number2* は *interface-number1* 以上の値にしてください。指定しない場合、すべてのポートのスパニングツリーに関する統計情報を削除します。

説明

reset stp コマンドはスパニングツリーの統計情報を削除します。スパニングツリーの統計情報は、TCN BPDU の数、configuration BPDU、RST BPDU、および指定したポートで送受信された MST BPDU が含まれます。

例

GigabitEthernet 1/0/1～GigabitEthernet 1/0/3 のスパニングツリーの統計情報を削除します。

<Switch> reset stp interface gigabitethernet 1/0/1 to gigabitethernet 1/0/3

関連コマンド

display stp

8.1.15 revision-level

Syntax

revision-level *level*

undo revision-level

デフォルト

0

View

MST region view

定義済みユーザロール

network-admin

パラメータ

level: MSTP リビジョンレベルを指定します。設定範囲は 0～65535 です。

説明

revision-level コマンドは MSTP リビジョンレベルを設定します。

undo revision-level コマンドはデフォルトに戻します。

装置の MSTP リビジョンレベル、MST リージョン名、VLAN-インスタンスマッピングテーブルは、装置の MST リージョンによって決まります。

このコマンドを設定した後、MST リージョン名をアクティブにするため、**active region-configuration** コマンドを実行します。

例

MST リージョンの MSTP リビジョンレベルを 5 に設定します。

<Switch> system-view

[Switch] stp region-configuration

[Switch-mst-region] revision-level 5

関連コマンド

- **active region-configuration**
- **check region-configuration**
- **display stp region-configuration**
- **instance**
- **region-name**
- **vlan-mapping modulo**

8.1.16 snmp-agent trap enable stp

Syntax

snmp-agent trap enable stp [**new-root** | **tc**]

undo snmp-agent trap enable stp [**new-root** | **tc**]

デフォルト

新規ルートブリッジの選択イベントが発生した場合、SNMP notification の送信は無効です。

MSTP モードでは、スパニングツリーのトポロジの変更が発生した場合、MSTI 0 の SNMP notification の送信は有効です。ほかの MSTI の SNMP notification の送信は無効です。

PVST モードでは、すべての VLAN のスパニングツリーのトポロジの変更が発生した場合、SNMP notification の送信は無効です。

View

System view

定義済みユーザロール

network-admin

パラメータ

new-root: 装置が新しいルートブリッジとして選択された場合、SNMP notification の送信を有効にします。このパラメータは動作モードが STP モード、MSTP モード、RSTP モードであるときのみ有効です。

tc: 装置が TCN BPDU を受信すると trap の送信を有効にします。このパラメータは動作モードが PVST モードであるときのみ有効です。

説明

snmp-agent trap enable stp コマンドは新規ルートブリッジの選択イベントあるいはスパニングツリートポロジの変更が発生すると SNMP notification の送信を有効にします。

undo snmp-agent trap enable stp コマンドは新規ルートブリッジの選択イベントあるいはスパニングツリーのトポロジの変更が発生すると SNMP notification の送信を無効にします。

パラメータを指定しない場合、**snmp-agent trap enable stp** コマンドは、以下のように動作モードによって、適用されるイベントが異なります。

- STP、MSTP、RSTP モードでは、新規ルートブリッジの選択イベントが発生すると、コマンドは SNMP notification の送信を適用します。
- PVST モードでは、スパニングツリーのトポロジの変更が発生すると、コマンドは SNMP notification の送信を適用します。

例

新規ルートブリッジの選択イベントが発生すると、SNMP notification の送信を有効にします。

<Switch> system-view

[Switch] snmp-agent trap enable stp new-root

8.1.17 stp bpdu-protection

Syntax

stp bpdu-protection

undo stp bpdu-protection

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

stp bpdu-protection コマンドはグローバルで BPDU ガード機能を有効にします。

undo stp bpdu-protection コマンドはグローバルで BPDU ガード機能を無効にします。

例

グローバルで BPDU ガード機能を有効にします。

<Switch> system-view

[Switch] stp bpdu-protection

関連コマンド

- **stp edged-port**
- **stp port bpdu-protection**

8.1.18 stp bridge-diameter

Syntax

stp [**vlan** *vlan-id-list*] **bridge-diameter** *diameter*

undo stp [**vlan** *vlan-id-list*] **bridge-diameter**

デフォルト

7

View

System view

定義済みユーザロール

network-admin

パラメータ

vlan *vlan-id-list*: VLAN を指定します。半角スペースで区切り 10 まで設定するか、VLAN の範囲で設定することができます。VLAN を範囲で指定する形式は *vlan-id1* [**to** *vlan-id2*] です。*vlan-id2* は *vlan-id1* 以上の値にしてください。設定範囲は 1～4094 です。STP、RSTP、MSTP では使用しません。

diameter: スイッチネットワークのダイアメータを指定します。設定範囲は 2～7 です。

説明

stp bridge-diameter コマンドはスイッチネットワークのネットワークダイアメータを設定します。ネットワークダイアメータは、端末装置がルートブリッジを経由して、スイッチネットワーク上の別の端末装置に到達するためのステーションの最大数を示します。

undo stp bridge-diameter コマンドはデフォルトに戻します。

Hello 時間、転送遅延、最大エージング時間を適切に設定するとネットワーク収束の速度を上げることができます。これらのタイマの値はネットワークサイズに関連しています。ネットワークダイアメータを設定することで、これら 3 つのタイマを間接的に設定する

ことができます。ネットワークダイアメータが 7（デフォルト値）に設定されていると、3 つのタイマもデフォルトに設定されます。

STP、RSTP、MSTP モードでは、各 MST リージョンは装置と認識され、CIST（あるいは共通ルートブリッジ）のみ適用することができます。

PVST モードでは、指定した VLAN のルートブリッジのみ適用することができます。

例

MSTP モードでスイッチネットワークのネットワークダイアメータを 5 に設定します。

<Switch> system-view

[Switch] stp bridge-diameter 5

MSTP モードでスイッチネットワークの VLAN 2 のネットワークダイアメータを 5 に設定します。

<Switch> system-view

[Switch] stp vlan 2 bridge-diameter 5

関連コマンド

- **stp timer forward-delay**
- **stp timer hello**
- **stp timer max-age**

8.1.19 stp compliance

Syntax

stp compliance { **auto** | **dot1s** | **legacy** }

undo stp compliance

デフォルト

auto

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

auto: ポートが自動で MSTP BPDU フォーマットを認識し、それに従って送信する MSTP BPDU のフォーマットを決定するよう設定します。

dot1s: ポートが標準フォーマット（802.1s 準拠）の MSTP BPDU のみ送受信するよう設定します。

legacy: ポートが互換性のあるフォーマットの MSTP BPDU のみを送受信するよう設定します。

説明

stp compliance コマンドは指定したポートが MSTP BPDU の認識および送信に使用するモードを設定します。

undo stp compliance コマンドはデフォルトに戻します。

interface view で設定を行うと、設定は、現在のインタフェースでのみ有効になります。

aggregate interface view で設定を行うと、設定はアグリゲートインタフェースでのみ有効になります。

アグリゲーショングループのメンバポートで設定を行うと、ポートがアグリゲーショングループを除外した後に有効になります。

例

GigabitEthernet 1/0/1 が標準フォーマット（802.1s）の MSTP パケットのみを送信するよう設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] stp compliance dot1s

8.1.20 stp config-digest-snooping

Syntax

stp config-digest-snooping

undo stp config-digest-snooping

デフォルト

無効

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

stp config-digest-snooping コマンドは Digest Snooping を有効にします。

undo stp config-digest-snooping コマンドは Digest Snooping を無効にします。

この設定はグローバル、およびほかのベンダの装置に接続されたポートの両方で有効にする必要があります。影響を最小限にするため、グローバルで有効にする前に関連したポートの機能を有効にしてください。

interface view で設定を行うと、設定は、現在のインタフェースでのみ有効になります。

aggregate interface view で設定を行うと、設定はアグリゲートインタフェースでのみ有効になります。

アグリゲーショングループのメンバポートで設定を行うと、ポートがアグリゲーショングループを除外した後に有効になります。

例

Digest Snooping を GigabitEthernet 1/0/1 とグローバルで有効にします。

<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

関連コマンド

- **display stp**
- **stp global config-digest-snooping**

8.1.21 stp cost

Syntax

stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **cost** *cost-value*

undo stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **cost**

デフォルト

装置は各スパニングツリーのポートのパスコストを、対応する標準にもとづいて自動的に計算します。

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

instance *instance-list*: MSTI を指定します。半角スペースで区切り 10 まで設定するか、MSTI の範囲で設定することができます。MSTI を範囲で指定する形式は *instance-id1* [**to** *instance-id2*]です。*instance-id2* は *instance-id1* 以上の値にしてください。設定範囲は 0～4094 です。0 は CIST を示します。

vlan *vlan-id-list*: VLAN を指定します。半角スペースで区切り 10 まで設定するか、VLAN の範囲で設定することができます。VLAN を範囲で指定する形式は *vlan-id1* [**to** *vlan-id2*] です。*vlan-id2* は *vlan-id1* 以上の値にしてください。設定範囲は 1～4094 です。

cost-value: ポートのパスコストを指定します。設定範囲は、採用されているパスコスト計算基準によって決まります。

- パスコスト計算に IEEE 802.1d-1998 が選択されている場合、設定範囲は 1～65535 です。
- パスコスト計算に IEEE 802.1t が選択されている場合、設定範囲は 1～200000000 です。
- パスコスト計算にプライベート標準が選択されている場合、コスト範囲は 1～200000 です。

説明

stp cost コマンドはポートのパスコストを設定します。

undo stp cost コマンドはデフォルトに戻します。

パスコストはスパニングツリー計算を行う際の重要な要素です。MSTI のポートに異なるパスコストを設定すると、VLAN トラフィックのフローが異なる物理的リンクを通って転送され、VLAN ベースのロードバランスを行うことができます

ポートのパスコストの設定はポートのロール役割に影響します。ポートのロール役割が変更されたとき、システムはポートのロール役割を計算し、状態遷移を開始します。

interface view で設定を行うと、設定は、現在のインタフェースでのみ有効になります。

aggregate interface view で設定を行うと、設定はアグリゲートインタフェースでのみ有効になります。

アグリゲーショングループのメンバポートで設定を行うと、ポートがアグリゲーショングループを除外した後に有効になります。

MSTI あるいは VLAN を指定しない場合、このコマンドは MSTP CIST あるいは STP、RSTP スパニングツリーのポートのパスコストを設定します。

例

MSTP モードで MSTI 2 の GigabitEthernet 1/0/1 のパスコストを 200 に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] stp instance 2 cost 200

PVST モードで VLAN 2 の GigabitEthernet 1/0/1 のパスコストを 200 に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] stp vlan 2 cost 200

関連コマンド

- **display stp**
- **stp pathcost-standard**

8.1.22 stp dispute-protection

Syntax

stp dispute-protection

undo stp dispute-protection

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

stp dispute-protection コマンドは Dispute Guard を有効にします。

undo stp dispute-protection コマンドは Dispute Guard を無効にします。

スパニングツリー機能によってポートで単方向リンクが検出された場合、ポートをブロックしてループを防止します。

一部の VLAN ネットワークでは、ダウンストリーム装置のアップリンクポートが PVID からのパケットを拒否するように設定されています。その結果、ダウンストリーム装置はアップストリーム装置から PVID の BPDU を受信できません。

ただし、アップストリーム装置はダウンストリーム装置から BPDU を受信できます。この場合、Dispute Guard はアップストリーム装置の受信ポートをブロックし、トラフィックの中断を引き起こします。

サービスの継続性を確保し、リンクがブロックされないようにするには、**undo stp dispute-protection** コマンドを使用して Dispute Guard を無効にします。

例

Dispute guard を無効にします。

<Switch> system-view

[Switch] undo stp dispute-protection

8.1.23 stp edged-port

Syntax

stp edged-port

undo stp edged-port

デフォルト

すべてのポートは非エッジポートです。

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

stp edged-port コマンドはポートを Edge ポートに設定します。

undo stp edged-port コマンドはポートをデフォルトに戻します。

Edge ポートとは、ほかの Ethernet スイッチや共有ネットワークセグメントに接続されず、ユーザ端末等に直接接続しているポートを示します。ネットワークトポロジが変化した場合、Edge ポートは一時的なループを起こしません。ポートを Edge ポートとして設定すると、そのポートは早急に転送状態に遷移することができます。ユーザ端末に直接接続されているポートを Edge ポートとして設定することを推奨します。

通常、Edge ポートはほかの装置に接続されていないため、ほかの装置からの configuration BPDU は、Edge ポートには到達しません。BPDU ガード機能が無効であるとき、configuration BPDU を受信すると、Edge ポートとして設定されたポートは非 Edge ポートとして動作します。

ポートでループガード機能と Edge ポートの設定は同時に設定することはできません。

interface view で設定を行うと、設定は、現在のインタフェースでのみ有効になります。

aggregate interface view で設定を行うと、設定はアグリゲートインタフェースでのみ有効になります。

アグリゲーショングループのメンバポートで設定を行うと、ポートがアグリゲーショングループを除外した後に有効になります。

例

GigabitEthernet 1/0/1 を Edge ポートとして設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] stp edged-port

関連コマンド

- **stp bpdu-protection**
- **stp loop-protection**
- **stp port bpdu-protection**
- **stp root-protection**

8.1.24 stp enable

Syntax

stp enable

undo stp enable

デフォルト

有効

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

stp enable コマンドはスパニングツリー機能を有効にします。

undo stp enable コマンドはスパニングツリー機能を無効にします。

スパニングツリー機能を有効にしたとき、装置はスパニングツリーのモードの設定に従い STP、RSTP、PVST、MSTP モードで動作します。

スパニングツリー機能を有効にしたとき、装置は受信した configuration BPDU にもとづいて VLAN のスパニングツリーの状態を自動で維持します。スパニングツリー機能を無効にしたとき、装置はスパニングツリーの状態の維持を停止します。

interface view で設定を行うと、設定は、現在のインタフェースでのみ有効になります。

aggregate interface view で設定を行うと、設定はアグリゲートインタフェースでのみ有効になります。

アグリゲーショングループのメンバポートで設定を行うと、ポートがアグリゲーショングループを除外した後に有効になります。

例

MSTP モードで、GigabitEthernet 1/0/1 のスパニングツリー機能を無効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] undo stp enable

関連コマンド

- **stp global enable**
- **stp mode**
- **stp vlan enable**

8.1.25 stp global config-digest-snooping

Syntax

stp global config-digest-snooping

undo stp global config-digest-snooping

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

stp global config-digest-snooping コマンドはグローバルで Digest Snooping を有効にします。

undo stp global config-digest-snooping コマンドはグローバルで Digest Snooping を無効にします。

この設定はグローバル、およびほかのベンダの装置に接続されたポートの両方で有効にする必要があります。影響を最小限にするため、グローバルで有効にする前に関連したポートの機能を有効にしてください。

例

Digest Snooping を GigabitEthernet 1/0/1 とグローバルで有効にします。

<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

関連コマンド

- **display stp**
- **stp config-digest-snooping**

8.1.26 stp global enable

Syntax

stp global enable

undo stp global enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

stp global enable コマンドはスパニングツリー機能をグローバルで有効にします。

undo stp global enable コマンドはスパニングツリー機能をグローバルで無効にします。

スパニングツリー機能を有効にしたとき、スパニングツリーのモードの設定により装置は STP、RSTP、PVST、MSTP モードで動作します。

スパニングツリー機能が有効であるとき、装置は受信した configuration BPDU にもとづいて VLAN のスパニングツリーの状態を維持します。スパニングツリー機能が無効であるとき、装置はスパニングツリーの状態の維持を停止します。

例

スパニングツリー機能をグローバルで有効にします。

<Switch> system-view

[Switch] stp global enable

関連コマンド

- **stp enable**
- **stp mode**

8.1.27 stp global mcheck

Syntax

stp global mcheck

View

System view

定義済みユーザロール

network-admin

説明

stp global mcheck コマンドはグローバルで mCheck を実行します。

MSTP、RSTP、PVST のポートが STP 装置に接続し、STP BPDU を受信すると、ポートは自動で STP モードに遷移します。しかし以下の状況ではポートは自動でもとのモードに戻ることができません。

- ピアの STP 装置がシャットダウンあるいは削除されたとき。
- ポートが変更を検出できないとき。

この場合、mCheck を実行して、ポートをもとのモードに強制的に移行させることができます。

スパニングツリーのモードの設定により装置は STP、RSTP、PVST、MSTP モードで動作します。

装置が MSTP、RSTP、PVST モードで動作しているときのみ **stp global mcheck** コマンドが適用されます。

例

グローバルで mCheck を実行します。

<Switch> system-view

[Switch] stp global mcheck

関連コマンド

- **stp mcheck**
- **stp mode**

8.1.28 stp ignore-pvid-inconsistency

Syntax

stp ignore-pvid-inconsistency

undo stp ignore-pvid-inconsistency

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

stp ignore-pvid-inconsistency コマンドは一貫性のない PVID 保護を無効にします。

undo stp ignore-pvid-inconsistency コマンドは一貫性のない PVID 保護を有効にします。

このコマンドは、装置が PVST モードで動作している場合にのみ有効です。

一貫性のない PVID 保護を無効にすると、スパニングツリーの計算エラーが発生する可能性があります。このようなエラーを回避するには、次の要件を満たしていることを確認します。

- ある装置の VLAN が、別の装置のピアポート(デフォルト VLAN を除く)の PVID と同じ ID を使用していないことを確認します。
- ローカルポートまたはそのピアがハイブリッドポートである場合は、ローカルポートとピアポートを同じ VLAN のタグ無メンバとして設定しないでください。
- ローカル装置とピア装置の両方で、矛盾する PVID 保護を無効にします。

例

PVST モードでは、不整合のある PVID 保護機能を無効にします。

<Switch> system-view

[Switch] stp mode pvst

[Switch] stp ignore-pvid-inconsistency

8.1.29 stp log enable tc

Syntax

stp log enable tc

undo stp log enable tc

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

stp log enable tc コマンドは、PVST モードで TCN BPDU を検出したとき、あるいは受信したとき、装置でログを作成することを有効にします。

undo stp log enable tc コマンドはデフォルトに戻します。

stp log enable tc コマンドは PVST モードでのみ適用します。

例

PVST モードで TCN BPDU を検出したとき、あるいは受信したとき、装置でログを作成することを有効にします。

<Switch> system-view

[Switch] stp log enable tc

8.1.30 stp loop-protection

Syntax

stp loop-protection

undo stp loop-protection

デフォルト

無効

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

stp loop-protection コマンドはポートのループガード機能を有効にします。

undo stp loop-protection コマンドはポートのループガード機能を無効にします。

ポートのループガード機能はルートガード機能あるいは Edge ポートの設定を同時に設定することはできません。

interface view で設定を行うと、設定は、現在のインタフェースでのみ有効になります。

aggregate interface view で設定を行うと、設定はアグリゲートインタフェースでのみ有効になります。

アグリゲーショングループのメンバポートで設定を行うと、ポートがアグリゲーショングループを除外した後に有効になります。

例

GigabitEthernet 1/0/1 のループガード機能を有効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] stp loop-protection

関連コマンド

- **stp edged-port**
- **stp root-protection**

8.1.31 stp max-hops

Syntax

stp max-hops *hops*

undo stp max-hops

デフォルト

20

View

System view

定義済みユーザロール

network-admin

パラメータ

hops: 最大ホップ数を設定します。設定範囲は 1～40 です。

説明

stp max-hops コマンドは MST リージョンの最大ホップ数を設定します。

undo stp max-hops コマンドはデフォルトに戻します。

例

MST リージョンの最大ホップ数を 35 に設定します。

<Switch> system-view

[Switch] stp max-hops 35

関連コマンド

display stp

8.1.32 stp mcheck

Syntax

stp mcheck

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

stp mcheck コマンドはポートで mCheck を実行します。

MSTP、RSTP、PVST のポートが STP 装置に接続し、STP BPDU を受信すると、ポートは自動で STP モードに遷移します。しかし以下の状況ではポートは自動でもとのモードに戻ることができません。

- ピアの STP 装置がシャットダウンあるいは削除されたとき。
- ポートが変更を検出できないとき。

この場合、mCheck オペレーションを実行して、ポートをもとのモードに強制的に移行させることができます。

たとえば、デバイス A、デバイス B、デバイス C が一列に接続されています。デバイス A は STP を動作し、デバイス B はスパニングツリープロトコルが動作しておらず、デバイス C は RSTP、MSTP あるいは PVST で動作します。デバイス C がデバイス B から透過的に転送された STP BPDU を受信すると、受信したポートは STP モードに遷移します。デバイス B をデバイス C と RSTP、MSTP、PVST で動作するように設定した場合、デバイス B とデバイス C に接続しているポートで mCheck を実行します。

スパニングツリーのモードの設定により装置は STP、RSTP、PVST、MSTP モードで動作します。

装置が MSTP、RSTP、PVST モードで動作しているときのみ **stp mcheck** コマンドが適用されます。

interface view で設定を行うと、設定は、現在のインタフェースでのみ有効になります。

aggregate interface view で設定を行うと、設定はアグリゲートインタフェースでのみ有効になります。

アグリゲーショングループのメンバポートで設定を行うと、ポートがアグリゲーショングループを除外した後に有効になります。

例

GigabitEthernet 1/0/1 で mCheck を実行します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] stp mcheck

関連コマンド

- **stp global mcheck**
- **stp mode**

8.1.33 stp mode

Syntax

stp mode { **mstp** | **pvst** | **rstp** | **stp** }

undo stp mode

デフォルト

mstp

View

System view

定義済みユーザロール

network-admin

パラメータ

mstp: MSTP モードで動作するように設定します。

pvst: PVST モードで動作するように設定します。

rstp: RSTP モードで動作するように設定します。

stp: STP モードで動作するように設定します。

説明

stp mode コマンドはスパニングツリーの動作モードを設定します。

undo stp mode コマンドはデフォルトに戻します。

MSTP モードは RSTP モードと互換性があります。RSTP モードは STP モードと互換性があります。

PVST モードの互換性はポートのリンクタイプに依存します。

- **アクセスポート**－PVST モードはすべての VLAN でほかのスパニングツリーと互換性があります。
- **トランクポートあるいはハイブリッドポート**－PVST モードは、デフォルト VLAN でほかのスパニングツリーと互換性があります。

例

スパニングツリーの動作モードを STP に設定します。

<Switch> system-view

[Switch] stp mode stp

関連コマンド

- **stp enable**
- **stp global enable**
- **stp global mcheck**
- **stp mcheck**
- **stp vlan enable**

8.1.34 stp no-agreement-check

Syntax

stp no-agreement-check

undo stp no-agreement-check

デフォルト

無効

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

stp no-agreement-check コマンドはポートの No Agreement Check（高速切り替え）機能を有効にします。

undo stp no-agreement-check コマンドはポートの No Agreement Check（高速切り替え）機能を無効にします。

このコマンドはルートポートでのみ有効です。

interface view で設定を行うと、設定は、現在のインタフェースでのみ有効になります。

aggregate interface view で設定を行うと、設定はアグリゲートインタフェースでのみ有効になります。

アグリゲーショングループのメンバポートで設定を行うと、ポートがアグリゲーショングループを除外した後に有効になります。

例

GigabitEthernet 1/0/1 の No Agreement Check（高速切り替え）機能を有効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] stp no-agreement-check

8.1.35 stp pathcost-standard

Syntax

stp pathcost-standard { **dot1d-1998** | **dot1t** | **legacy** }

undo stp pathcost-standard

デフォルト

legacy

View

System view

定義済みユーザロール

network-admin

パラメータ

dot1d-1998: IEEE 802.1d-1998 規格にもとづいて、ポートのデフォルトパスコストを計算します。

dot1t: IEEE 802.1t 規格にもとづいて、ポートのデフォルトパスコストを計算します。

legacy: 独自の規格にもとづいて、ポートのデフォルトパスコストを計算します。

説明

stp pathcost-standard コマンドはポートのデフォルトパスコストを計算するときに使用する装置の規格を指定します。

undo stp pathcost-standard コマンドはデフォルトに戻します。

装置がデフォルトパスコストの計算に使用する規格を変更すると、ポートパスコストの値はデフォルトに戻ります。

例

IEEE 802.1d-1998 規格にもとづいて、ポートのデフォルトパスコストを計算するように設定します。

<Switch> system-view

[Switch] stp pathcost-standard dot1d-1998

関連コマンド

- **display stp**
- **stp cost**

8.1.36 stp point-to-point

Syntax

stp point-to-point { **auto** | **force-false** | **force-true** }

undo stp point-to-point

デフォルト

デフォルトは auto で、スパニングツリーの装置は自動でポートがポイントツーポイントのリンクに接続するかどうか検出します。

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

auto: リンクタイプの自動検出を指定します。

force-false: 非ポイントツーポイントのリンクタイプを指定します。

force-true: ポイントツーポイントのリンクタイプを指定します。

説明

stp point-to-point コマンドはポートのリンクタイプを設定します。

undo stp point-to-point コマンドはデフォルトに戻します。

非ポイントツーポイントリンクに接続している場合、ポートは高速でステート遷移することはできません。

現在のポートがアグリゲーションインタフェースあるいは full の動作モードで動作しているポートである場合、ポートをポイントツーポイントリンクとしてリンクタイプを設定することができます。装置が自動でリンク状態を検出するよう、デフォルト設定を使用することを推奨します。

MSTP モードあるいは PVST モードで **stp point-to-point force-false** コマンドあるいは **stp point-to-point force-true** コマンドが設定されたポートはすべての MSTI あるいは VLAN で有効です。

ポートに接続している物理的リンクがポイントツーポイントリンクではないとき、ポート強制的にポイントツーポイントリンクになるよう設定した場合、一時的なループが発生することがあります。

interface view で設定を行うと、設定は、現在のインタフェースでのみ有効になります。

aggregate interface view で設定を行うと、設定はアグリゲートインタフェースでのみ有効になります。

アグリゲーショングループのメンバポートで設定を行うと、ポートがアグリゲーショングループを除外した後に有効になります。

例

GigabitEthernet 1/0/3 をポイントツーポイントリンクとして接続するよう設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] stp point-to-point force-true

関連コマンド

display stp

8.1.37 stp port bpdu-protection

Syntax

stp port bpdu-protection { **enable** | **disable** }

undo port stp bpdu-protection

デフォルト

edge ポートに設定されていません。インタフェースの BPDU ガード機能の状態はグローバルでの BPDU ガード機能と同一です。

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

enable: BPDU ガード機能を有効にします。

disable: BPDU ガード機能を無効にします。

説明

stp port bpdu-protection コマンドはインタフェースで BPDU ガード機能を有効にします。

undo port stp bpdu-protection コマンドはデフォルトに戻します。

Ethernet interface view で設定した場合、インタフェースでのみ有効です。

aggregate interface view で設定した場合、アグリゲートインタフェースでのみ有効です。

アグリゲーショングループのメンバポートで設定されている場合、ポートをアグリゲーショングループから削除したのち適用されます。

例

GigabitEthernet 1/0/1 で BPDU ガード機能を有効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] stp port bpdu-protection enable

関連コマンド

- **stp bpdu-protection**
- **stp edged-port**

8.1.38 stp port priority

Syntax

stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **port priority** *priority*

undo stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **port priority**

デフォルト

128

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

instance *instance-list*: MSTI を指定します。半角スペースで区切り 10 まで設定するか、MSTI の範囲で設定することができます。MSTI を範囲で指定する形式は *instance-id1* [**to** *instance-id2*]です。*instance-id2* は *instance-id1* 以上の値にしてください。設定範囲は 0～4094 です。0 は CIST を示します。

vlan *vlan-id-list*: VLAN を指定します。半角スペースで区切り 10 まで設定するか、VLAN の範囲で設定することができます。VLAN を範囲で指定する形式は *vlan-id1* [**to** *vlan-id2*] です。*vlan-id2* は *vlan-id1* 以上の値にしてください。設定範囲は 1～4094 です。

priority: ポートのプライオリティを指定します。設定範囲は 0～240 で、16 の倍数です。（0、16、32、・・・のように設定します）

説明

stp port priority コマンドはポートのプライオリティを設定します。ポートのプライオリティはスパニングツリーのポートの役割に影響します。

undo stp port priority コマンドはデフォルトに戻します。

priority を小さい値にするとポートのプライオリティが高くなります。装置上のすべてのプライオリティが同一である場合、プライオリティの値はポートインデックスに依存します。インデックスが小さいとプライオリティが高くなります。

interface view で設定を行うと、設定は、現在のインタフェースでのみ有効になります。

aggregate interface view で設定を行うと、設定はアグリゲートインタフェースでのみ有効になります。

アグリゲーショングループのメンバポートで設定を行うと、ポートがアグリゲーショングループを除外した後に有効になります。

MSTI あるいは VLAN を指定しない場合、MSTP CIST、STP あるいは RSTP のポートのプライオリティを設定します。

例

MSTP モードで MSTI 2 の GigabitEthernet 1/0/1 のプライオリティを 16 に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] stp instance 2 port priority 16

PVST モードで VLAN 2 の GigabitEthernet 1/0/1 のプライオリティを 16 に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] stp vlan 2 port priority 16

関連コマンド

display stp

8.1.39 stp port shutdown permanent

Syntax

stp port shutdown permanent

undo stp port shutdown permanent

デフォルト

無効

Views

System view

定義済みユーザロール

network-admin

説明

stp port shutdown permanent コマンドで BPDU ガードによって shutdown されたエッジポートの再活性化をしないように設定します。

undo stp port shutdown permanent コマンドでデフォルトに戻します。

本コマンドにより shutdown されたポートを再活性化するには、**undo shutdown** コマンドの実行が必要です。

例

BPDU ガードによって shutdown されたエッジポートの再活性化をできなくします。

<Switch> system-view

[Switch] stp port shutdown permanent

8.1.40 stp port-log

Syntax

stp port-log { **all** | **instance** *instance-list* | **vlan** *vlan-id-list* }

undo stp port-log { **all** | **instance** *instance-list* | **vlan** *vlan-id-list* }

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

パラメータ

all: すべての MSTI あるいは VLAN を指定します。

instance *instance-list*: MSTI を指定します。半角スペースで区切り 10 まで設定するか、MSTI の範囲で設定することができます。MSTI を範囲で指定する形式は *instance-id1* [**to** *instance-id2*]です。*instance-id2* は *instance-id1* 以上の値にしてください。設定範囲は 0～4094 です。0 は CIST を示します。

vlan *vlan-id-list*: VLAN を指定します。半角スペースで区切り 10 まで設定するか、VLAN の範囲で設定することができます。VLAN を範囲で指定する形式は *vlan-id1* [**to** *vlan-id2*] です。*vlan-id2* は *vlan-id1* 以上の値にしてください。設定範囲は 1～4094 です。

説明

stp port-log コマンドはポート状態の遷移情報の出力を有効にします。

undo stp port-log コマンドはポート状態の遷移情報の出力を無効にします。

例

MSTP モードで MSTI 2 のポート状態の遷移情報の出力を有効にします。

<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.
```

出力では、MSTI 2 において GigabitEthernet 1/0/1 のポート状態が破棄に遷移し、GigabitEthernet 1/0/2 のポート状態が転送に遷移したことを示しています。

PVST モードで VLAN 1～VLAN 4094 のポート状態の遷移情報の出力を有効にします。

<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.
```

出力では、VLAN 2 において GigabitEthernet 1/0/1 のポート状態が破棄に遷移し、GigabitEthernet 1/0/2 のポート状態が転送に遷移したことを示しています。

8.1.41 stp priority

Syntax

stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **priority** *priority*

undo stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **priority**

デフォルト

32768

View

System view

定義済みユーザロール

network-admin

パラメータ

instance *instance-list*: MSTI を指定します。半角スペースで区切り 10 まで設定するか、MSTI の範囲で設定することができます。MSTI を範囲で指定する形式は *instance-id1* [**to** *instance-id2*]です。*instance-id2* は *instance-id1* 以上の値にしてください。設定範囲は 0～4094 です。0 は CIST を示します。

vlan *vlan-id-list*: VLAN を指定します。半角スペースで区切り 10 まで設定するか、VLAN の範囲で設定することができます。VLAN を範囲で指定する形式は *vlan-id1* [**to** *vlan-id2*] です。*vlan-id2* は *vlan-id1* 以上の値にしてください。設定範囲は 1～4094 です。

priority: 装置のプライオリティを指定します。設定範囲は 0～61440 で、4096 の倍数です（0、4096、8192・・・のように設定します）。装置で 16 までプライオリティを設定することができます。プライオリティの値を小さくすると、装置のプライオリティが高くなります。

説明

stp priority コマンドは装置のプライオリティを設定します。

undo stp priority コマンドはデフォルトのプライオリティに戻します。

MSTI あるいは VLAN を指定しない場合、MSTP CIST、STP あるいは RSTP のポートのプライオリティを設定します。

例

MSTI モードで MSTI 1 の装置のプライオリティを 4096 に設定します。

<Switch> system-view

[Switch] stp instance 1 priority 4096

PVST モードで VLAN 1 の装置のプライオリティを 4096 に設定します。

<Switch> system-view

[Switch] stp vlan 1 priority 4096

8.1.42 stp pvst-bpdu-protection

Syntax

stp pvst-bpdu-protection

undo stp pvst-bpdu-protection

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

stp pvst-bpdu-protection コマンドは PVST BPDU ガード機能を有効にします。

undo stp pvst-bpdu-protection コマンドは PVST BPDU ガード機能を無効にします。

ポートが PVST BPDU を受信する場合、MSTP が有効な装置はポートをシャットダウンします。シャットダウンしたポートは検出間隔が終了したのち、up となります。検出間隔を設定する場合、**shutdown-interval** コマンドを使用します。

例

MSTP モードで PVST BPDU ガード機能を有効にします。

<Switch> system-view

[Switch] stp pvst-bpdu-protection

関連コマンド

shutdown-interval (コマンドマニュアルのセクション 1 *はじめに “装置管理”*)

8.1.43 stp region-configuration

Syntax

stp region-configuration

undo stp region-configuration

デフォルト

MST リージョンのデフォルト設定は以下です。

- 装置の MST リージョン名は装置の MAC アドレスです。
- すべての VLAN は CIST にマッピングされています。
- MSTP のリージョンレベルは 0 です。

View

System view

定義済みユーザロール

network-admin

説明

stp region-configuration コマンドは MST region view に移行します。

undo stp region-configuration コマンドはデフォルトの MST リージョンの設定に戻します。

MST region view に移行した後、リージョン名、VLAN-インスタンスマッピング、レビジョンレベルを含む MST リージョンのパラメータを設定することができます。

例

MST region view に移行します。

<Switch> system-view

[Switch] stp region-configuration

[Switch-mst-region]

8.1.44 stp role-restriction

Syntax

stp role-restriction

undo stp role-restriction

デフォルト

無効

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

stp role-restriction コマンドはポート役割の制限機能を有効にします。

undo stp role-restriction コマンドはポート役割の制限機能を無効にします。

ポート役割の制限機能がポートで有効にした場合、ポートはルートポートにできません。

interface view で設定を行うと、設定は、現在のインタフェースでのみ有効になります。

aggregate interface view で設定を行うと、設定はアグリゲートインタフェースでのみ有効になります。

アグリゲーショングループのメンバポートで設定を行うと、ポートがアグリゲーショングループを除外した後に有効になります。

例

GigabitEthernet 1/0/1 のポート役割の制限機能を有効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] stp role-restriction

8.1.45 stp root primary

Syntax

stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **root primary**

undo stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **root**

デフォルト

装置はルートブリッジではありません。

View

System view

定義済みユーザロール

network-admin

パラメータ

instance *instance-list*: MSTI を指定します。半角スペースで区切り 10 まで設定するか、MSTI の範囲で設定することができます。MSTI を範囲で指定する形式は *instance-id1* [**to** *instance-id2*]です。*instance-id2* は *instance-id1* 以上の値にしてください。設定範囲は 0～4094 です。0 は CIST を示します。

vlan *vlan-id-list*: VLAN を指定します。半角スペースで区切り 10 まで設定するか、VLAN の範囲で設定することができます。VLAN を範囲で指定する形式は *vlan-id1* [**to** *vlan-id2*] です。*vlan-id2* は *vlan-id1* 以上の値にしてください。設定範囲は 1～4094 です。

説明

stp root primary コマンドは装置をルートブリッジとして設定します。

undo stp root コマンドはデフォルトに戻します。

装置をルートブリッジに指定した後は、装置のプライオリティを変更することはできません。

MSTI あるいは VLAN を指定しない場合、装置を MSTP CIST、STP あるいは RSTP のルートブリッジとして設定します。

例

MSTP モードで MSTI 1 のルートブリッジとして装置を指定します。

<Switch> system-view

[Switch] stp instance 1 root primary

PVST モードで VLAN 1 のルートブリッジとして装置を指定します。

<Switch> system-view

[Switch] stp vlan 1 root primary

関連コマンド

- **stp priority**
- **stp root secondary**

8.1.46 stp root secondary

Syntax

stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **root secondary**

undo stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **root**

デフォルト

装置はセカンダリルートブリッジではありません。

View

System view

定義済みユーザロール

network-admin

パラメータ

instance *instance-list*: MSTI を指定します。半角スペースで区切り 10 まで設定するか、MSTI の範囲で設定することができます。MSTI を範囲で指定する形式は *instance-id1* [**to** *instance-id2*]です。*instance-id2* は *instance-id1* 以上の値にしてください。設定範囲は 0～4094 です。0 は CIST を示します。

vlan *vlan-id-list*: VLAN を指定します。半角スペースで区切り 10 まで設定するか、VLAN の範囲で設定することができます。VLAN を範囲で指定する形式は *vlan-id1* [**to** *vlan-id2*] です。*vlan-id2* は *vlan-id1* 以上の値にしてください。設定範囲は 1～4094 です。

説明

stp root secondary コマンドは装置をセカンダリルートブリッジとして設定します。

undo stp root コマンドはデフォルトに戻します。

装置をルートブリッジに指定した後は、装置のプライオリティを変更することはできません。

MSTI あるいは VLAN を指定しない場合、装置を MSTP CIST、STP あるいは RSTP のセカンダリルートブリッジとして設定します。

例

MSTP モードで MSTI 1 のセカンダリルートブリッジとして装置を指定します。

<Switch> system-view

[Switch] stp instance 1 root secondary

PVST モードで VLAN 1 のセカンダリルートブリッジとして装置を指定します。

<Switch> system-view

[Switch] stp vlan 1 root secondary

関連コマンド

- **stp priority**
- **stp root primary**

8.1.47 stp root-protection

Syntax

stp root-protection

undo stp root-protection

デフォルト

無効

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

stp root-protection コマンドはポートでルートガード機能を有効にします。

undo stp root-protection コマンドはポートでルートガード機能を無効にします。

ポートのルートガード機能はループガード機能の設定を同時に設定することはできません。

interface view で設定を行うと、設定は、現在のインタフェースでのみ有効になります。

aggregate interface view で設定を行うと、設定はアグリゲートインタフェースでのみ有効になります。

アグリゲーショングループのメンバポートで設定を行うと、ポートがアグリゲーショングループを除外した後に有効になります。

例

GigabitEthernet 1/0/1 でルートガード機能を有効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] stp root-protection

関連コマンド

- **stp edged-port**
- **stp loop-protection**

8.1.48 stp tc-protection

Syntax

stp tc-protection

undo stp tc-protection

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

stp tc-protection コマンドは装置の TC-BPDU ガード機能を有効にします。

undo stp tc-protection コマンドは装置の TC-BPDU ガード機能を無効にします。

TC-BPDU ガードを有効にすると、最初に TC-BPDU を受信した後、10 秒ごとに、転送アドレスエントリを即座に削除する最大数を設定することができます。TC-BPDU を制限以上受信した場合、一定の期間が経過した後、装置は、転送アドレスエントリを削除します。これにより、頻繁に転送アドレスエントリの削除を行うことを防ぐことができます。

例

装置の TC-BPDU ガード機能を無効にします。

<Switch> system-view

[Switch] undo stp tc-protection

関連コマンド

stp tc-protection threshold

8.1.49 stp tc-protection threshold

Syntax

stp tc-protection threshold *number*

undo stp tc-protection threshold

デフォルト

6

View

System view

定義済みユーザロール

network-admin

パラメータ

number: TC-BPDU を受信した直後から、10 秒ごとに装置が即座に転送アドレスエントリを削除する最大の回数を指定します。設定範囲は 1～255 です。

説明

stp tc-protection threshold コマンドは TC-BPDU を受信した直後から 10 秒ごとに、装置が即座に転送アドレスエントリを削除する最大の回数を設定します。

undo stp tc-protection threshold コマンドはデフォルトに戻します。

例

10 秒ごとに装置が即座に転送アドレスエントリを削除する最大の回数を 10 に設定します。

<Switch> system-view

[Switch] stp tc-protection threshold 10

関連コマンド

stp tc-protection

8.1.50 stp tc-snooping

Syntax

stp tc-snooping

undo stp tc-snooping

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

stp tc-snooping コマンドは TC Snooping を有効にします。

undo stp tc-snooping コマンドは TC Snooping を無効にします。

TC Snooping とスパニングツリーは同時に設定することができません。TC Snooping を有効にする前に、グローバルでスパニングツリーを無効にしてください。

例

グローバルでスパニングツリーを無効にし、TC Snooping を有効にします。

<Switch> system-view

[Switch] undo stp global enable

[Switch] stp tc-snooping

関連コマンド

stp global enable

8.1.51 stp timer forward-delay

Syntax

stp [**vlan** *vlan-id-list*] **timer forward-delay** *time*

undo stp [**vlan** *vlan-id-list*] **timer forward-delay**

デフォルト

1500 センチ秒

View

System view

定義済みユーザロール

network-admin

パラメータ

vlan *vlan-id-list*: VLAN を指定します。半角スペースで区切り 10 まで設定するか、VLAN の範囲で設定することができます。VLAN を範囲で指定する形式は *vlan-id1* [**to** *vlan-id2*] です。*vlan-id2* は *vlan-id1* 以上の値にしてください。設定範囲は 1～4094 です。STP、RSTP、MSTP では使用しません。

time: 転送遅延を設定します。単位はセンチ秒です。設定範囲は 400～3000 で、100 の倍数です。（400、500、600、・・・のように設定します）

説明

stp timer forward-delay コマンドは転送遅延タイマを設定します。

undo stp timer forward-delay コマンドはデフォルトに戻します。

転送遅延タイマは状態の遷移の時間間隔を決定します。一時的なループを防ぐため、スパニングツリーのポートは廃棄状態から転送状態に遷移する前に、学習（中間）状態になります。リモート装置と同期を維持するため、ポートは転送遅延タイマの間、状態遷移を待ちます。

stp bridge-diameter コマンドでスイッチネットワークのダイアメータを指定し、**stp timer forward-delay** コマンドで転送遅延を設定しないことを推奨します。

この **stp bridge-diameter** コマンドによってスパニングツリーは転送遅延タイマを最適な値に自動で計算します。ネットワークダイアメータがデフォルト値である場合、転送遅延タイマもデフォルト値を使用します。

例

MSTP モードで転送遅延タイマを 2000 センチ秒に設定します。

<Switch> system-view

[Switch] stp timer forward-delay 2000

PVST モードで VLAN 2 の転送遅延タイマを 2000 センチ秒に設定します。

<Switch> system-view

[Switch] stp vlan 2 timer forward-delay 2000

関連コマンド

- **stp bridge-diameter**
- **stp timer hello**
- **stp timer max-age**

8.1.52 stp timer hello

Syntax

stp [**vlan** *vlan-id-list*] **timer hello** *time*

undo stp [**vlan** *vlan-id-list*] **timer hello**

デフォルト

200 センチ秒

View

System view

定義済みユーザロール

network-admin

パラメータ

vlan *vlan-id-list*: VLAN を指定します。半角スペースで区切り 10 まで設定するか、VLAN の範囲で設定することができます。VLAN を範囲で指定する形式は *vlan-id1* [**to** *vlan-id2*] です。*vlan-id2* は *vlan-id1* 以上の値にしてください。設定範囲は 1～4094 です。STP、RSTP、MSTP では使用しません。

time: hello 時間を設定します。単位はセンチ秒です。設定範囲は 100～1000 で、100 の倍数です。（100、200、300、・・・のように設定します）

説明

stp timer hello コマンドは hello 時間を設定します。

undo stp timer hello コマンドはデフォルトに戻します。

hello 時間はスパニングツリーを維持するため、装置が configuration BPDU を送信する間隔です。装置が指定した時間以内に configuration BPDU を受信できない場合、新たなスパニングツリー計算が開始されます。

stp bridge-diameter コマンドでスイッチネットワークのダイアメータを指定し、**stp timer hello** コマンドで hello 時間を設定しないことを推奨します。この **stp bridge-diameter** コマンドによってスパニングツリーは hello 時間を最適な値に自動で計算します。ネットワークダイアメータがデフォルト値である場合、hello 時間もデフォルト値を使用します。

例

MSTP モードで hello 時間を 400 センチ秒に設定します。

<Switch> system-view

[Switch] stp timer hello 400

PVST モードで VLAN 2 の hello 時間を 400 センチ秒に設定します。

<Switch> system-view

[Switch] stp vlan 2 timer hello 400

関連コマンド

- **stp bridge-diameter**
- **stp timer forward-delay**
- **stp timer max-age**

8.1.53 stp timer max-age

Syntax

stp [**vlan** *vlan-id-list*] **timer max-age** *time*

undo stp [**vlan** *vlan-id-list*] **timer max-age**

デフォルト

2000 センチ秒

View

System view

定義済みユーザロール

network-admin

パラメータ

vlan *vlan-id-list*: VLAN を指定します。半角スペースで区切り 10 まで設定するか、VLAN の範囲で設定することができます。VLAN を範囲で指定する形式は *vlan-id1* [**to** *vlan-id2*] です。*vlan-id2* は *vlan-id1* 以上の値にしてください。設定範囲は 1～4094 です。STP、RSTP、MSTP では使用しません。

time: 最大エージングタイマを設定します。単位はセンチ秒です。設定範囲は 600～4000 で、100 の倍数です。（600、700、800、・・・のように設定します）

説明

stp timer max-age コマンドは装置の最大エージングタイマを設定します。

undo stp timer max-age コマンドはデフォルトに戻します。

MSTP ネットワークの CIST で、装置は最大エージングタイマにもとづいて、ポートが受信した configuration BPDU がタイムアウトしているかどうかを判断します。ポートで configuration BPDU の受信がタイムアウトした場合、新しいスパニングツリーの再計算が開始されます。最大エージングタイマは、CIST（あるいは MSTI 0）のみ有効です。

stp bridge-diameter コマンドでスイッチネットワークのダイアメータを指定し、**stp timer max-age** コマンドで最大エージングタイマを設定しないことを推奨します。この **stp bridge-diameter** コマンドによってスパニングツリーは最大エージングタイマを最適な値に自動で計算します。ネットワークダイアメータがデフォルト値である場合、最大エージングタイマもデフォルト値を使用します。

例

MSTP モードで最大エージングタイマを 1000 センチ秒に設定します。

<Switch> system-view

[Switch] stp timer max-age 1000

PVST モードで VLAN 2 の最大エージングタイマを 1000 センチ秒に設定します。

<Switch> system-view

[Switch] stp vlan 2 timer max-age 1000

関連コマンド

- **stp bridge-diameter**
- **stp timer forward-delay**
- **stp timer hello**

8.1.54 stp timer-factor

Syntax

stp timer-factor *factor*

undo stp timer-factor

デフォルト

3

View

System view

定義済みユーザロール

network-admin

パラメータ

factor: タイムアウトファクタを指定します。設定範囲は 1～20 です。

説明

stp timer-factor コマンドはタイムアウト時間を決めるタイムアウトファクタを設定します。

タイムアウト時間 = タイムアウトファクタ × 3 × hello 時間

undo stp timer-factor コマンドはデフォルトに戻します。

ネットワークトポロジが安定した後、各非ルートブリッジは、リンク異常を確認するために周囲の装置に対し、hello 時間の間隔で設定 BPDU を転送します。通常、装置が上流装置から hello 時間の 9 倍の時間内に BPDU を受信しないと、装置は上流装置が故障しているとみなし、新たなスパニングツリー計算を開始します。

安定したネットワークにおいては、このようなスパニングツリー計算は、上流装置がビジー状態の場合に起こります。この場合、タイムアウト時間を長く（4 以上に）設定することにより、このような不要なスパニングツリー計算を避け、ネットワークリソースを節約できます。安定したネットワークでは、タイムアウトファクタを 5、6、または 7 に設定することが推奨されます。

例

タイムアウトファクタを 7 に設定します。

<Switch> system-view

[Switch] stp timer-factor 7

関連コマンド

stp timer hello

8.1.55 stp transmit-limit

Syntax

stp transmit-limit *limit*

undo stp transmit-limit

デフォルト

すべてのポートの BPDU の転送レートは 10 です。各ポートは各 hello 時間内に 10 の BPDU を送信します。

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

limit: BPDU 転送レートを設定します。設定範囲は 1～255 です。

説明

stp transmit-limit コマンドはポートの BPDU 転送レートを設定します。

undo stp transmit-limit コマンドはデフォルトに戻します。

各 hello 時間以内にポートが送信できる BPDU の最大数は、BPDU 転送レートと hello 時間の合計に等しいです。

BPDU 転送レートを大きくするとは多くのシステムリソースが必要となります。最大 BPDU 転送レートを適切に設定することにより、ポートが BPDU を送信するスピードを制限し、ネットワークトポロジが変更した際に過剰な帯域リソースを使用しないようにできます。デフォルト値を使うことを推奨します。

interface view で設定を行うと、設定は、現在のインタフェースでのみ有効になります。

aggregate interface view で設定を行うと、設定はアグリゲートインタフェースでのみ有効になります。

アグリゲーショングループのメンバポートで設定を行うと、ポートがアグリゲーショングループを除外した後に有効になります。

例

GigabitEthernet 1/0/1 の BPDU 転送レートを 5 に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] stp transmit-limit 5

8.1.56 stp vlan enable

Syntax

stp vlan *vlan-id-list* **enable**

undo stp vlan *vlan-id-list* **enable**

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

パラメータ

vlan *vlan-id-list*: VLAN を指定します。半角スペースで区切り 10 まで設定するか、VLAN の範囲で設定することができます。VLAN を範囲で指定する形式は *vlan-id1* [**to** *vlan-id2*] です。*vlan-id2* は *vlan-id1* 以上の値にしてください。設定範囲は 1～4094 です。このオプションを指定しない場合、グローバルでスパニングツリー機能（VLAN が含まれません）を有効あるいは無効にしてください。

説明

stp vlan enable コマンドは VLAN でスパニングツリーを有効にします。

undo stp enable コマンドは VLAN でスパニングツリーを無効にします。

スパニングツリー機能を有効にしたとき、スパニングツリーのモードの設定により装置は STP、RSTP、PVST、MSTP モードで動作します。

スパニングツリー機能を有効にしたとき、装置は設定された configuration BPDU にもとづいて自動で VLAN のスパニングツリーの状態を維持します。スパニングツリー機能を無効にしたとき、装置はスパニングツリーの状態の維持を停止します。

例

PVST モードにおいてグローバルでスパニングツリーを有効にし、VLAN 2 でスパニングツリーを有効にします。

<Switch> system-view

[Switch] stp mode pvst

[Switch] stp global enable

[Switch] stp vlan 2 enable

関連コマンド

- **stp enable**
- **stp global enable**
- **stp mode**

8.1.57 vlan-mapping modulo

Syntax

vlan-mapping modulo *modulo*

デフォルト

すべての VLAN は CIST（MSTI 0）にマッピングされています。

View

MST region view

定義済みユーザロール

network-admin

パラメータ

modulo: モジュロの値を設定します。設定範囲は 1～64 です。

説明

vlan-mapping modulo コマンドは指定モジュロの値に従って MST リージョンの VLAN を MSTI にマッピングし、VLAN-インスタンスマッピングテーブルの作成を早急に行います。

異なる MSTI に VLAN をマッピングすることはできません。すでに MSTI にマッピングされている VLAN を新しい MSTI にマッピングすると、古いマッピングは自動的に削除されます。

このコマンドは、次の式のとおり VLAN をマッピングする MSTI の ID を決定します。

ID ＝ （VLAN ID － 1） %modulo ＋ 1

（VLAN ID － 1） %modulo は（VLAN ID － 1）に対してモジュロ演算を行うことを意味します。モジュロの値が 15 である場合、VLAN 1 は MSTI 1 に、VLAN 2 は MSTI 2 に、VLAN 15 は MSTI 15 に、VLAN 16 は MSTI 16 のようにマッピングされます。

例

VLAN を MSTI にモジュロ 8 でマッピングします。

<Switch> system-view

[Switch] stp region-configuration

[Switch-mst-region] vlan-mapping modulo 8

関連コマンド

- **active region-configuration**
- **check region-configuration**
- **display stp region-configuration**
- **region-name**
- **revision-level**

目次

このセクションのページは **3-x-x** です。

9 章 ループ検出 9-1
9.1 ループ検出設定コマンド 9-1
9.1.1 display loopback-detection 9-1
9.1.2 loopback-detection action 9-2
9.1.3 loopback-detection enable 9-4
9.1.4 loopback-detection global action 9-5
9.1.5 loopback-detection global enable 9-6
9.1.6 loopback-detection interval-time 9-7

9章 ループ検出

9.1 ループ検出設定コマンド

9.1.1 display loopback-detection

Syntax

display loopback-detection

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display loopback-detection コマンドはループバック検出の設定と状態を表示します。

例

ループバック検出の設定と状態を表示します。

<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
```

表 9-1 コマンド出力

フィールド	説明

Action mode	ループガードのアクションです。
	• **Block**–ポートでループが検出されたとき、装置は以下の処理を行います。
	  • ログを出力します。
	  • MACアドレスの学習を無効にします。
	  • ポートをブロックします。
	• **None**–ポートでループが検出されたとき、装置はログを出力しますが、ポートでアクションは行いません。
	• **No-learning**–ポートでループが検出されたとき、装置はログを出力し、MACアドレスの学習を無効にします。

9.1.2 loopback-detection action

Syntax

Layer 2 Ethernet interface view：

loopback-detection action { **block** | **no-learning** | **shutdown** }

undo loopback-detection action

Layer 2 aggregate interface view：

loopback-detection action shutdown

undo loopback-detection action

デフォルト

Layer 2 Ethernet interface view：

ループが検出されたとき、ブロックアクションを行います。

Layer 2 aggregate interface view

ループが検出されたとき、装置はログを出力しますが、保護アクションは行いません。

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

block: ブロックモードを有効にします。ループを検出すると、装置は以下の処理を行います。

- ログを出力します。
- MAC アドレスの学習を無効にします。
- ポートの入力トラフィックをブロックします。

アグリゲートインタフェースではサポートしていません。

no-learning: **no-learning** モードを有効にします。ループを検出すると、装置はログを出力し、MAC アドレスの学習を無効にします。アグリゲートインタフェースではサポートしていません。

shutdown: シャットダウンモードを有効にします。ループを検出すると、装置はログを出力し、すべてのフレームの送受信を無効にするためポートをシャットダウンします。装置は検出タイマが終了すると、自動でポートをアップします。**shutdown-interval** コマンドで検出タイマを設定することができます。詳細はコマンドマニュアルのセクション 1 *はじめに* “*装置管理*”を参照してください。

説明

loopback-detection action コマンドはポートのループ保護のアクションを設定します。

undo loopback-detection action コマンドは無効に設定します。

アクションをデフォルト値に戻すときは loopback-detection action block コマンドを実行してください。

グローバルでループ保護のアクションを設定する場合、**loopback-detection global action** コマンドを使用します。

グローバルの設定はすべてのポートで適用されます。ポートの設定は指定されたポートで適用されます。ポートの設定はグローバルの設定よりも優先されます。

例

GigabitEthernet 1/0/1 のループ保護のアクションをシャットダウンに設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] loopback-detection action shutdown

関連コマンド

- **display loopback-detection**
- **loopback-detection global action**

9.1.3 loopback-detection enable

Syntax

loopback-detection enable vlan { *vlan-id-list* | **all** }

undo loopback-detection enable vlan { *vlan-id-list* | **all** }

デフォルト

Layer 2 Ethernet interface view：Vlan1 のループ検出が有効

Layer 2 aggregate interface view：無効

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id-list: VLAN リストを指定します。半角スペースで区切り 10 まで設定するか、VLAN の範囲で設定することができます。VLAN を範囲で指定する形式は *vlan-id1* [**to** *vlan-id2*] です。設定範囲は 1～4094 です。*vlan-id2* は *vlan-id1* 以上の値にしてください。

all: 既存のすべての VLAN を指定します。

説明

loopback-detection enable コマンドはポートでループ検出を有効にします。

undo loopback-detection enable コマンドはポートでループ検出を無効にします。

有効 VLAN をデフォルト値に戻すときは、**undo loopback-detection enable vlan all** コマンド実行後に **loopback-detection enable vlan 1** コマンドを実行してください。

グローバルでループ検出を有効にする場合、**loopback-detection global enable** コマンドを使用します。

ポートのループ検出の設定はグローバルでループ検出の設定が行われたのち適用されます。

以下の要件が満たされている場合、ポートでループ検出が無効であったとしてもポートのループ保護アクションは開始することができます。

- 装置でループ検出がグローバルで有効、あるいはほかのすべてのポートで有効です。
- ポートはすべての VLAN のループ検出フレームを受信します。

例

VLAN 10～VLAN 20 の GigabitEthernet 1/0/1 でループ検出を有効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] loopback-detection enable vlan 10 to 20

関連コマンド

- **display loopback-detection**
- **loopback-detection global enable**

9.1.4 loopback-detection global action

Syntax

loopback-detection global action shutdown

undo loopback-detection global action

デフォルト

ループが検出されたとき、装置はログを出力しますが、保護アクションは行いません。

View

System view

定義済みユーザロール

network-admin

パラメータ

shutdown: シャットダウンモードを有効にします。ループを検出すると、装置はログを出力し、ポートをシャットダウンします。装置は検出タイマが終了すると、自動でポートを転送状態にします。**shutdown-interval** コマンドで検出タイマを設定することができます。詳細はコマンドマニュアルのセクション 1 *はじめに* “*装置管理*”を参照してください。

説明

loopback-detection global action コマンドはグローバルでループ保護のアクションを設定します。

undo loopback-detection global action コマンドはデフォルトに戻します。

ポートでループ保護のアクションを設定する場合、interface view で **loopback-detection action** コマンドを使用します。

グローバルの設定はすべてのポートで適用されます。ポートの設定は指定されたポートで適用されます。ポートの設定はグローバルの設定よりも優先されます。

🕮 **メモ**：

- **shutdown** アクションを設定し、ポートでループが検出されたとき、ポートをシャットダウンし、ループ状態を解除するため、アクション実行時に RECOVERED のログも出力します。
- **shutdown** アクションによるポートのシャットダウンは、**display interface** コマンドの Current state フィールドの状態が DOWN（Loopback detection down）と表示されます。

例

グローバルでループ保護のアクションをシャットダウンに設定します。

<Switch> system-view

[Switch] loopback-detection global action shutdown

関連コマンド

- **display loopback-detection**
- **loopback-detection action**

9.1.5 loopback-detection global enable

Syntax

loopback-detection global enable vlan { *vlan-id-list* | **all** }

undo loopback-detection global enable vlan { *vlan-id-list* | **all** }

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

パラメータ

vlan-id-list: VLAN リストを指定します。半角スペースで区切り 10 まで設定するか、VLAN の範囲で設定することができます。VLAN を範囲で指定する形式は *vlan-id1* [**to** *vlan-id2*] です。設定範囲は 1～4094 です。*vlan-id2* は *vlan-id1* 以上の値にしてください。

all: 既存のすべての VLAN を指定します。

説明

loopback-detection global enable コマンドはグローバルでループ検出を有効にします。

undo loopback-detection global enable コマンドはグローバルでループ検出を無効にします。

ポートでループ検出を有効にする場合、interface view で **loopback-detection enable** コマンドを使用します。

グローバルの設定は指定された VLAN のすべてのポートで適用されます。ポートの設定は指定された VLAN に所属するポートで適用されます。ポートの設定はグローバルの設定よりも優先されます。

以下の要件が満たされている場合、ポートでループ検出が無効であったとしてもポートのループ保護アクションは開始することができます。

- 装置でループ検出がグローバルで有効、あるいはほかのすべてのポートで有効です。
- ポートはすべての VLAN のループ検出フレームを受信します。

例

VLAN 10～VLAN 20 のすべてのポートでループ検出を有効にします。

<Switch> system-view

[Switch] loopback-detection global enable vlan 10 to 20

関連コマンド

- **display loopback-detection**
- **loopback-detection enable**

9.1.6 loopback-detection interval-time

Syntax

loopback-detection interval-time *interval*

undo loopback-detection interval-time

デフォルト

5 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

interval: ループ検出間隔を設定します。設定範囲は 1～300 秒です。

説明

loopback-detection interval-time コマンドはループ検出間隔を設定します。

undo loopback-detection interval-time コマンドはデフォルトに戻します。

ループ検出が有効であるとき、装置は指定された間隔でループ検出フレームを送信します。検出間隔が短い場合、精度が高くなりますが、多くのリソースが消費されます。ループ検出間隔を設定する場合、システムの性能とループ検出速度を考慮してください。

🕮 **メモ**:

undo loopback-detection interval-time コマンドを実行しても、デフォルト設定には戻りません。**undo** コマンドを実行した場合は、30 秒のループ検出間隔で動作する設定となります。デフォルト値に戻す場合は、**loopback-detection interval-time 5** コマンドを実行してください。

例

ループ検出間隔を 10 秒に設定します。

<Switch> system-view

[Switch] loopback-detection interval-time 10

関連コマンド

display loopback-detection

目次

このセクションのページは **3-x-x** です。

10 章 VLAN 10-1
10.1 VLAN 設定コマンド 10-1
10.1.1 description 10-1
10.1.2 display interface vlan-interface 10-2
10.1.3 display vlan 10-6
10.1.4 display vlan brief 10-8
10.1.5 interface vlan-interface 10-9
10.1.6 name 10-10
10.1.7 reset counters interface vlan-interface 10-11
10.1.8 shutdown 10-11
10.1.9 vlan 10-13
10.2 ポートベース VLAN 設定コマンド 10-14
10.2.1 display port 10-14
10.2.2 port 10-15
10.2.3 port access vlan 10-16
10.2.4 port hybrid pvid 10-17
10.2.5 port hybrid vlan 10-18
10.2.6 port link-type 10-19
10.2.7 port trunk permit vlan 10-20
10.2.8 port trunk pvid 10-21
10.3 MAC アドレスベース VLAN 設定コマンド 10-22
10.3.1 display mac-vlan 10-22
10.3.2 display mac-vlan interface 10-24
10.3.3 mac-vlan enable 10-25
10.3.4 mac-vlan mac-address 10-25
10.3.5 mac-vlan trigger enable 10-27
10.3.6 port pvid forbidden 10-28
10.3.7 vlan precedence 10-28
10.4 IP サブネットベース VLAN 設定コマンド 10-29
10.4.1 display ip-subnet-vlan interface 10-29
10.4.2 display ip-subnet-vlan vlan 10-31
10.4.3 ip-subnet-vlan 10-32
10.4.4 port hybrid ip-subnet-vlan 10-33
10.5 プロトコルベース VLAN 設定コマンド 10-35
10.5.1 display protocol-vlan interface 10-35
10.5.2 display protocol-vlan vlan 10-36

10.5.3 port hybrid protocol-vlan 10-37
10.5.4 protocol-vlan 10-39

10章 VLAN

10.1 VLAN設定コマンド

10.1.1 description

Syntax

description *text*

undo description

デフォルト

VLAN の説明は VLAN *vlan-id* です。*vlan-id* は VLAN の ID です。たとえば、VLAN 100 の VLAN の説明は VLAN 0100 です。

VLAN インタフェースの説明はインタフェースの名前です。たとえば Vlan-interface1 Interface です。

View

VLAN view

VLAN interface view

定義済みユーザロール

network-admin

パラメータ

text: VLAN あるいは VLAN インタフェースの説明を指定します。設定範囲は 1～255 です。大文字、小文字を区別します。

説明

description コマンドは VLAN あるいは VLAN インタフェースの説明を指定します。

undo description コマンドはデフォルトに戻します。

VLAN あるいは VLAN インタフェースの機能あるいは説明を設定することができます。

装置で多くの VLAN あるいは VLAN インタフェースを識別するのに役立ちます。

例

VLAN 2 の説明を sales-private に設定します。

<Switch> system-view

[Switch] vlan 2

[Switch-vlan2] description sales-private

VLAN インタフェース 2 の説明を linktoPC56 に設定します。

<Switch> system-view

[Switch] vlan 2

[Switch-vlan2] quit

[Switch] interface vlan-interface 2

[Switch-Vlan-interface2] description linktoPC56

関連コマンド

- **display interface vlan-interface**
- **display vlan**

10.1.2 display interface vlan-interface

Syntax

display interface vlan-interface [*interface-number*] [**brief** [**description** | **down**]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

vlan-interface *interface-number*: VLAN インタフェース番号を指定します。指定しない場合、すべての VLAN インタフェースの情報を表示します。

brief: インタフェースの概要情報を表示します。指定しない場合、VLAN インタフェースの詳細情報を表示します。

description: 完全なインタフェースの説明を表示します。指定しない場合、説明の最初の 27 文字のみを表示します。

down: down 状態の VLAN インタフェース、原因を表示します。指定しない場合、すべての状態の VLAN インタフェースの情報を表示します。

説明

display interface vlan-interface コマンドは VLAN インタフェースの情報を表示します。

例

VLAN インタフェース 2 の情報を表示します。（VLAN インタフェース 2 はインタフェース統計情報の収集を行います。）

<Switch> display interface vlan-interface 2

```
Vlan-interface2
Current state: DOWN
Line protocol state: DOWN
Description: Vlan-interface2 Interface
Bandwidth: 100000 kbps
Maximum transmission unit: 1500
Internet protocol processing : Disabled
IP packet frame type: Ethernet II, hardware address: 000f-e249-8050
IPv6 packet frame type: Ethernet II, hardware address: 000f-e249-8050
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
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
```

VLAN インタフェース 10 の情報を表示します。（VLAN インタフェース 10 はインタフェース統計情報の収集を行いません。）

<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
```

VLAN インタフェース 2 の概要情報を表示します。

<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     --
```

表 10-1 コマンド出力

フィールド	説明
Vlan-interface2	VLANインタフェース名です。
Current state	VLANインタフェースの物理状態です。 ● **Administratively DOWN**–**shutdown**コマンドでVLANインタフェースがシャットダウンしています。インタフェースは運用上においてdownしています。 ● **DOWN**–**shutdown**コマンドでVLANインタフェースがシャットダウンしていませんが、物理的にdownしています。VLANインタフェースのVLANはup状態の物理ポートがありません。ポートが物理的に接続されていない、あるいはリンクに失敗している可能性があります。 ● **UP**–VLANインタフェースが運用上も物理的にも起動している状態です。
Line protocol state	VLANインタフェースのプロトコルリンクレイヤの状態です。 ● **DOWN**–VLANインタフェースがプロトコルリンクレイヤでdownしています。 ● **UP**–VLANインタフェースがプロトコルリンクレイヤでupしています。
Description	VLANインタフェースの説明です。
Bandwidth	VLANインタフェースの予期された帯域幅です。
Maximum Transmit Unit	VLANインタフェースのMTUです。
Internet protocol processing : Disabled	VLANインタフェースにIPアドレスが設定されておらず、IPパケットの処理できません。
Internet Address	VLANインタフェースのIPアドレスです。**primary**はIPアドレスがプライマリIPアドレスであることを示します。
IP packet frame type	IPv4の送信フレームタイプです。
hardware address	VLANインタフェースに対応するMACアドレスです。
IPv6 packet frame type	IPv6の送信フレームタイプです。
Output queue - Urgent queuing: Size/Length/Discards 0/100/0 Output queue - Protocol queuing: Size/Length/Discards 0/500/0 Output queue - FIFO queuing: Size/Length/Discards 0/75/0	緊急、プロトコル、FIFO出力キューの情報です。 ● **Size**–キューのパケット数です。 ● **Length**–キューが含まれるパケット最大数です。 ● **Discards**–廃棄されたパケット数です。

フィールド	説明
Last clearing of counters	インタフェースで**reset counters interface**コマンドを最後に使用した時間です。 **Never**は装置が起動してから**reset counters interface**コマンドを一度も使用していないことを示します。
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	過去300秒以内の平均送受信トラフィックです。単位はバイト/秒、bps、ppsです。
Input: 0 packets, 0 bytes, 0 drops	インタフェースで受信されたパケットの総数、パケットサイズと廃棄されたパケット数です。パケットサイズの単位はバイトです。
Output: 0 packets, 0 bytes, 0 drops	インタフェースで送信されたパケットの総数、パケットサイズと廃棄されたパケット数です。パケットサイズの単位はバイトです。
Brief information on interfaces in route mode	レイヤ3インタフェースの概要情報です。
Interface	省略したインタフェース名です。
Link	インタフェースの物理リンク状態です。 ● **UP**–リンクがupです。 ● **DOWN**–リンクが物理的にdownしています。 ● **ADM**–リンクが運用上でシャットダウンしています。物理状態を回復するために、**undo shutdown**コマンドを実行します。 ● **Stby**–インタフェースがバックアップインタフェースとして動作します。プライマリインタフェースを表示する場合、**display interface-backup state**コマンドを使用します。
Protocol	インタフェースのリンクレイヤの状態です。 ● **UP**－インタフェースのリンクがupです。 ● **DOWN**－インタフェースのリンクがdownです。 ● **UP(s)**–インタフェースのリンクがオンデマンドリンクあるいは準備ができていない状態です。ここで（**s**）はスプーフィングのフラグを示します。
Primary IP	インタフェースのプライマリIPアドレスです。

関連コマンド

reset counters interface vlan-interface

10.1.3 display vlan

Syntax

display vlan [*vlan-id1* [**to** *vlan-id2*] | **all** | **dynamic** | **reserved** | **static**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

vlan-id1: VLAN ID で指定された VLAN の情報を表示します。設定範囲は 1～4094 です。

vlan-id1 **to** *vlan-id2*: VLAN ID の範囲を指定します。*vlan-id1* と *vlan-id2* の設定範囲は 1～4094 です。*vlan-id2* は *vlan-id1* よりも大きい値にする必要があります。

all: 予約済み VLAN を除くすべての VLAN の情報を表示します。

dynamic: ダイナミック VLAN の番号と各ダイナミック VLAN の ID を表示します。ダイナミック VLAN は MVRP あるいは RADIUS サーバによって作成されます。

reserved: 予約済み VLAN の情報を表示します。プロトコルモジュールは、機能の実装状態に従って予約済み VLAN を定義し、予約済み VLAN はプロトコルモジュールに使用されます。予約済み VLAN の設定はできません。

static: スタティック VLAN 番号と各スタティック VLAN の ID を表示します。スタティック VLAN は手動で作成されます。

説明

display vlan コマンドは VLAN 情報を表示します。

例

VLAN 2 の情報を表示します。

<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
```

VLAN 3 の情報を表示します。

<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
```

表 10-2 コマンド出力

フィールド	説明
VLAN type	VLANタイプです。スタティックあるいはダイナミックがあります。
Route interface	VLANインタフェースが設定されているかどうかを示します。 ● **Not configured**ー設定されていません。 ● **Configured**ー設定されています。
Description	VLANの説明です。
Name	VLANに設定された名前です。
IP address	VLANインタフェースのプライマリIPv4アドレスです。このフィールドはVLANインタフェースにIPv4アドレスが設定されている場合のみ表示されます。セカンダリIPアドレスが存在する場合、以下のいずれかの方法で表示することができます。 ● **display interface vlan-interface**コマンドを使用します。 ● VLAN interface viewで**display this**コマンドを使用します。
Subnet mask	プライマリIPアドレスのサブネットマスクです。このフィールドはVLANインタフェースにIPアドレスが設定されている場合のみ表示されます。
Tagged ports	タグ付きVLANパケットを通すポートです。
Untagged ports	タグなしVLANパケットを通すポートです。

関連コマンド

vlan

10.1.4 display vlan brief

Syntax

display vlan brief

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display vlan brief コマンドは VLAN の概要情報を表示します。

例

VLAN の概要情報を表示します。

<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
```

表 10-3 コマンド出力

フィールド	説明
Default VLAN ID	システムのデフォルトVLAN IDです。
Name	VLAN名です。
Port	VLANを通してパケットを許可するポートです。

10.1.5 interface vlan-interface

Syntax

interface vlan-interface *interface-number*

undo interface vlan-interface *interface-number*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

interface-number: VLAN インタフェース番号を指定します。設定範囲は 1～4094 です。

説明

interface vlan-interface コマンドは VLAN インタフェースを作成し、作成された VLAN インタフェースの view に移行あるいは既存の VLAN インタフェースの view に移行します。

undo interface vlan-interface コマンドは VLAN インタフェースを削除します。

VLAN インタフェースを作成する前に、VLAN を作成してください。

例

VLAN インタフェース 2 を作成し、作成された VLAN インタフェースの view に移行します。

<Switch> system-view

[Switch] vlan 2

[Switch-vlan2] quit

[Switch] interface vlan-interface 2

[Switch-Vlan-interface2]

関連コマンド

display interface vlan-interface

10.1.6 name

Syntax

name *text*

undo name

デフォルト

デフォルトの VLAN 名は VLAN *vlan-id* です。*vlan-id* は 4 桁の VLAN の ID です。ID が 4 桁よりも少ない場合、先頭に 0 が追加されます。たとえば、VLAN 100 の VLAN 名は VLAN 0100 です。

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

text: VLAN 名を指定します。設定範囲は 1～32 です。大文字、小文字を区別します。

説明

name コマンドは VLAN の名前を設定します。

undo name コマンドは VLAN の名前をデフォルトに戻します。

装置に 802.1X または MAC アドレス認証の設定が行われる場合、VLAN ID または VLAN 名を使用して許可 VLAN を指定することができます。VLAN の数が非常に多い場合、識別するために VLAN 名を使用します。

例

VLAN 2 の名前を test vlan として設定します。

<Switch> system-view

[Switch] vlan 2

[Switch-vlan2] name test vlan

関連コマンド

display vlan

10.1.7 reset counters interface vlan-interface

Syntax

reset counters interface vlan-interface [*interface-number*]

View

User view

定義済みユーザロール

network-admin

パラメータ

vlan-interface *interface-number*: VLAN インタフェース番号を指定します。指定しない場合、すべての VLAN インタフェースの統計情報を削除します。

説明

reset counters interface vlan-interface コマンドは VLAN インタフェースの統計情報を削除します。

一定期間、トラフィックの統計情報を収集する場合、以前に収集された統計情報の履歴を削除し、このコマンドを使用します。

例

VLAN インタフェース 2 の統計情報を削除します。

<Switch> reset counters interface vlan-interface 2

関連コマンド

display interface vlan-interface

10.1.8 shutdown

Syntax

shutdown

undo shutdown

デフォルト

VLAN インタフェースは手動でシャットダウンしていません。以下のガイドラインが適用されます。

- VLAN のすべてのポートが down している場合、VLAN インタフェースは down になります。
- 1 つ以上の VLAN が up である場合、VLAN インタフェースは up になります。

View

VLAN interface view

定義済みユーザロール

network-admin

説明

shutdown コマンドは VLAN インタフェースをシャットダウンします。

undo shutdown コマンドは VLAN インタフェースを up にします。

コマンドを使用した場合、VLAN インタフェースは DOWN（Administratively）状態のままになります。この場合、VLAN インタフェースの状態は VLAN のポートの状態に影響しません。

VLAN インタフェースのパラメータを設定する前に、ネットワークへの影響から設定を防ぐため、**shutdown** コマンドで VLAN インタフェースをシャットダウンしてください。VLAN インタフェースのパラメータを設定した後、設定を適用するため、**undo shutdown** コマンドを使用してください。

故障した VLAN インタフェースのトラブルシューティングを行うため、**shutdown** コマンドを使用してください。インタフェースが回復したかどうかを確認するため、**undo shutdown** コマンドを使用してください。

VLAN 内のすべての Ethernet ポートの状態は、VLAN インタフェースの状態とは無関係です。

例

VLAN インタフェース 2 をシャットダウンし、up にします。

<Switch> system-view

[Switch] interface vlan-interface 2

[Switch-Vlan-interface2] shutdown

[Switch-Vlan-interface2] undo shutdown

10.1.9 vlan

Syntax

vlan { *vlan-id1* [**to** *vlan-id2*] | **all** }

undo vlan { *vlan-id1* [**to** *vlan-id2*] | **all** }

デフォルト

VLAN 1（システムデフォルト VLAN）

View

System view

定義済みユーザロール

network-admin

パラメータ

vlan-id1: VLAN ID を指定します。設定範囲は 1～4094 です。

vlan-id1 **to** *vlan-id2*: VLAN の範囲を指定します。*vlan-id1* と *vlan-id2* は VLAN ID を指定します。設定範囲は 1～4094 です。*vlan-id2* は *vlan-id1* 以上の値にしてください。

all: 予約済み VLAN を除いてすべての VLAN を作成あるいは削除します。**all** パラメータは装置で作成できる VLAN の最大数が 4094 より少ない場合、サポートしません。

説明

vlan *vlan-id* コマンドは VLAN を作成し、その view あるいは既存の VLAN の view に移行します。

vlan *vlan-id1* **to** *vlan-id2* コマンドは予約済み VLAN を除いて *vlan-id1* から *vlan-id2* の VLAN を作成します。

vlan all コマンドは VLAN 1～VLAN 4094 を作成します。

undo vlan コマンドは指定された VLAN を削除します。

システムデフォルト VLAN（VLAN 1）、予約済み VLAN を作成あるいは削除することはできません。

ダイナミック VLAN、アプリケーションによって固定された VLAN を削除するため、**undo vlan** コマンドを使用することはできません。これらの VLAN を削除するため、最初に VLAN から設定を削除してください。

例

VLAN 2 を作成し、その view に移行します。

<Switch> system-view

[Switch] vlan 2

[Switch-vlan2]

VLAN 4～VLAN 100 を作成します。

<Switch> system-view

[Switch] vlan 4 to 100

関連コマンド

display vlan

10.2 ポートベースVLAN設定コマンド

10.2.1 display port

Syntax

display port { **hybrid** | **trunk** }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

hybrid: ハイブリッドポートを指定します。

trunk: トランクポートを指定します。

説明

display port コマンドはハイブリッドポートあるいはトランクポートに関する情報を表示します。

例

ハイブリッドポートの情報を表示します。

<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
```

トランクポートの情報を表示します。

<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
```

表 10-4 コマンド出力

フィールド	説明
Interface	ポート名です。
PVID	ポートのVLAN IDです。
VLAN Passing	ポートで許可されたVLANです。
Tagged	VLANタグを削除しないでポートがパケットを送信するVLANです。
Untagged	VLANタグを削除した後、ポートがパケットを送信するVLANです。

10.2.2 port

Syntax

port *interface-list*

undo port *interface-list*

デフォルト

VLAN 1

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

interface-list: インタフェースを指定します。半角スペースで区切り 10 まで設定するか、インタフェースの範囲で設定することができます。インタフェースを範囲で指定する形式は *interface-type interface-number1* [**to** *interface-type interface-number2*]です。*interface-number2* は *interface-number1* 以上の値にしてください。

説明

port コマンドは指定したアクセスポートに VLAN を割り当てます。

undo port コマンドは VLAN から指定したアクセスポートを削除します。

このコマンドはアクセスポートのみ適用可能です。

デフォルトですべてのポートはアクセスポートです。ポートタイプを **port link-type** コマンドで設定することができます。

例

GigabitEthernet 1/0/1～GigabitEthernet 1/0/3 に VLAN 2 を割り当てます。

<Switch> system-view

[Switch] vlan 2

[Switch-vlan2] port gigabitethernet 1/0/1 to gigabitethernet 1/0/3

関連コマンド

display vlan

10.2.3 port access vlan

Syntax

port access vlan *vlan-id*

undo port access vlan

デフォルト

すべての VLAN は VLAN1 に所属しています。

View

Layer 2 aggregate interface view

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id: VLAN ID を指定します。設定範囲は 1～4094 です。

説明

port access vlan コマンドはアクセスポートを指定した VLAN に割り当てます。

undo port access vlan コマンドはデフォルトに戻します。

アクセスポートを VLAN に割り当てる前に、VLAN が作成されていることを確認してください。

例

GigabitEthernet 1/0/1 に VLAN 3 を割り当てます。

<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

Syntax

port hybrid pvid vlan *vlan-id*

undo port hybrid pvid

デフォルト

リンクタイプがアクセスであるとき、ハイブリッドポートの PVID はポートが所属している VLAN の ID です。

View

Layer 2 aggregate interface view

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id: VLAN ID を指定します。設定範囲は 1～4094 です。

説明

port hybrid pvid コマンドはハイブリッドポートの PVID を設定します。

undo port hybrid pvid コマンドはハイブリッドポートの PVID を 1 に設定します。

ハイブリッドポートの PVID として存在しない VLAN を使用することができます。**undo vlan** コマンドでハイブリッドポートの PVID を削除する場合、ポートの PVID の設定は適用されません。

ローカルとリモートのハイブリッドポートに同じ PVID を設定することを推奨します。

PVID からのパケットの転送を許可するためにハイブリッドポートの設定に **port hybrid pvid** コマンドを使用してください。

例

ハイブリッドポートの GigabitEthernet 1/0/1 の PVID を VLAN100 に設定し、GigabitEthernet 1/0/1 に VLAN100 を割り当てます。

<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

関連コマンド

- **port hybrid vlan**
- **port link-type**

10.2.5 port hybrid vlan

Syntax

port hybrid vlan *vlan-id-list* { **tagged** | **untagged** }

undo port hybrid vlan *vlan-id-list*

デフォルト

リンクタイプがアクセスであるとき、ハイブリッドポートはポートが所属している VLAN のタグなしメンバです。

View

Layer 2 aggregate interface view

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id-list: VLAN を指定します。半角スペースで区切り 10 まで設定するか、VLAN ID の範囲で設定することができます。VLAN を範囲で指定する形式は *vlan-id1* **to** *vlan-id2* です。設定範囲は 1～4094 です。*vlan-id2* は *vlan-id1* 以上の値にしてください。指定する VLAN はすでに作成されていることを確認してください。

tagged: ポートは VLAN タグを削除しないで指定した VLAN のパケットを送信するように設定します。

untagged: ポートは VLAN タグを削除したのち、指定した VLAN のパケットを送信するように設定します。

説明

port hybrid vlan コマンドは指定した VLAN にハイブリッドポートを割り当てます。

undo port hybrid vlan コマンドは指定した VLAN からハイブリッドポートを削除します。

ハイブリッドポートは、複数の VLAN が通過できます。**port hybrid vlan** コマンドを繰り返し実行すると、ハイブリッドポートを通過する VLAN は、各実行の *vlan-id-list* により指定された VLAN に設定されます。

例

GigabitEthernet 1/0/1 をハイブリッドポートに設定します。VLAN 2、VLAN 4 および VLAN 50～VLAN 100 に割り当て、これらの VLAN のパケットにタグを付けて送信するよう GigabitEthernet 1/0/1 に設定します。

<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

関連コマンド

port link-type

10.2.6 port link-type

Syntax

port link-type { **access** | **hybrid** | **trunk** }

undo port link-type

デフォルト

access

View

Layer 2 aggregate interface view

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

access: ポートのリンクタイプをアクセスとして指定します。

hybrid: ポートのリンクタイプをハイブリッドとして指定します。

trunk: ポートのリンクタイプをトランクとして指定します。

説明

port link-type コマンドはポートのリンクタイプを設定します。

undo port link-type コマンドはデフォルトに戻します。

トランクポートからハイブリッドポート（またはその逆）のリンクタイプを変更するには、まずリンクタイプをアクセスに設定する必要があります。

例

GigabitEthernet 1/0/1 のリンクタイプをトランクポートに設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] port link-type trunk

10.2.7 port trunk permit vlan

Syntax

port trunk permit vlan { *vlan-id-list* | **all** }

undo port trunk permit vlan { *vlan-id-list* | **all** }

デフォルト

トランクポートは VLAN 1 からのパケットのみ通過できるように許可します。

View

Layer 2 aggregate interface view

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id-list: インタフェースを指定します。半角スペースで区切り 10 まで設定するか、VLAN ID の範囲で設定することができます。VLAN を範囲で指定する形式は *vlan-id1* **to** *vlan-id2* です。設定範囲は 1～4094 です。*vlan-id2* は *vlan-id1* 以上の値にしてください。

all: すべての VLAN を通過できるように許可します。許可されていない VLAN ユーザがポートを通して制限されたリソースにアクセスすることを防ぐため、注意して **port trunk permit vlan all** コマンドを使用してください。

説明

port trunk permit vlan コマンドはトランクポートを指定した VLAN に割り当てます。

undo port trunk permit vlan コマンドはトランクポートを指定した VLAN から削除します。

トランクポートは複数の VLAN を通過できます。**port trunk permit vlan** コマンドを繰り返し実行すると、トランクポートを通過する VLAN は、各 *vlan-id-list* により指定された VLAN に設定されます。

トランクポート上では、PVID のトラフィックのみタグなしで通過することができます。

例

GigabitEthernet 1/0/1 をトランクポートに設定します。VLAN 2、VLAN 4 および VLAN 50～VLAN 100 に割り当てます。

<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

関連コマンド

port link-type

10.2.8 port trunk pvid

Syntax

port trunk pvid vlan *vlan-id*

undo port trunk pvid

デフォルト

VLAN 1

View

Layer 2 aggregate interface view

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id: VLAN ID を指定します。設定範囲は 1～4094 です。

説明

port trunk pvid コマンドはトランクポートの PVID を設定します。

undo port trunk pvid コマンドはデフォルトに戻します。

トランクポートの PVID として存在しない VLAN を使用することができます。**undo vlan** コマンドを使用してトランクポートの PVID を削除しても、ポートの PVID の設定には影響しません。

ローカルおよびリモートのトランクポートは、PVID のトラフィックが正常に送信されるために同じ PVID を使用する必要があります。

PVID からのパケットの転送を許可するためにトランクポートの設定に **port trunk permit vlan** コマンドを使用してください。

例

GigabitEthernet 1/0/1 をトランクポートに設定します。PVID を VLAN 100 に設定し、GigabitEthernet 1/0/1 に VLAN 100 を割り当てます。

<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

関連コマンド

- **port link-type**
- **port trunk permit vlan**

10.3 MACアドレスベースVLAN設定コマンド

10.3.1 display mac-vlan

Syntax

display mac-vlan { **all** | **dynamic** | **mac-address** *mac-address* [**mask** *mac-mask*] | **static** | **vlan** *vlan-id* }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all: すべての MAC アドレス-VLAN エントリを指定します。

dynamic: ダイナミックに設定された MAC アドレス-VLAN エントリを指定します。

mac-address *mac-address*: MAC アドレス-VLAN エントリの MAC アドレスを指定します。形式は H-H-H です。

mask *mac-mask*: MAC アドレス-VLAN エントリの MAC アドレスにマッチするマスクを指定します。*mac-mask* は上位側ビット（全バイナリビット=1）と下位側ビット（全バイナリビット=0）で構成されます。デフォルトは ffff-ffff-ffff です。

static: スタティックに設定された MAC アドレス-VLAN エントリを指定します。

vlan *vlan-id*: MAC アドレス-VLAN エントリの VLAN を指定します。設定範囲は 1～4094 です。

説明

display mac-vlan コマンドは MAC アドレス-VLAN エントリを表示します。

例

すべての MAC アドレス-VLAN エントリを表示します。

<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
```

表 10-5 コマンド出力

フィールド	説明
S - Static	スタティックに設定されたMACアドレス-VLANエントリです。
D - Dynamic	ダイナミックに設定されたMACアドレス-VLANエントリです。
MAC address	MACアドレス-VLANエントリのMACアドレスです。
Mask	MACアドレス-VLANエントリのMACアドレスのマスクです。
VLAN ID	MACアドレス-VLANエントリのVLAN IDです。
Dot1q	MACアドレス-VLANエントリのVLANの802.1pプライオリティです。

フィールド	説明
State	MACアドレス-VLANエントリの状態です。 ● **S**－MACアドレス-VLANエントリがスタティックに設定されることを示します。 ● **D**－MACアドレス-VLANエントリが認証サーバからダイナミックに設定されることを示します。 ● **S&D**－MACアドレス-VLANエントリがスタティックおよびダイナミックの両方で設定されることを示します。

関連コマンド

mac-vlan mac-address

10.3.2 display mac-vlan interface

Syntax

display mac-vlan interface

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display mac-vlan interface コマンドは MAC アドレスベース VLAN で有効なすべてのポートを表示します。

例

MAC アドレスベース VLAN で有効なすべてのポートを表示します。

<Switch> display mac-vlan interface

```
MAC VLAN is enabled on following ports:
GigabitEthernet1/0/1  GigabitEthernet1/0/2  GigabitEthernet1/0/3
```

関連コマンド

mac-vlan enable

10.3.3 mac-vlan enable

Syntax

mac-vlan enable

undo mac-vlan enable

デフォルト

無効

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

説明

mac-vlan enable コマンドはポートで MAC アドレスベース VLAN を有効にします。

undo mac-vlan enable コマンドはデフォルトに戻します。

例

GigabitEthernet 1/0/1 で MAC アドレスベース VLAN を有効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] mac-vlan enable

関連コマンド

display mac-vlan interface

10.3.4 mac-vlan mac-address

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* }

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

mac-address *mac-address*: MAC アドレスを指定します。形式は H-H-H です。MAC アドレスはマルチキャスト MAC アドレス、あるいは値がすべて 0 の MAC アドレスを指定することができません。H が 0 である場合、省略できます。たとえば、000f-00e2-0001 を指定する場合、f-e2-1 を入力することで指定できます。

mask *mac-mask*: MAC アドレスのマスクを指定します。*mac-mask* は上位側ビット（全バイナリビット=1）と下位側ビット（全バイナリビット=0）で構成されます。デフォルトは 16 進数ですべて ffff-ffff-ffff です。

vlan *vlan-id*: VLAN ID を指定します。設定範囲は 1～4094 です。

dot1q *priority*: VLAN の 802.1p プライオリティを MAC アドレス-VLAN エントリに指定します。設定範囲は 0～7 です。デフォルトは 0 です。値が高いほどプライオリティは高くなります。

all: すべてのスタティック MAC アドレス-VLAN エントリを削除します。

説明

mac-vlan mac-address コマンドは MAC アドレス-VLAN エントリを設定します。

undo mac-vlan コマンドは MAC アドレス-VLAN エントリを削除します。

スタティックと MAC アドレスベース VLAN の割り当てを行うため、MAC アドレス-VLAN エントリを作成したとき、スタティック VLAN を使用します。

mask を指定することで異なるタイプの MAC アドレス-VLAN エントリが作成されます。

- **mask** を指定したとき、作成された MAC アドレス-VLAN エントリは、MAC アドレスのグループ、VLAN、VLAN の 802.1p プライオリティの関係を示します。
- **mask** を指定しないとき、作成された MAC アドレス-VLAN エントリは、MAC アドレス、VLAN、VLAN の 802.1p プライオリティの関係を示します。

これらの異なるタイプの MAC アドレス-VLAN エントリは 2 つのテーブルに区別されて記録されます。システムは設定に従い 2 つのテーブルをアップデートします。

例

MAC アドレス 0000-0001-0001 を VLAN 100 に関連づけ、エントリの VLAN 100 の 802.1p プライオリティを 7 に指定します。

<Switch> system-view

[Switch] mac-vlan mac-address 0-1-1 vlan 100 dot1q 7

VLAN 100 および 802.1p プライオリティ 4 を、16 進数の上位 6 桁が 121122 の MAC アドレスと関連づけます。

<Switch> system-view

[Switch] mac-vlan mac-address 1211-2222-3333 mask ffff-ff00-0000 vlan 100 dot1q 4

関連コマンド

display mac-vlan

10.3.5 mac-vlan trigger enable

Syntax

mac-vlan trigger enable

undo mac-vlan trigger enable

デフォルト

無効

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

説明

mac-vlan trigger enable コマンドはダイナミック MAC アドレスベース VLAN の割り当てを有効にします。

undo mac-vlan trigger enable コマンドはデフォルトに戻します。

受信パケットの送信元 MAC アドレスが MAC－VLAN エントリで MAC アドレスと完全に一致しているときのみ、ポートの VLAN 割り当てが発生します。

受信したパケットの送信元 MAC アドレスが、MAC アドレス-VLAN エントリに一致した場合のみ、受信ポートをエントリに対応する VLAN に割り当てます。

例

GigabitEthernet 1/0/1 でダイナミック MAC アドレスベース VLAN の割り当てを有効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] mac-vlan trigger enable

関連コマンド

- **mac-vlan mac-address**
- **port pvid forbidden**

10.3.6 port pvid forbidden

Syntax

port pvid forbidden

undo port pvid forbidden

デフォルト

パケットの送信元 MAC アドレスが MAC アドレス-VLAN エントリに一致しないとき、ポートは PVID で転送します。

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

説明

port pvid forbidden コマンドはパケットの送信元 MAC アドレスが MAC アドレス-VLAN エントリに一致しないとき、PVID でのパケットの転送を無効にします。

undo port pvid forbidden コマンドはデフォルトに戻します。

このコマンドはダイナミック MAC アドレスベース VLAN の割り当てに使用します。

例

GigabitEthernet 1/0/1 でパケットの送信元 MAC アドレスが MAC アドレス-VLAN エントリに一致しないとき、PVID でのパケットの転送を無効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] port pvid forbidden

関連コマンド

mac-vlan trigger enable

10.3.7 vlan precedence

Syntax

vlan precedence { **mac-vlan** | **ip-subnet-vlan** }

undo vlan precedence

デフォルト

mac-vlan

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

mac-vlan: MAC アドレスベース VLAN を優先します。

ip-subnet-vlan: IP サブネットベース VLAN を優先します。

説明

vlan precedence コマンドは MAC アドレスベース VLAN と IP サブネットベース VLAN の両方がポートに設定されたときの VLAN の優先順位を設定します。

undo vlan precedence コマンドはデフォルトに戻します。

このコマンドは MAC アドレスベース VLAN と IP サブネットベース VLAN でのみ適用されます。

ダイナミック MAC ベース VLAN が有効なとき、MAC ベース VLAN の優先度を保証するため、**vlan precedence mac-vlan** コマンドを設定することを推奨します。**vlan precedence ip-subnet-vlan** コマンドを使用している場合、このコマンドは適用されません。

例

GigabitEthernet 1/0/1 で MAC アドレスベース VLAN を優先します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] vlan precedence mac-vlan

関連コマンド

mac-vlan trigger enable

10.4 IPサブネットベースVLAN設定コマンド

10.4.1 display ip-subnet-vlan interface

Syntax

display ip-subnet-vlan interface { *interface-type interface-number1* [**to** *interface-type interface-number2*] | **all** }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface-type interface-number1 **to** *interface-type interface-number2*:インタフェース範囲を指定します。*interface-type interface-number1* と *interface-type interface-number2*は、どちらもインタフェースタイプとインタフェース番号を表します。*interface-number2* の値は、*interface-number1* の値以上である必要があります。

all: すべてのポートを指定します。

説明

display ip-subnet-vlan interface コマンドは指定したポートに関連づけられた IP サブネットベース VLAN を表示します。

例

GigabitEthernet1 / 0/1 に IP サブネットベースの VLAN を表示します。

<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
```

表 10-6 コマンド出力

フィールド	説明
VLAN ID	IPサブネットベースVLANのIDです。
Subnet index	IPサブネットのインデックスです。 IPサブネットベースVLANが設定されていない場合、**N/A**と表示されます。
IP address	サブネットのIPアドレスです。IPアドレスあるいはサブネットアドレスです。 VLANのIPサブネットが設定されていない場合、**N/A**と表示されます。
Subnet mask	IPサブネットのマスクです。 VLANのサブネットマスクが設定されていない場合、**N/A**と表示されます。

フィールド	説明

Status	IPサブネットベースVLANがポートで有効になっているかどうかを示します。
	• **Active**–IPサブネットベースVLANが有効です。
	• **Inactive**–IPサブネットベースVLANが有効ではありません。たとえば、次のいずれかの場合、このフィールドには**Inactive**と表示されます。
	  • IPサブネットベースVLANの設定が完了していません。
	  • ポートがIPサブネットベースVLANを許可していません。

関連コマンド

- **display ip-subnet-vlan vlan**
- **ip-subnet-vlan**
- **port hybrid ip-subnet-vlan**

10.4.2 display ip-subnet-vlan vlan

Syntax

display ip-subnet-vlan vlan { *vlan-id1* [**to** *vlan-id2*] | **all** }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

vlan-id1: IP サブネットベース VLAN の VLAN ID を指定します。設定範囲は 1～4094 です。

vlan-id1 **to** *vlan-id2*: VLAN ID の範囲を指定します。設定範囲は 1～4094 です。*vlan-id2* は *vlan-id1* 以上の値にしてください。

all: すべての IP サブネットベース VLAN を指定します。

説明

display ip-subnet-vlan vlan コマンドは IP サブネットベース VLAN の情報を表示します。

例

すべての IP サブネットベース VLAN の情報を表示します。

<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
```

表 10-7 コマンド出力

フィールド	説明
VLAN ID	IPサブネットベースVLANのVLAN IDです。
Subnet index	IPサブネットのインデックスです。
IP address	サブネットのIPアドレスです。IPアドレスあるいはサブネットアドレスです。
Subnet mask	IPサブネットのマスクです。

関連コマンド

- **display ip-subnet-vlan interface**
- **ip-subnet-vlan**
- **port hybrid ip-subnet-vlan**

10.4.3 ip-subnet-vlan

Syntax

ip-subnet-vlan [*ip-subnet-index*] **ip** *ip-address* [*mask*]

undo ip-subnet-vlan { *ip-subnet-index* [**to** *ip-subnet-end*] | **all** }

デフォルト

設定なし

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

ip-subnet-index: IP サブネットの開始インデックスです。設定範囲は 0～65535 です。この値はユーザによって設定することができます。またシステムによって IP サブネットあるいは IP アドレスが VLAN に関連づけられた順番にもとづいて自動で番号が付けられます。

ip *ip-address* [*mask*]: サブネットベース VLAN の分類のもとになっている送信元 IP アドレスまたはネットワークアドレスを、ドット区切り 10 進法で指定します。*mask* は、ドット区切り 10 進法の送信元 IP アドレスまたはネットワークアドレスのサブネットマスクで、デフォルト値は 255.255.255.0 です。

to *ip-subnet-end*: IP サブネットインデックス範囲の終了インデックスを指定します。設定範囲は 0～65535 です。*ip-subnet-end* は IP サブネットの開始インデックス以上の値にしてください。

all: VLAN に関連付けられているすべての IP サブネットまたは IP アドレスを指定します。

説明

ip-subnet-vlan コマンドは指定した IP サブネットまたは IP アドレスに VLAN を関連づけます。

undo ip-subnet-vlan コマンドは指定した IP サブネットまたは IP アドレスから VLAN の関連づけを削除します。

IP サブネットあるいは IP アドレスはマルチキャストネットワークセグメントあるいはマルチキャストアドレスにすることはできません。

例

VLAN 3 を IP サブネットベース VLAN になるよう設定し、これをサブネット 192.168.1.0/24 に関連づけます。

<Switch> system-view

[Switch] vlan 3

[Switch-vlan3] ip-subnet-vlan ip 192.168.1.0 255.255.255.0

関連コマンド

- **display ip-subnet-vlan interface**
- **display ip-subnet-vlan vlan**
- **port hybrid ip-subnet-vlan**

10.4.4 port hybrid ip-subnet-vlan

Syntax

port hybrid ip-subnet-vlan vlan *vlan-id*

undo port hybrid ip-subnet-vlan { **vlan** *vlan-id* | **all** }

デフォルト

設定なし

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

vlan *vlan-id*: VLAN ID を指定します。設定範囲は 1～4094 です。

all: すべての VLAN を指定します。

説明

port hybrid ip-subnet-vlan コマンドはポートを指定の IP サブネットベース VLAN に関連づけます。

undo port hybrid ip-subnet-vlan コマンドは指定した IP サブネットベース VLAN からポートの関連づけを削除します。

このコマンドを有効にするには、次のタスクを実行します。

1. VLAN を作成し、指定した IP サブネットまたは IP アドレスに関連付けます。
2. ポートリンクタイプをハイブリッドに設定します。
3. ポートを設定して、IP サブネットベース VLAN が通過できるようにします。

例

GigabitEthernet 1/0/1 を IP サブネットベース VLAN 3 に関連づけます。

<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

レイヤ 2 アグリゲートインタフェース Bridge-aggregation 1 を IP サブネットベース VLAN 3 に関連づけます。

<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

関連コマンド

- **display ip-subnet-vlan interface**
- **display ip-subnet-vlan vlan**
- **ip-subnet-vlan**

10.5 プロトコルベースVLAN設定コマンド

10.5.1 display protocol-vlan interface

Syntax

display protocol-vlan interface { *interface-type interface-number1* [**to** *interface-type interface-number2*] | **all** }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface-type interface-number1 **to** *interface-type interface-number2*: インタフェースの範囲をインタフェースのタイプと番号で指定します。*interface-number2* は *interface-number1* 以上の値にしてください。

all: すべてのポートを指定します。

説明

display protocol-vlan interface コマンドは指定されたポートに関連づけられたプロトコルベース VLAN の情報を表示します。

例

GigabitEthernet 1/0/1 に関連づけられたプロトコルベース VLAN の情報を表示します。

<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
```

表 10-8 コマンド出力

フィールド	説明
VLAN ID	プロトコルベースVLANのIDです。
Protocol index	プロトコルテンプレートインデックスです。
Protocol type	プロトコルテンプレートで指定されたプロトコルタイプです。 プロトコルタイプが指定されていない場合、**N/A**と表示されます。
Status	プロトコルベースVLANがポートで適用されているかどうかを示します。 ● **Active**–プロトコルベースVLANが適用されています ● **Inactive**–プロトコルベースVLANが適用されていません。

関連コマンド

- **display protocol-vlan vlan**
- **port hybrid protocol-vlan**
- **protocol-vlan**

10.5.2 display protocol-vlan vlan

Syntax

display protocol-vlan vlan { *vlan-id1* [**to** *vlan-id2*] | **all** }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

vlan-id1: プロトコルベース VLAN の VLAN ID を指定します。設定範囲は 1～4094 です。

vlan-id1 **to** *vlan-id2*: VLAN ID の範囲を指定します。設定範囲は 1～4094 です。*vlan-id2* は *vlan-id1* 以上の値にしてください。

all: すべてのプロトコルベース VLAN を指定します。

説明

display protocol-vlan vlan コマンドはプロトコルベース VLAN の情報を表示します。

例

すべてのプロトコルベース VLAN の情報を表示します。

<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
```

表 10-9 コマンド出力

フィールド	説明
VLAN ID	プロトコルベースVLANのIDです。
Protocol index	プロトコルベーステンプレートインデックスです。
Protocol type	プロトコルテンプレートで指定されたプロトコルタイプあるいはカプセル化フォーマットです。

関連コマンド

- **display protocol-vlan interface**
- **port hybrid protocol-vlan**
- **protocol-vlan**

10.5.3 port hybrid protocol-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** }

デフォルト

設定なし

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

vlan *vlan-id*: VLAN ID を指定します。設定範囲は 1～4094 です。

protocol-index: プロトコルテンプレートインデックスの開始インデックスです。設定範囲は 0～65535 です。

to *protocol-end*: プロトコルテンプレートの終了インデックスを指定します。設定範囲は 0～65535 です。*protocol-end* はプロトコルテンプレートの開始インデックス以上の値にしてください。

all: すべてのプロトコルテンプレートを指定します。

説明

port hybrid protocol-vlan コマンドはハイブリッドポートを VLAN の指定されたプロトコルに関連づけます。

undo port hybrid protocol-vlan コマンドは関連づけを削除します。

このコマンドを設定する前に、以下の設定を行ってください。

- VLAN を作成し、VLAN と指定したプロトコルを関連づけてください。
- リンクタイプをハイブリッドに設定してください。
- 通過するプロトコルベース VLAN を許可するポートを設定してください。

undo port hybrid protocol-vlan コマンドを使用するとき、以下のガイドラインに従ってください。

- *vlan-id* と **all** を指定した場合、指定した VLAN のすべてのプロトコルテンプレートからポートの関連づけを削除します。
- **all** のみ指定した場合、すべての VLAN のすべてのプロトコルテンプレートからポートの関連づけを削除します。

例

GigabitEthernet 1/0/1 をハイブリッドインタフェースに設定し、タグなしメンバとして VLAN 2 に割り当てます。プロトコルテンプレート 1 に関連づけます。

<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

ハイブリッドアグリゲートインタフェース Bridge-Aggregation 1 をハイブリッドインタフェースに設定し、タグなしメンバとして VLAN 2 に割り当てます。プロトコルテンプレート 1 に関連づけます。

<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

Syntax

protocol-vlan [*protocol-index*] { **at** | **ipv4** | **ipv6** | **ipx** { **ethernetii** | **llc** | **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** }

デフォルト

設定なし

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

at: AppleTalk ベース VLAN を指定します。

ipv4: IPv4 ベース VLAN を指定します。

ipv6: IPv6 ベース VLAN を指定します。

ipx: IPXベース VLAN を指定します。**ethernetii、llc、raw** および **snap** は IPXのカプセル化フォーマットです。

mode: VLAN 用の自己定義したプロトコルテンプレートを設定します。**ethernetii、llc、**および **snap** は有効なカプセル化フォーマットです。

ethernetii etype *etype-id*: イーサネット 2 カプセル化フォーマットが、対応するプロトコルタイプの値に一致するよう指定します。*etype-id* はインバウンドパケットのプロトコルタイプ ID です。設定範囲は 0x0600～0xffff です。0x0800、0x86DD、0x809B、0x8137 を除きます。

llc: 一致する LLC カプセル化フォーマットを指定します。

dsap *dsap-id*: DSAP（Destination Service Access Point）を指定します。設定範囲は 0x00～0xff です。

ssap *ssap-id*: SSAP（Source Service Access Point）を指定します。設定範囲は 0x00～0xff です。

snap etype *etype-id*: SNAP カプセル化フォーマットと対応するプロトコルタイプの値が一致するよう指定します。*etype-id* はインバウンドパケットのイーサネットタイプです。設定範囲は 0x8137 を除く 0x0600～0xffff です。

protocol-index: プロトコルインデックスを指定します。設定範囲は 0～65535 です。指定しない場合、システムは自動的にインデックスを割り当てます。

to *protocol-end*: プロトコルテンプレートの終了インデックスを指定します。設定範囲は 0～65535 です。*protocol-end* は *protocol-index* 以上の値にしてください。

all: VLAN に割り当てられたすべてのプロトコルを指定します。

説明

⚠ **注意:**

IP はイーサネットのアドレス解決のため ARP を使用します。通信障害を防止するため、同一の VLAN の IP と ARP のテンプレートを設定し、同一のポートでそれらを関連づけてください。

---

protocol-vlan コマンドは VLAN をプロトコルベース VLAN およびプロトコルテンプレートに設定します。

undo protocol-vlan コマンドは設定されているプロトコルテンプレートを削除します。

mode パラメータを使用した場合、以下のガイドラインに従ってください。

- **ethernetii etype** *etype-id* パラメータで以下の *etype-id* の値を設定しないでください。
  - **0x0800**–イーサネット 2 カプセル化フォーマットの IPv4 プロトコル
  - **0x809B**–イーサネット 2 カプセル化フォーマットの AppleTalk プロトコル
  - **0x8137**–イーサネット 2 カプセル化フォーマットの IPX プロトコル

- □ **0x86DD**–イーサネット 2 カプセル化フォーマットの IPv6 プロトコル

- **llc** パラメータを指定した場合、*dsap-id* と *ssap-id* パラメータの両方で以下の設定を行わないでください。
  - □ **0xE0**–IPX パケットの 802.2 LLC カプセル化フォーマット
  - □ **0xFF**–IPX パケットの 802.3 raw カプセル化フォーマット
  - □ **0xAA**–802.2 SNAP カプセル化フォーマット

  dsap-id、*ssap-id* パラメータのどちらかを設定した場合、システムはもう一方に 0xAA を割り当ててください。

- **snap etype** *etype-id* パラメータの *etype-id* パラメータを 0x8137 に設定しないでください。そうでなければテンプレートフォーマットは IPX プロトコルのテンプレートフォーマットと同一になります。*etype-id* パラメータは 0x0800、0x809B、0x86DD に設定することができます。それぞれ IPv4、AppleTalk、IPv6 に対応します。

例

イーサネット 2 カプセル化フォーマットに ARP パケットを割り当て、転送を行うため IPv4 パケットを VLAN 3 に割り当てます。(ARP のプロトコルタイプ ID は 0x0806 です)

<Switch> system-view

[Switch] vlan 3

[Switch-vlan3] protocol-vlan 1 ipv4

[Switch-vlan3] protocol-vlan 2 mode ethernetii etype 0806

関連コマンド

- **display protocol-vlan interface**
- **display protocol-vlan vlan**
- **port protocol-vlan**

目次

このセクションのページは **3-x-x** です。

11 章 Private VLAN 11-1
11.1 Private VLAN 設定コマンド.....11-1
11.1.1 display private-vlan 11-1
11.1.2 port private-vlan host.....11-4
11.1.3 port private-vlan promiscuous 11-5
11.1.4 port private-vlan trunk promiscuous.....11-8
11.1.5 port private-vlan trunk secondary 11-11
11.1.6 private-vlan (VLAN interface view) 11-15
11.1.7 private-vlan (VLAN view).....11-17
11.1.8 private-vlan isolated 11-18
11.1.9 private-vlan primary 11-20

11章 Private VLAN

11.1 Private VLAN設定コマンド

11.1.1 display private-vlan

Syntax

display private-vlan [*primary-vlan-id*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

primary-vlan-id: プライマリ VLAN ID を指定します。設定範囲は 1～4094 です。

プライマリ VLAN を指定しない場合は、すべてのプライマリ VLAN ID と関連するセカンダリ VLAN を表示します。

説明

display private-vlan コマンドはプライマリ VLAN と関連するセカンダリ VLAN の情報を表示します。

例

プライマリ VLAN と関連するセカンダリ VLAN の情報を表示します。

<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
```

表 11-1 コマンド出力

フィールド	説明
VLAN type	VLANタイプを示します。Dynamicまたはstaticを表示します。
Private VLAN type	プライベートVLANタイプ示します。 ● **Primary**：プライマリVLAN ● **Secondary**：セカンダリVLAN ● **Isolated secondary**：L2で隔離したセカンダリVLAN
Route interface	VLANインタフェースのありなしを示します。 ● Configured ● Not configured

フィールド	説明
IPv4 address	VLANインタフェースのプライマリIPv4アドレスを示します。このフィールドはIPv4アドレスを設定しているときに表示されます。セカンダリIPv4アドレスについても同様です。 以下のいずれかのコマンドで確認ができます。 ● display interface vlan-interface. ● display this (VLAN interface view).
IPv4 subnet mask	VLANインタフェースのプライマリIPv4アドレスのサブネットを示します。このフィールドはIPv4アドレスを設定しているときに表示されます。
IPv6 global unicast addresses	VLANインタフェースのグローバルユニキャストIPv6アドレスを示します。このフィールドはIPv6アドレスを設定しているときに表示されます。 IPv6アドレスの状態を以下に示します。 ● **TENTATIVE**：初期状態。DADの処理前か処理中を示します。この状態のアドレスは送信元アドレスまたは宛先アドレスとして使用できません。 ● **DUPLICATE**：DADによるアドレス重複検出。アドレスがユニークでないため使用できません。 ● **PREFERRED**：アドレスがpreferredで送信元または宛先として使用できます。このコマンドではこのアドレスの状態を表示しません。 ● **DEPRECATED**：アドレスがpreferredライフタイムとvalidライフタイムの間にある状態を示します。有効なアドレスですが、新規の通信には使用できません。
Description	VLANの説明を示します。
Name	VLAN名を示します。
Tagged ports	VLANのTaggedメンバを示します。
Untagged ports	VLANのUntaggedメンバを示します。

関連コマンド

- **private-vlan (VLAN view)**
- **private-vlan primary**

11.1.2 port private-vlan host

Syntax

port private-vlan host

undo port private-vlan

デフォルト

設定なし

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

port private-vlan host コマンドはポートをホストポートに設定します。

undo port private-vlan コマンドは設定をデフォルトに戻します。

ポートがセカンダリ VLAN に指定されると、このコマンドはプライマリ VLAN にセカンダリ VLAN を関連付けて割り当てます。設定時には以下のイベントが発生します。

- アクセスポートでは以下の操作が行われます。
  - ポートのリンクタイプをハイブリッドに変更します。
  - セカンダリ VLAN を PVID に設定します。
  - プライマリ VLAN を untagged メンバとして設定します。
- トランクポートではリンクタイプまたは PVID を変更しません。
- ハイブリッドポートではリンクタイプまたは PVID を変更しません。
  - ハイブリッドポートがプライマリ VLAN の tagged または untagged メンバである場合、このメンバはプライマリ VLAN のままとなります。
  - ハイブリッドポートがプライマリ VLAN に割り当てられていない場合、そのポートを untagged メンバとしてプライマリ VLAN に割り当てます。

このコマンドを実行する前でも後でもセカンダリ VLAN の指定ができます。**undo port private-vlan** コマンドはそのポートの VLAN 属性（セカンダリ VLAN、リンクタイプ、PVID）を変更しません。

port private-vlan host コマンドは **port private-vlan trunk promiscuous** コマンドや **port private-vlan trunk secondary** コマンドと相互排他的に動作します。

例

VLAN20 を VLAN2 のプライマリ VLAN のセカンダリ VLAN と設定している装置に実行した場合の例を示します。

GigabitEthernet 1/0/1 をホストポートに設定して、設定を確認します。

```
<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 private-vlan host
#
return
```

GigabitEthernet 1/0/1 を VLAN 20 に設定して、設定を確認します。

```
[Switch-GigabitEthernet1/0/1] port access vlan 20
[Switch-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
 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
```

出力は以下を示します。

- GigabitEthernet 1/0/1 はセカンダリ VLAN20 とプライマリ VLAN2 の untagged メンバです。
- GigabitEthernet 1/0/1 のリンクタイプはハイブリッドで PVID は VLAN20 です。

関連コマンド

- **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

Syntax

port private-vlan *vlan-id* **promiscuous**

undo port private-vlan

デフォルト

設定なし

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id：VLAN ID を指定します。設定範囲は 1～4094 です。VLAN 1 は設定可能な範囲ですが、コマンドによる設定はできません。

説明

port private-vlan promiscuousコマンドは指定した VLAN とポートをその VLAN のプロミスカスポートに設定します。**undo port private-vlan** コマンドはデフォルトに戻します。

指定された VLAN がセカンダリ VLAN を関連付けられているプライマリ VLAN の場合、コマンドは関連付けされているセカンダリ VLAN に割り当てます。設定時には以下のイベントが発生します。

- アクセスポートでは以下の操作が行われます。
  - ポートのリンクタイプをハイブリッドに変更します。
  - プライマリ VLAN を PVID に設定します。
  - ポートをプライマリポートに設定してセカンダリ VLAN を untagged メンバとして設定します。
- トランクポートではリンクタイプまたは PVID を変更しません。
- ハイブリッドポートではリンクタイプまたは PVID を変更しません。
  - ハイブリッドポートがプライマリ VLAN とセカンダリ VLAN に関連付けされている tagged または untagged メンバである場合、このメンバの属性はこれらの VLAN のままとします。
  - ハイブリッドポートがいかなるプライマリ VLAN とセカンダリ VLAN に関連付けられていない場合、装置はこれらの VLAN を untagged メンバとして設定します。

同じポートでこのコマンドを複数回実行すると最後の設定が有効となります。

undo port private-vlan コマンドはポートの VLAN 属性（セカンダリ VLAN、リンクタイプ、PVID）を変更しません。**undo port private-vlan** コマンドをプロミスカスポートで実行すると、VLAN からそのポートを削除します。

このコマンドを実行する前でも後でもプライマリ VLAN の指定ができます。

このコマンドは **port private-vlan trunk promiscuous** コマンドや **port private-vlan trunk secondary** コマンドと相互排他的に動作します。

例

VLAN20 を VLAN2 のプライマリ VLAN のセカンダリ VLAN と設定している装置に実行した場合の例を示します。

GigabitEthernet 1/0/1 の設定情報を表示します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] display this

```
#
interface GigabitEthernet1/0/1
#
return
```

GigabitEthernet 1/0/1 を VLAN2 のプロミスカスポートに設定して設定を確認します。

[Switch-GigabitEthernet1/0/1] port private-vlan 2 promiscuous

[Switch-GigabitEthernet1/0/1] display this

```
#
interface GigabitEthernet1/0/1
 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
```

出力は以下を示します。

- GigabitEthernet 1/0/1 は VLAN2 のプロミスカスポートです。
- GigabitEthernet 1/0/1 はプライマリ VLAN2 とセカンダリ vlan20 の untagged メンバです。
- GigabitEthernet 1/0/1 のリンクタイプはハイブリッドで PVID は VLAN2 です。

GigabitEthernet 1/0/1 で **undo port private-vlan** コマンドを実行して、設定を確認します。

[Switch-GigabitEthernet1/0/1] undo port private-vlan

[Switch-GigabitEthernet1/0/1] display this

#

interface GigabitEthernet1/0/1

```
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 20 untagged
```

```
 port hybrid pvid vlan 2
#
return
```

出力は以下を示します。

- GigabitEthernet 1/0/1 がプライマリ VLAN2 から削除されます。
- GigabitEthernet 1/0/1 は VLAN2 の untagged メンバです。
- GigabitEthernet 1/0/1 のリンクタイプと PVID は変更されません。

関連コマンド

- **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

Syntax

port private-vlan *vlan-id-list* **trunk promiscuous**

undo port private-vlan *vlan-id-list* **trunk promiscuous**

デフォルト

設定なし

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id-list： プライマリ VLAN リストを最大 10 個まで設定します。設定範囲は 1～4094 です。プライマリ VLAN の指定はスペースを空けて指定するか、*vlan-id1* **to** *vlan-id2* の形式で指定します。*vlan-id2* の値は *vlan-id1* の値と同じか大きな値を指定してください。

VLAN 1 は設定可能な範囲ですが、コマンドによる設定はできません。

説明

port private-vlan trunk promiscuous コマンドは指定した VLAN とポートをそれらの VLAN のトランクプロミスカスポートに設定します。

undo port private-vlan trunk promiscuous コマンドは指定した VLAN のトランクプロミスカス属性を解除します。

指定した VLAN はセカンダリ vlan と関連付けされたプライマリ VLAN である場合、そのコマンドはポートを関連付けられたセカンダリ VLAN に割り当てます。設定時には以下のイベントが発生します。

- アクセスポートでは以下の操作が行われます。
  - □ リンクタイプをハイブリッドに変更します。PVID は変更しません。
  - □ ポートをプライマリ VLAN と tagged メンバとして関連付けられたセカンダリ VLAN に設定します。
- トランクポートではリンクタイプまたは PVID を変更しません。
- ハイブリッドポートではリンクタイプまたは PVID を変更しません。
  - □ ハイブリッドポートがプライマリ VLAN とセカンダリ VLAN に関連付けされている tagged または untagged メンバである場合、このメンバの属性はこれらの VLAN のままとします。装置はハイブリッドポートを残りのプライマリ VLAN と tagged メンバとして関連付けられたセカンダリ VLAN に割り当てます。
  - □ ハイブリッドポートがいかなるプライマリ VLAN とセカンダリ VLAN に関連付けられていない場合、装置はこれらの VLAN を tagged メンバとして設定します。

undo コマンドはポートの VLAN 属性（セカンダリ VLAN、リンクタイプ、PVID）を変更しません。

トランクプロミスカスポートで undo コマンドを実行した場合、そのコマンドは *vlan-id-list* によって指定された VLAN からそのポートを削除します。

このコマンドを実行する前でも後でもプライマリ VLAN の指定ができます。

このコマンドは **port private-vlan host** コマンド、**port private-vlan promiscuous** コマンド、**port private-vlan trunk secondary** コマンドと相互排他的に動作します。

複数のプライマリ VLAN を許可するアップリンクポートでは、これらの VLAN を割り当てるために **port private-vlan trunk promiscuous** コマンドを使用してください。そのポートはプライマリ VLAN からタグ VLAN でパケットを転送します。1 つのプライマリ VLAN を許可するアップリンクポートでは、その VLAN を割り当てるために **port private-vlan promiscuous** コマンドを使用してください。そのポートはプライマリ VLAN からタグなし VLAN でパケットを転送します。

例

VLAN2 と 3 をプライマリ VLAN、VLAN2 をセカンダリ VLAN20、VLAN3 をセカンダリ VLAN30 と関連付けしている装置に実行した場合の例を示します。

GigabitEthernet 1/0/1 の設定情報を確認します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] display this

```
#
interface GigabitEthernet1/0/1
#
return
```

GigabitEthernet 1/0/1 を VLAN2 と 3 のトランクプロミスカスポートに設定して、設定を確認します。

[Switch-GigabitEthernet1/0/1] port private-vlan 2 3 trunk promiscuous

[Switch-GigabitEthernet1/0/1] display this

```
#
interface GigabitEthernet1/0/1
 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
```

出力は以下を示します。

- GigabitEthernet 1/0/1 は VLAN2 と 3 のトランクプロミスカスポートです。
- GigabitEthernet1/0/1 は VLAN2,3,20,30 の tagged メンバです。
- GigabitEthernet 1/0/1 のリンクタイプはハイブリッドです。

GigabitEthernet 1/0/1 で **undo port private-vlan trunk promiscuous** コマンドを実行して設定を確認します。

[Switch-GigabitEthernet1/0/1] undo port private-vlan 2 3 trunk promiscuous

[Switch-GigabitEthernet1/0/1] display this

```
#
interface GigabitEthernet1/0/1
 port link-type hybrid
 port hybrid vlan 20 30 tagged
 port hybrid vlan 1 untagged
#
return
```

出力は以下を示します。

- GigabitEthernet 1/0/1 は VLAN2 と 3 から削除されています。
- GigabitEthernet 1/0/1 は vlan20,30 の tagged メンバです。
- GigabitEthernet 1/0/1 のリンクタイプと PVID は変更されません。

関連コマンド

- **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

Syntax

port private-vlan *vlan-id-list* **trunk secondary**

undo port private-vlan *vlan-id-list* **trunk secondary**

デフォルト

設定なし

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id-list： セカンダリ VLAN リストを最大 10 個まで設定します。設定範囲は 1～4094 です。セカンダリ VLAN の指定はスペースを空けて指定するか、*vlan-id1* **to** *vlan-id2* の形式で指定します。v*lan-id2* の値は *vlan-id1* の値と同じか大きな値を指定してください。

VLAN 1 は設定可能な範囲ですが、コマンドによる設定はできません。

説明

指定された VLAN がプライマリ VLAN に関連付けられたセカンダリ VLAN の場合、コマンドはそのポートを関連付けされたプライマリ VLAN にも割り当てます。以下のイベントが発生します。

- アクセスポートでは以下の操作が行われます。
  - □ リンクタイプをハイブリッドに変更します。ポートの PVID は変更しません。
  - □ そのポートをセカンダリ VLAN と関連付けられたプライマリ VLAN に tagged メンバとして割り当てます。
- トランクポートでは装置はリンクタイプまたは PVID を変更しません。
- ハイブリッドポートでは装置はリンクタイプまたは PVID を変更しません。
  - □ そのポートがセカンダリ VLAN とそれらに関連付けられたプライマリ VLAN の untagged または tagged メンバの場合、このメンバ属性はこれらの VLAN に残ります。装置はポートを残りのセカンダリ VLAN と tagged メンバとして関連付けられたプライマリ VLAN に割り当てます。

□ ハイブリッドポートがいかなるセカンダリ VLAN や関連付けられたプライマリ VLAN にも許可されていない場合、装置はそのポートをこれらの VLAN に tagged メンバとして割り当てます。

トランクセカンダリポートはプライマリ VLAN と関連付けられたすべてのセカンダリ VLAN のうち 1 つのセカンダリ VLAN だけに関連付けできますが、プライマリ VLAN が異なる場合は複数のセカンダリ VLAN への関連付けができます。

undo コマンドはポートの VLAN 属性（プライマリ VLAN、リンクタイプ、PVID）は変更しません。

vlan-id-list によって指定された VLAN のトランクセカンダリポート上で undo コマンドを実行した場合、以下のうち 1 つのイベントが発生します。

- ポートがアクセスポートの場合、装置はそのポートの VLAN 設定を変更しません。
- ポートがトランクポートまたはハイブリッドポートの場合、装置は指定された VLAN からそのポートを削除します。
- このコマンドを実行する前でも後でもプライマリ VLAN の指定ができます。

このコマンドを実行する前でも後でも指定された VLAN をそれぞれのプライマリ VLAN と関連付けできます。

このコマンドは以下の条件では指定された VLAN 上で動作しません。

- 指定された VLAN が存在しません。
- 指定された VLAN がセカンダリ VLAN ではなく、他の目的に使用されています。
- 指定された VLAN が同じプライマリ VLAN を他のセカンダリ VLAN と共有し、現在のポートが他のセカンダリポートの 1 つでトランクセカンダリポートとして設定されています。

このコマンドは **port private-vlan host** コマンド、**port private-vlan promiscuous** コマンド、**port private-vlan trunk promiscuous** コマンドと相互排他的に動作します。

異なるプライマリ VLAN と関連付けされた複数のセカンダリ VLAN を許可するダウンリンクポートでは、そのポートをセカンダリ VLAN に割り当てるために **port private-vlan trunk secondary** コマンドを使用してください。そのポートはセカンダリ VLAN から VLAN タグ付きパケットを転送します。1 つのセカンダリ VLAN だけ許可するダウンリンクポートの場合は、セカンダリ VLAN を割り当てるために **port private-vlan host command** を使用してください。そのポートはセカンダリ VLAN から VLAN タグなしパケットを転送します。

例

- この例では、VLAN2 と 3 がプライマリ VLAN で、VLAN2 が VLAN20 のセカンダリ VLAN に関連付け、VLAN3 が VLAN30 のセカンダリ VLAN に関連付けされています。

GigabitEthernet 1/0/1 の設定情報を確認します。

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] display this
#
```

```
interface GigabitEthernet1/0/1
#
return
```

GigabitEthernet 1/0/1 を VLAN20 と 30 のトランクセカンダリポートに設定して、設定情報を確認します。

[Switch-GigabitEthernet1/0/1] port private-vlan 20 30 trunk secondary

[Switch-GigabitEthernet1/0/1] display this

```
#
interface GigabitEthernet1/0/1
 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
```

出力は以下を示します。

- GigabitEthernet 1/0/1 は VLAN20 と 30 のトランクセカンダリポートです。
- GigabitEthernet 1/0/1 は VLAN2、3、20、30 の tagged メンバです。
- GigabitEthernet 1/0/1 のリンクタイプはハイブリッドです。

undo port private-vlan trunk secondary コマンドを GigabitEthernet 1/0/1 で実行して、設定を確認します。

[Switch-GigabitEthernet1/0/1] undo port private-vlan 20 30 trunk secondary

[Switch-GigabitEthernet1/0/1] display this

```
#
interface GigabitEthernet1/0/1
 port link-type hybrid
 port hybrid vlan 2 3 tagged
 port hybrid vlan 1 untagged
#
return
```

出力は以下を示します。

- GigabitEthernet 1/0/1 が VLAN20 と 30 から削除されました。
- GigabitEthernet 1/0/1 は VLAN2 と 3 の tagged メンバです。
- GigabitEthernet 1/0/1 のリンクタイプと PVID は変更されません。

- この例では、VLAN10 がセカンダリ VLAN ではありません。

GigabitEthernet 1/0/1 の設定情報を確認します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] display this

```
#
interface GigabitEthernet1/0/1
#
return
```

GigabitEthernet 1/0/1 を VLAN10 のトランクセカンダリポートに設定して、設定情報を確認します。

[Switch-GigabitEthernet1/0/1] port private-vlan 10 trunk secondary

[Switch-GigabitEthernet1/0/1] display this

```
#
interface GigabitEthernet1/0/1
 port link-type hybrid
 port hybrid vlan 10 tagged
 port hybrid vlan 1 untagged
 port private-vlan 10 trunk secondary
#
return
```

出力は以下を示します。

- GigabitEthernet 1/0/1 は VLAN10 のトランクセカンダリポートです。
- GigabitEthernet 1/0/1 は VLAN10 の tagged メンバポートです。
- GigabitEthernet 1/0/1 のリンクタイプはハイブリッドです。

undo port private-vlan trunk secondary コマンドを GigabitEthernet1/0/1 で実行して、設定情報を確認します。

[Switch-GigabitEthernet1/0/1] undo port private-vlan 10 trunk secondary

[Switch-GigabitEthernet1/0/1] display this

```
#
interface GigabitEthernet1/0/1
 port link-type hybrid
 port hybrid vlan 1 untagged
#
return
```

出力は以下を示します。

- GigabitEthernet 1/0/1 が VLAN10 から削除されました。
- GigabitEthernet 1/0/1 のリンクタイプと PVID は変更されません。

関連コマンド

- **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)

Syntax

private-vlan secondary *vlan-id-list*

undo private-vlan [**secondary** *vlan-id-list*]

デフォルト

セカンダリ VLAN はレイヤ 3 で隔離されます。

View

VLAN interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id-list： セカンダリ VLAN リストを最大 10 個まで設定します。設定範囲は 1～4094 です。セカンダリ VLAN の指定はスペースを空けて指定するか、*vlan-id1* **to** *vlan-id2* の形式で指定します。v*lan-id2* の値は *vlan-id1* の値と同じか大きな値を指定してください。

VLAN 1 は設定可能な範囲ですが、コマンドによる設定はできません。

説明

private-vlan secondary コマンドはプライマリ VLAN と関連付けられたセカンダリ VLAN 間のレイヤ 3 通信を有効にします。

undo private-vlan コマンドはプライマリ VLAN と関連付けられたセカンダリ VLAN 間のレイヤ 3 通信を無効にします。

このコマンドは以下の条件で動作します。

- コマンドはプライマリ VLAN インタフェースの VLAN interface view で実行されます。
- セカンダリ VLAN はプライマリ VLAN と関連付けられます。
- セカンダリ VLAN には VLAN インタフェースは作成されません。
- IP アドレスはプライマリ VLAN インタフェースに割り当てられます。
- プライマリ VLAN インタフェースのローカルプロキシ ARP が有効です。

レイヤ 3 通信が有効ではないセカンダリ VLAN のために VLAN インタフェースを作成できます。セカンダリ VLAN でレイヤ 3 通信が有効である場合は、この機能のために VLAN インタフェースを作成しないでください。

このコマンドを同じプライマリ VLAN インタフェース上で複数実行した場合、すべての指定されたセカンダリ VLAN がレイヤ 3 で通信が可能です。

undo private-vlan を実行する場合は、以下のガイドラインに従ってください。

- **secondary** *vlan-id-list* オプションを指定する場合は、指定されたセカンダリ VLAN に対するレイヤ 3 通信の設定を削除してください。
- **secondary** *vlan-id-list* オプションを指定しない場合は、プライマリ VLAN のすべてのセカンダリ VLAN に対するレイヤ 3 通信の設定を削除してください。

例

この例の要件を以下に示します。

- VLAN4 はプライマリ VLAN2 に関連付けるセカンダリ VLAN です。
- アップリンクポート(GigabitEthernet 1/0/2)は VLAN2 のプロミスカスポートです。
- ダウンリンクポート(GigabitEthernet 1/0/3 と GigabitEthernet 1/0/4)はそれぞれ VLANs 3 と 4 のホストポートです。
- セカンダリ VLAN3 と 4 はレイヤ 3 通信ができます。

VLAN 2 をプライマリ VLAN に設定してセカンダリ VLAN3 と 4 を関連付けます。

<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

GigabitEthernet 1/0/2 を VLAN2 のプロミスカスポートに設定します。

[Switch] interface gigabitethernet 1/0/2

[Switch-GigabitEthernet1/0/2] port private-vlan 2 promiscuous

[Switch-GigabitEthernet1/0/2] quit

GigabitEthernet 1/0/3 を VLAN 3 に割り当てホストポートに設定します。

[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

GigabitEthernet 1/0/4 を VLAN 4 に割り当てホストポートに設定します。

[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

VLAN インタフェース 2 を作成して、VLAN3 と 4 とのレイヤ 3 通信を有効にします。

[Switch] interface vlan-interface 2

[Switch-Vlan-interface2] private-vlan secondary 3 to 4

IP アドレスを VLAN インタフェース 2 に割り当てます。

[Switch-Vlan-interface2] ip address 192.168.1.1 255.255.255.0

ローカルプロキシ ARP を VLAN インタフェース 2 で有効にします。

[Switch-Vlan-interface2] local-proxy-arp enable

関連コマンド

- **private-vlan (VLAN view)**
- **private-vlan primary**

11.1.7 private-vlan (VLAN view)

Syntax

private-vlan secondary *vlan-id-list*

undo private-vlan [**secondary** *vlan-id-list*]

デフォルト

プライマリ VLAN とセカンダリ VLAN の関連付けはありません。

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

vlan-id-list： セカンダリ VLAN リストを最大 10 個まで設定します。設定範囲は 1～4094 です。セカンダリ VLAN の指定はスペースを空けて指定するか、*vlan-id1* **to** *vlan-id2* の形式で指定します。*vlan-id2* の値は *vlan-id1* の値と同じか大きな値を指定してください。

VLAN 1 は設定可能な範囲ですが、コマンドによる設定はできません。

説明

private-vlan コマンドはプライマリ VLAN に指定したセカンダリ VLAN に関連付けます。

undo private-vlan コマンドは指定したセカンダリ VLAN とプライマリ VLAN の関連付けを削除します。

プライマリ VLAN は複数のセカンダリ VLAN と関連付けできます。このコマンドを同じ VLAN view で複数回実行すると、すべての指定されたセカンダリ VLAN がプライマリ VLAN に関連付けされます。

設定コマンドの同期動作は以下の条件に従います。

- このコマンドはプライマリ VLAN に設定されます。

- ポートはプロミスカス、トランクプロミスカス、またはホストポートです。

undo private-vlan コマンドを実行する場合は, 以下のガイドラインに従ってください。

- **secondary** *vlan-id-list* オプションを指定する場合は、このコマンドは指定されたセカンダリ VLAN からプライマリ VLAN との関連付けを削除します。
- **secondary** *vlan-id-list* オプションを指定しない場合は、このコマンドはすべてのセカンダリ VLAN からプライマリ VLAN との関連付けを削除します。

例

プライマリ VLAN2 とセカンダリ VLAN2 と 3 を関連付けます。

<Switch> system-view

[Switch] vlan 3 to 4

[Switch] vlan 2

[Switch-vlan2] private-vlan primary

[Switch-vlan2] private-vlan secondary 3 to 4

関連コマンド

- **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

Syntax

private-vlan isolated

undo private-vlan isolated

デフォルト

同じセカンダリ VLAN に属するポート間でレイヤ 2 通信ができます。

View

VLAN view

定義済みユーザロール

network-admin

説明

private-vlan isolated コマンドは同じセカンダリ VLAN のレイヤ 2 通信を隔離します。

undo private-vlan isolated コマンドは設定をデフォルトに戻します。

このコマンドは以下の条件で動作します。

- セカンダリ VLAN はプライマリ VLAN に関連付けされています。
- ポートはセカンダリ VLAN のホストポートまたはトランクセカンダリポートに設定されています。

例

この例の要件を以下に示します。

- VLAN4 はプライマリ VLAN2 に関連付けられたセカンダリ VLAN です。
- GigabitEthernet 1/0/1 は VLAN2 のプロミスカスポートです。
- GigabitEthernet 1/0/2 と GigabitEthernet 1/0/3 はホストポートです。
- GigabitEthernet 1/0/2 と GigabitEthernet 1/0/3 はセカンダリ VLAN4 をレイヤ 2 で隔離します。

VLAN2 とプライマリ VLAN とし、セカンダリ VLAN4 と関連付けます。

<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

GigabitEthernet 1/0/1 を VLAN2 のプロミスカスポートに設定します。

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] port private-vlan 2 promiscuous

[Switch-GigabitEthernet1/0/1] quit

GigabitEthernet 1/0/2 を VLAN4 に割り当てホストポートに設定します。

[Switch] interface gigabitethernet 1/0/2

[Switch-GigabitEthernet1/0/2] port access vlan 4

[Switch-GigabitEthernet1/0/2] port private-vlan host

GigabitEthernet 1/0/3 を VLAN 4 に割り当てホストポートに設定します。

[Switch] interface gigabitethernet 1/0/3

[Switch-GigabitEthernet1/0/3] port access vlan 4

[Switch-GigabitEthernet1/0/3] port private-vlan host

セカンダリ VLAN4 のレイヤ 2 を隔離します。

[Switch] vlan 4

[Switch-vlan4] private-vlan isolated

関連コマンド

- **private-vlan (VLAN view)**
- **private-vlan primary**

11.1.9 private-vlan primary

Syntax

private-vlan primary

undo private-vlan primary

デフォルト

設定なし

View

VLAN view

定義済みユーザロール

network-admin

説明

private-vlan primary コマンドは VLAN をプライマリ VLAN に設定します。

undo private-vlan primary コマンドは設定をデフォルトに戻します。

設定コマンドの同期動作は以下の条件に従います。

- このコマンドはセカンダリ VLAN と関連付けられた VLAN に設定されます。
- ポートはプロミスカス、トランクプロミスカス、ホスト、トランクセカンダリポートです。

例

VLAN5 をプライマリ VLAN に設定します。

<Switch> system-view

[Switch] vlan 5

[Switch-vlan5] private-vlan primary

関連コマンド

- **port private-vlan host**
- **port private-vlan promiscuous**
- **port private-vlan trunk promiscuous**
- **port private-vlan trunk secondary**
- **private-vlan primary**

目次

このセクションのページは **3-x-x** です。

12 章 Voice VLAN 12-1
12.1 Voice VLAN 設定コマンド.....12-1
12.1.1 display voice-vlan mac-address 12-1
12.1.2 display voice-vlan state 12-2
12.1.3 voice-vlan aging.....12-3
12.1.4 voice-vlan enable.....12-4
12.1.5 voice-vlan mac-address 12-5
12.1.6 voice-vlan mode auto 12-6
12.1.7 voice-vlan qos 12-7
12.1.8 voice-vlan qos trust 12-8
12.1.9 voice-vlan security enable 12-9

12章 Voice VLAN

12.1 Voice VLAN設定コマンド

12.1.1 display voice-vlan mac-address

Syntax

display voice-vlan mac-address

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display voice-vlan mac-addressコマンドは装置でサポートされている OUI アドレスを表示します。

例

#装置でサポートされている OUI アドレスを表示します。

<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
```

表 12-1 コマンド出力

フィールド	説明
OUI address	装置で許可されるOUIアドレスです。
Mask	OUIアドレスのマスクです。

フィールド	説明
Description	OUIアドレスの説明です。

関連コマンド

voice-vlan mac-address

12.1.2 display voice-vlan state

Syntax

display voice-vlan state

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display voice-vlan state コマンドは voice VLAN の情報を表示します。

例

voice VLAN の情報を表示します。

<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
```

表 12-2 コマンド出力

フィールド	説明
Current Voice VLANs	既存のvoice VLANの番号です。
Voice VLAN security mode	voice VLAN動作モードです。 ● **Security**ーセキュリティモードです。 ● **Normal**ー通常モードです。

フィールド	説明
Voice VLAN enabled ports and their modes	voice VLANが有効なポートとvoice VLANの動作モードです。
Port	voice VLANが有効なポートの名前です。
VLAN	ポートのvoice VLAN IDです。
Mode	ポートのvoice VLAN動作モードです。 ● **Auto**－自動です。 ● **Normal**－手動です。

関連コマンド

- **voice-vlan aging**
- **voice-vlan enable**
- **voice-vlan mode auto**
- **voice-vlan security enable**

12.1.3 voice-vlan aging

Syntax

voice-vlan aging *minutes*

undo voice-vlan aging

デフォルト

1440 分（24 時間）

View

System view

定義済みユーザロール

network-admin

パラメータ

minutes: voice VLAN のエージングタイマを設定します。設定範囲は 5～43200 分です。

説明

voice-vlan aging コマンドは voice VLAN のエージングタイマを設定します。

undo voice-vlan aging コマンドはデフォルトに戻します。

自動 voice VLAN 動作モードで、voice VLAN にポートを割り当てるとき、システムは voice VLAN のエージングタイマを開始します。エージングタイマが終了する前にポートで voice パケットを受信しない場合、システムは voice VLAN からポートを削除します。

このコマンドは自動 voice VLAN 動作モードでのみ有効です。

例

エージングタイマを 100 分に設定します。

<Switch> system-view

[Switch] voice-vlan aging 100

関連コマンド

display voice-vlan state

12.1.4 voice-vlan enable

Syntax

voice-vlan *vlan-id* **enable**

undo voice-vlan [*vlan-id*] **enable**

デフォルト

無効

View

Layer 2 aggregate interface view

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id: voice VLAN の ID を指定します。設定範囲は 2～4094 です。

説明

voice-vlan enable コマンドは voice VLAN 機能を有効にします。

undo voice-vlan enable コマンドは voice VLAN 機能を無効にします。

このコマンドは自動 voice VLAN 動作モードのハイブリッドあるいはトランクポートで動作するポートでのみ有効です。

voice-vlan enable コマンドを実行する前に、VLAN が作成されていることを確認してください。

例

GigabitEthernet 1/0/1 で voice VLAN 機能を有効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] voice-vlan 2 enable

関連コマンド

- **display voice-vlan state**
- **voice-vlan mode auto**

12.1.5 voice-vlan mac-address

Syntax

voice-vlan mac-address *mac-address* **mask** *oui-mask* [**description** *text*]

undo voice-vlan mac-address *oui*

デフォルト

システムのデフォルト OUI アドレスを表 12-3 に示します。

表 12-3 デフォルト OUI アドレス

番号	OUI アドレス	ベンダ
1	0001-E300-0000	Siemens phone
2	0003-6B00-0000	Cisco phone
3	0004-0D00-0000	Avaya phone
4	0060-B900-0000	Philips/NEC phone
5	00D0-1E00-0000	Pingtel phone
6	00E0-7500-0000	Polycom phone
7	00E0-BB00-0000	3Com phone

View

System view

定義済みユーザロール

network-admin

パラメータ

mac-address: 音声トラフィックの送信元 MAC アドレスを指定します。形式は H-H-H です。たとえば、1234-1234-1234 です。

mask *oui-mask*: OUI アドレスの有効な長さをマスクで指定します。マスクは連続した 1 と 0 です。たとえば、FFFF-0000-0000 です。ベンダの音声装置をフィルタする場合、FFFF-FF00-0000 を設定します。

description *text*: OUI アドレスの説明を指定します。設定範囲は 1～30 です。大文字、小文字を区別します。

oui: 削除する OUI アドレスを指定します。形式は H-H-H です。たとえば、1234-1200-0000 です。OUI アドレスは *mac-address* と *oui-mask* の論理積です。ブロードキャストアドレス、マルチキャストアドレス、すべてが 0 のアドレスを含むことはできません。

説明

voice-vlan mac-address コマンドは音声パケットを識別するために OUI アドレスの情報を設定します。

undo voice-vlan mac-address コマンドは OUI アドレスを削除します。

システムのデフォルト OUI アドレスを手動で削除あるいは追加することができます。

システムはシステムデフォルト OUI アドレスを含み最大 128 までの OUI アドレスをサポートします。

例

MAC アドレス 1234-1234-1234 とマスク ffff-ff00-0000 を指定し、OUI アドレス 1234-1200-0000 を追加します。OUI アドレスの説明は PhoneA です。

<Switch> system-view

[Switch] voice-vlan mac-address 1234-1234-1234 mask ffff-ff00-0000 description PhoneA

関連コマンド

display voice-vlan mac-address

12.1.6 voice-vlan mode auto

Syntax

voice-vlan mode auto

undo voice-vlan mode auto

デフォルト

自動 voice VLAN 動作モードでポートは動作します。

View

Layer 2 aggregate interface view

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

説明

voice-vlan mode auto コマンドは自動 voice VLAN 動作モードで動作するポートを設定します。

undo voice-vlan mode auto コマンドは手動 voice VLAN 動作モードで動作するポートを設定します。

voice VLAN 機能が有効で手動モードで動作するポートでは、voice VLAN を適用するために手動で voice VLAN にポートを割り当てる必要があります。

例

GigabitEthernet 1/0/1 を手動 voice VLAN 動作モードで動作するように設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] undo voice-vlan mode auto

関連コマンド

display voice-vlan state

12.1.7 voice-vlan qos

Syntax

voice-vlan qos *cos-value dscp-value*

undo voice-vlan qos

デフォルト

CoS は 6、DSCP は 46 です。

View

Layer 2 aggregate interface view

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

cos-value: CoS を指定します。設定範囲は 0～7 です。値が大きいほどプライオリティが高くなります。

dscp-value: DSCP を指定します。設定範囲は 0～63 です。値が大きいほどプライオリティが高くなります。

説明

voice-vlan qos コマンドは、入力 voice VLAN パケットの CoS、DSCP をポートで変更するように設定します。

undo voice-vlan qos コマンドはデフォルトに戻します。

ポートでコマンドを設定する前に、voice VLAN 機能が無効であることを確認してください。

voice-vlan qos コマンドと **voice-vlan qos trust** コマンドの両方を設定した場合、最後に行った設定が適用されます。

例

GigabitEthernet 1/0/1 の voice VLAN の CoS を 5、DSCP を 45 に変更します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] voice-vlan qos 5 45

関連コマンド

voice-vlan qos trust

12.1.8 voice-vlan qos trust

Syntax

voice-vlan qos trust

undo voice-vlan qos

デフォルト

CoS は 6、DSCP は 46 です。

View

Layer 2 aggregate interface view

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

説明

voice-vlan qos trust コマンドは入力 voice VLAN パケットのプライオリティの設定を信用し、ポートのプライオリティとして設定します。

undo voice-vlan qos コマンドはデフォルトに戻します。

ポートが入力 voice VLAN パケットの QoS プライオリティの設定を信用したとき、ポートは CoS、DSCP の値を変更しません。

ポートでコマンドを設定する前に、voice VLAN 機能が無効であることを確認してください。

voice-vlan qos コマンドと **voice-vlan qos trust** コマンドの両方を設定した場合、最後に行った設定が適用されます。

例

#入力 voice VLAN パケットのプライオリティの設定を信用し、GigabitEthernet 1/0/1 のプライオリティとして設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] voice-vlan qos trust

関連コマンド

voice-vlan qos

12.1.9 voice-vlan security enable

Syntax

voice-vlan security enable

undo voice-vlan security enable

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

voice-vlan security enable コマンドは voice VLAN のセキュリティモードを有効にします。

undo voice-vlan security enable コマンドは voice VLAN のセキュリティモードを無効にします。

セキュリティモードでは送信元 MAC アドレスが OUI アドレスに一致する音声パケットのみ voice VLAN に転送することができます。

通常モードでは、voice VLAN は音声パケットに加えて非音声パケットも転送します。

例

voice VLAN のセキュリティモードを無効にします。

<Switch> system-view

[Switch] undo voice-vlan security enable

関連コマンド

display voice-vlan state

目次

このセクションのページは **3-x-x** です。

13 章 QinQ 13-1
13.1 QinQ 設定コマンド 13-1
13.1.1 display qinq 13-1
13.1.2 qinq enable 13-2
13.1.3 qinq ethernet-type (interface view) 13-3
13.1.4 qinq ethernet-type (system view) 13-4
13.1.5 qinq transparent-vlan 13-6

13章 QinQ

13.1 QinQ設定コマンド

13.1.1 display qinq

Syntax

display qinq [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: インタフェースのタイプと番号を指定します。指定しない場合、QinQ が有効なすべてのインタフェースを表示します。

説明

display qinq コマンドは QinQ が有効なインタフェースを表示します。

インタフェースで QinQ が無効である場合、表示されません。

例

GigabitEthernet 1/0/1 で QinQ を有効にします。QinQ がインタフェースで有効であるかどうかを確認します。

<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
```

GigabitEthernet 1/0/1、GigabitEthernet 1/0/3 で QinQ を有効にします。QinQ がインタフェースで有効であるかどうかを確認します。

<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
```

関連コマンド

qinq enable

13.1.2 qinq enable

Syntax

qinq enable

undo qinq enable

デフォルト

無効

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

qinq enable コマンドはインタフェースで QinQ を有効にします。

undo qinq enable コマンドはデフォルトに戻します。

例

GigabitEthernet 1/0/1 で QinQ を有効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] qinq enable

関連コマンド

display qinq

13.1.3 qinq ethernet-type (interface view)

Syntax

qinq ethernet-type service-tag *hex-value*

undo qinq ethernet-type service-tag

デフォルト

0x8100

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

service-tag: SVLAN タグに TPID 値を設定します。

hex-value: 16 進数の TPID を設定します。設定範囲は 0x0001～0xffff です。表 13-1 に示す予約済み EtherType 値を除きます。

表 13-1 予約済み EtherType 値

プロトコルタイプ	値
ARP	0x0806
PUP	0x0200
RARP	0x8035
IP	0x0800
IPv6	0x86dd
PPPoE	0x8863/0x8864
MPLS	0x8847/0x8848
IPX/SPX	0x8137
IS-IS	0x8000

プロトコルタイプ	値
LACP	0x8809
802.1X	0x888e
802.1ag	0x8902
LLDP	0x88cc
Cluster	0x88a7
Reserved	0xfffd/0xfffe/0xffff

説明

qinq ethernet-type コマンドはインタフェースの SVLAN タグの TPID を設定します。

undo qinq ethernet-type コマンドはインタフェースの SVLAN タグのデフォルト TPID に戻します。

QinQ が有効になっていないポートは、SVLAN TPID を使用して入力タグ付きフレームを照合します。ポートは、出力フレームの SVLAN タグ内の TPID を設定値として変更します。

例

GigabitEthernet 1/0/1 の SVLAN タグの TPID 値を 9100（16 進数）に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] qinq ethernet-type service-tag 9100

関連コマンド

qinq ethernet-type (system view)

13.1.4 qinq ethernet-type (system view)

Syntax

qinq ethernet-type customer-tag *hex-value*

undo qinq ethernet-type customer-tag

デフォルト

0x8100

View

System view

定義済みユーザロール

network-admin

パラメータ

customer-tag： CVLAN タグの TPID 値を設定します。

hex-value: 16 進数の TPID を設定します。設定範囲は 0x0001～0xffff です。表 13-2 に示す予約済み EtherType 値を除きます。

表 13-2 予約済み EtherType 値

プロトコルタイプ	値
ARP	0x0806
PUP	0x0200
RARP	0x8035
IP	0x0800
IPv6	0x86dd
PPPoE	0x8863/0x8864
MPLS	0x8847/0x8848
IPX/SPX	0x8137
IS-IS	0x8000
LACP	0x8809
802.1X	0x888e
802.1ag	0x8902
LLDP	0x88cc
Cluster	0x88a7
Reserved	0xfffd/0xfffe/0xffff

説明

qinq ethernet-type コマンドは CVLAN タグの TPID を設定します。

undo qinq ethernet-type コマンドは CVLAN タグのデフォルト TPID に戻します。

例

CVLAN タグの TPID 値を 8200（16 進数）に設定します。

<Switch> system-view

[Switch] qinq ethernet-type customer-tag 8200

関連コマンド

qinq ethernet-type (interface view)

13.1.5 qinq transparent-vlan

Syntax

qinq transparent-vlan *vlan-id-list*

undo qinq transparent-vlan { *vlan-id-list* | **all** }

デフォルト

無効

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id-list: インタフェースを指定します。半角スペースで区切り 10 まで設定するか、VLAN ID の範囲で設定することができます。VLAN を範囲で指定する形式は *vlan-id1* **to** *vlan-id2* です。設定範囲は 1～4094 です。*vlan-id2* は *vlan-id1* 以上の値にしてください。

all: 既存のすべての VLAN を指定します。

説明

qinq transparent-vlan コマンドはポートの VLAN のリストでトランスペアレントな転送を有効にします。

undo qinq transparent-vlan コマンドはポートの VLAN のリストでトランスペアレントな転送を無効にします。

デフォルトで、QinQ はポートの PVID のすべての入力フレームにタグをつけます。このコマンドは QinQ で VLAN リストからの入力トラフィックにタグをつけることを無効にします。この VLAN はトランスペアレント VLAN と呼ばれます。

トランスペアレント VLAN のリストに VLAN を追加する場合、コマンドを繰り返してください。

トランスペアレント VLAN の転送を正常に行うため、以下の設定ガイドラインに従ってください。

- ポートのリンクタイプをトランクあるいはハイブリッドに設定し、PVID とトランスペアレント VLAN にポートを割り当ててください。
- ポートでトランスペアレント VLAN を行うため、他の VLAN を操作するアクションを設定しないでください。
- 転送経路上にあるすべてのポートで VLAN を通過できることを確認してください。
- インタフェースでトランスペアレント VLAN と VLAN マッピングの両方を使用する場合、トランスペアレント VLAN は、送信元の VLAN あるいは one-to-one VLAN マッピング、one-to-two VLAN マッピングで転送される VLAN にすることができません。

例

トランクポートとして GigabitEthernet 1/0/1 を設定し、VLAN 2、VLAN 3、VLAN 50 ～ VLAN 100 に割り当てます。GigabitEthernet 1/0/1 で QinQ を有効にし、VLAN 2 からのフレームをトランスペアレントに転送するようにポートを設定します。

```
<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
```

目次

このセクションのページは **3-x-x** です。

14 章 VLAN マッピング 14-1
14.1 VLAN マッピング設定コマンド 14-1
14.1.1 display vlan mapping 14-1
14.1.2 vlan mapping 14-2

14章 VLAN マッピング

⚠ **重要**：

QX-S5100G シリーズは、下記インタフェースでの VLAN マッピングをサポートしておりません。

- リンクアグリゲーションインタフェース
- ハイブリッドポートの untag VLAN
- アクセスポート

14.1 VLANマッピング設定コマンド

14.1.1 display vlan mapping

Syntax

display vlan mapping [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: インタフェースのタイプと番号を指定します。指定しない場合、すべてのインタフェースの VLAN マッピングを表示します。

説明

display vlan mapping コマンドは VLAN マッピングを表示します。

例

すべてのインタフェースの VLAN マッピングを表示します。

<Switch> display vlan mapping

```
Interface GigabitEthernet1/0/1:
  Outer VLAN    Inner VLAN    Translated Outer VLAN    Translated Inner VLAN
  10            N/A           120                      N/A
```

```
Interface GigabitEthernet1/0/3:
  Outer VLAN    Inner VLAN    Translated Outer VLAN    Translated Inner VLAN
  12            N/A           110                      12
```

表 14-1 コマンド出力

フィールド	説明
Outer VLAN	もとの外部VLANです。 このフィールドはOne-to-one VLANマッピング、One-to-two VLANマッピングで、もとのVLANが表示されます。
Inner VLAN	もとの内部VLANです。 このフィールドはOne-to-one VLANマッピング、One-to-two VLANマッピングで、**N/A**と表示されます。
Translated Outer VLAN	変換される外部VLANです。 このフィールドはOne-to-one VLANマッピングで変換されるVLANが表示されます。
Translated Inner VLAN	変換される内部VLANです。 このフィールドはOne-to-one VLANマッピングで**N/A**と表示されます。

関連コマンド

vlan mapping

14.1.2 vlan mapping

Syntax

vlan mapping { *vlan-id* **translated-vlan** *vlan-id* | **nest** { **range** *vlan-range-list* | **single** *vlan-id-list* } **nested-vlan** *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* }

デフォルト

設定なし

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id **translated-vlan** *vlan-id*: one-to-one VLAN マッピングでもとの VLAN と変換される VLAN を指定します。*vlan-id* の設定範囲は 1～4094 です。もとの VLAN と変換される VLAN は同一にすることができません。

nest range *vlan-range-list* **nested-vlan** *vlan-id*: one-to-two VLAN マッピングでの CVLAN の範囲と SVLAN を指定します。*vlan-range-list* は半角スペースで区切り 10 まで設定します。CVLAN ID を範囲で指定する形式は *vlan-id1* **to** *vlan-id2* です。設定範囲は 1～4094 です。*vlan-id2* は *vlan-id1* 以上の値にしてください。異なる CVLAN 範囲は重複することはできません。*vlan-id* は、SVLAN ID の範囲を 1～4094 で指定します。

nest single *vlan-id-list* **nested-vlan** *vlan-id*: one-to-two VLAN マッピングでの CVLAN と SVLAN を指定します。*vlan-range-list* は半角スペースで区切り 10 まで設定します。設定範囲は 1～4094 です。*vlan-id* は SVLAN ID を指定し、設定範囲は 1～4094 です。

all: インタフェースからのすべての VLAN マッピングの設定を削除します。

説明

vlan mapping コマンドはインタフェースの VLAN マッピングを設定します。

undo vlan mapping コマンドは VLAN マッピングを取り消します。

VLAN マッピングはインタフェースで受信された VLAN タグつきパケットのみ適用されます。

インタフェースの VLAN マッピングのもとの VLAN と変換される VLAN は以下の要件に適用する必要があります。

- インタフェースのさまざまなタイプの VLAN マッピングエントリで、もとの VLAN と変換される VLAN は重複することができません。
- one-to-one VLAN マッピングエントリで変換される VLAN は重複することができません。one-to-one VLAN マッピングエントリはもとの VLAN が重複した場合、最後に行われた設定が適用されます。

ポートで QinQ を有効あるいは無効にする前に、インタフェースですべての VLAN マッピングを削除してください。

インタフェースで、トランスペアレント VLAN はもとの VLAN あるいは変換される VLAN の両方を使用する場合、トランスペアレント VLAN は one-to-one VLAN マッピングと one-to-two VLAN マッピングのもとの VLAN あるいは変換される VLAN にすることはできません。

インタフェースの MTU はデフォルトで 1500 バイトです。パケットに VLAN タグを追加したのち、パケット長は 4 バイト追加されます。one-to-two VLAN マッピングを設定するとき、サービスプロバイダ側ネットワークのインタフェースの MTU を少なくとも 1504 バイトに設定することを推奨します。

VLAN マッピングを適用したインタフェースを経由し、かつ VLAN マッピング対象の VLAN インタフェースを経由する L3 通信は未サポートです。

VLAN マッピング対象の VLAN に VLAN インタフェースを作成および IP アドレスを設定する場合は、L3 通信の経路（送受信インタフェース）には VLAN マッピングを適用しないでください。

例

VLAN 1 に VLAN101 をマッピングするため GigabitEthernet 1/0/1 で one-to-one VLAN マッピングを設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] vlan mapping 1 translated-vlan 101

VLAN タグ 1～VLAN 10、VLAN 80 を送信するパケットに SVLAN タグ 101 を追加するため、GigabitEthernet 1/0/4 の one-to-two VLAN マッピングを設定します。

<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

関連コマンド

display vlan mapping

目次

このセクションのページは **3-x-x** です。

15 章 LLDP.....15-1
15.1 LLDP 設定コマンド 15-1
15.1.1 cdp voice-vlan 15-1
15.1.2 display lldp local-information 15-2
15.1.3 display lldp neighbor-information.....15-7
15.1.4 display lldp statistics 15-15
15.1.5 display lldp status 15-17
15.1.6 display lldp tlv-config 15-19
15.1.7 lldp admin-status 15-23
15.1.8 lldp check-change-interval 15-24
15.1.9 lldp compliance admin-status cdp 15-25
15.1.10 lldp compliance cdp.....15-26
15.1.11 lldp enable.....15-27
15.1.12 lldp encapsulation snap 15-28
15.1.13 lldp fast-count 15-29
15.1.14 lldp global enable 15-30
15.1.15 lldp hold-multiplier 15-30
15.1.16 lldp ignore-pvid-inconsistency 15-31
15.1.17 lldp management-address-format string.....15-32
15.1.18 lldp notification remote-change enable 15-33
15.1.19 lldp timer notification-interval.....15-34
15.1.20 lldp timer reinit-delay 15-35
15.1.21 lldp timer tx-interval 15-35
15.1.22 lldp tlv-enable 15-36

15章 LLDP

15.1 LLDP設定コマンド

15.1.1 cdp voice-vlan

Syntax

cdp voice-vlan *vlan-id*

undo cdp voice-vlan

デフォルト

CDP フレームで伝送されるように音声 VLAN ID が設定されていません。

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id: 送信する音声 VLAN ID を指定します。設定範囲は 1～4094 です。

説明

cdp voice-vlan コマンドは CDP フレームで伝送される音声 VLAN ID を設定します。

undo cdp voice-vlan コマンドはデフォルトに戻します。

このコマンドを設定すると、インタフェースから IP 電話に送信される CDP フレームは、このコマンドで指定された音声 VLAN ID を伝送します。IP 電話は、音声 VLAN ID を使用して音声トラフィックを送信します。

例

CDP フレームで伝送される音声 VLAN ID を 100 に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] cdp voice-vlan 100

15.1.2 display lldp local-information

Syntax

display lldp local-information [**global** | **interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

global: グローバルのローカル LLDP 情報を表示します。

interface *interface-type interface-number*: ポートのタイプと番号を指定します。

説明

display lldp local-information コマンドはローカル情報を表示します。

パラメータを指定しない場合、以下が含まれるすべてのローカル LLDP 情報を表示します。

- グローバルの LLDP 情報
- up 状態の LLDP が有効なポートの LLDP 情報

例

すべてのローカル LLDP 情報を表示します。

<Switch> display lldp local-information

```
Global LLDP local-information:
 Chassis ID         : 9023-b4e1-4238
 System name        : QX-S5124GT-4X
 System description  :
   Comware Platform Software, Software Version 6.1.3a
   ,NEC QX-S5124GT-4X

 System capabilities supported : Bridge, Router, Customer Bridge, Service Bridge
 System capabilities enabled   : Bridge, Router, Customer Bridge

 MED information:
 Device class             : Connectivity device
 MED inventory information of master board:
 HardwareRev              : Ver.B
 FirmwareRev              : 141
```

```
SoftwareRev             : 7.1.2
SerialNum               : 219801A2Q19211Q00002
Manufacturer name        : NEC
Model name              : QX-S5124GT-4X
Asset tracking identifier  : Unknown
```

表 15-1 コマンド出力

フィールド	説明
Chassis ID	装置のBridge MACアドレスです。
System capabilities supported	サポートされる機能です。 ● **Bridge**–スイッチングがサポートされます。 ● **Router**–ルーティングがサポートされます。 ● **Repeater**—信号のリピータがサポートされます。 ● **Telephone**—ローカル装置が電話として動作します。 ● **DocsisCableDevice**–ローカル装置がDOCSIS準拠のケーブル装置として動作します。 ● **StationOnly**–ローカル装置が基地局のみとして動作します。 ● **Customer Bridge**–カスタマブリッジ機能がサポートされます。 ● **Service Bridge**–サービスブリッジ機能がサポートされます。 ● **TPMR**–TPMR（The two-port MAC relay）機能がサポートされます。 ● **Other**–上記で記載されている以外の機能がサポートされます。
System capabilities enabled	有効な機能です。 ● **Bridge**–スイッチングが有効です。 ● **Router**–ルーティングが有効です。 ● **Repeater**—信号のリピータが有効です。 ● **Telephone**—ローカル装置が電話として動作しています。 ● **DocsisCableDevice**–ローカル装置がDOCSIS準拠のケーブル装置として動作しています。 ● **StationOnly**–ローカル装置が基地局のみとして動作しています。 ● **Customer Bridge**–カスタマブリッジ機能が有効です。 ● **Service Bridge**–サービスブリッジ機能が有効です。 ● **TPMR**– TPMR（The two-port MAC relay）機能が有効です。 ● **Other**–上記で記載されている以外の機能が有効です。

フィールド	説明
Device class	MED装置のクラスです。 ● **Connectivity device**–ネットワーク装置です。 ● **Class I**–通常の端末装置です。basic LLDP検出サービスが必要です。 ● **Class II**–メディア端末装置です。通常の端末装置に加えて、メディアストリームをサポートします。 ● **Class III**–通信端末装置です。通常の端末装置、メディアストリームに加えて、エンドユーザのIP通信システムをサポートします。
HardwareRev	ハードウェアバージョンです。
FirmwareRev	ファームウェアバージョンです。
SoftwareRev	ソフトウェアバージョンです。
SerialNum	シリアル番号です。
Manufacturer name	装置の製造メーカです。
Model name	装置モデルです。
Port ID type	ポートIDタイプです。 ● MACアドレスです。 ● インタフェース名です。
Port ID	ポートIDです。ポートIDタイプによって変わります。
Management address interface type	管理アドレスで識別されるインタフェースの番号タイプです。
Management address interface ID	管理アドレスで識別されるインタフェースのインデックスです。
Management address OID	管理アドレスのオブジェクトIDです。
Link aggregation supported	ポートのリンクアグリゲーションがサポートされているかどうかを示します。
Link aggregation enabled	ポートのリンクアグリゲーションが有効かどうかを示します。
Aggregation port ID	メンバポートIDです。リンクアグリゲーションが無効であるとき、0と表示されます。
Auto-negotiation supported	ポートのオートネゴシエーションがサポートされているかを示します。
Auto-negotiation enabled	ポートのオートネゴシエーションが有効かどうかを示します。

フィールド	説明
OperMau	ポートの通信速度、通信モードです。
Power port class	PoEポートのクラスです。 ● **PSE**–電力供給装置です。 ● **PD**–電力が供給された装置です。
PSE power supported	装置がPSEとして動作可能かどうかを示します。
PSE power enabled	装置がPSEとして動作しているかどうかを示します。
PSE pairs control ability	PSE-PD間のPoE電力管理機能が有効かどうかを示します。
Power pairs	電力供給モードです。 ● **Signal**–データ転送と同時に電力を供給します。 ● **Spare**–データ転送と別の信号線で電力を供給します。
Port power classification	PDのポート供給電力のクラスです。 ● **Class 0**ークラス0です。 ● **Class 1**ークラス1です。 ● **Class 2**ークラス2です。 ● **Class 3**ークラス3です。 ● **Class 4**ークラス4です。
Power type	PoE装置タイプです。 ● Type 1 PD ● Type 2 PD ● Type 1 PSE ● Type 2 PSE
Power source	● PSE電力タイプです。 • **Unknown**–不明な電力供給です。 • **Primary**–プライマリ電力供給です。 • **Backup**–バックアップ電力供給です。 • **Reserved**ー予備です。 ● PoE装置タイプがPDの場合、パラメータを示します。 • **Unknown**–不明な電力供給です。 • **PSE**–PSE電力供給です。 • **Local**–ローカル電力供給です。 • **PSE and local**–PSE電力供給とローカル電力供給です。

フィールド	説明
Power priority	PSEポートのPoE電力供給のプライオリティです。 ● Unknown ● Critical ● High ● Low
PD requested power value	PDが要求する電力です。単位はWです。
PSE allocated power value	PSEがPDに供給する電力です。単位はWです。
PoE PSE power source	PSE電力供給タイプです。 ● **Unknown**–不明な電力供給です。 ● **Primary**–プライマリ電力供給です。 ● **Backup**–バックアップ電力供給です。
PoE PD power source	PD電力供給タイプです。 ● **Unknown**–不明な電力供給です。 ● **PSE**–PSE電力供給です。 ● **Local**–ローカル電力供給です。 ● **PSE and local**–PSE電力供給とローカル電力供給です。
Port PSE priority	PSEポートのPoE電力供給のプライオリティです。 ● Unknown ● Critical ● High ● Low
Port available power value	PSEポートのPoE電力あるいはPDポートで必要な電力です。単位はWです。
Transmit Tw	ローカルクライアントのスリープ時間です。単位はμsです。
Receive Tw	ローカルクライアントによって予期されたピアのクライアントのスリープ時間です。単位はμsです。
Fallback Tw	ローカルクライアントによって予期されたピアのクライアント候補のスリープ時間です。単位はμsです。
Echo Transmit Tw	ピアのクライアントのスリープ時間です。単位はμsです。このフィールドは以下の場合、0と表示されます。 ● ローカルクライアントがピアのクライアントのスリープ時間を受信していません。 ● ピアのクライアントのスリープ時間が0μsです。

フィールド	説明
Echo Receive Tw	ピアのクライアントによって予期されたローカルクライアントのスリープ時間です。単位はμsです。 このフィールドは以下の場合、0と表示されます。 • ローカルクライアントがピアのクライアントから予期されたスリープ時間を受信していません。 • ピアのクライアントによって予期されたローカルクライアントのスリープ時間が0μsです。

15.1.3 display lldp neighbor-information

Syntax

display lldp neighbor-information [[[**interface** *interface-type interface-number*] [**verbose**]] | **list** [**system-name** *system-name*]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: ポートのタイプと番号を指定します。指定しない場合、隣接装置から受信するすべてのポートの LLDP 情報を表示します。

verbose: ローカル装置が隣接装置から受信する LLDP の詳細情報を表示します。指定しない場合、ローカル装置が隣接装置から受信する LLDP の概要情報を表示します。

list: ローカル装置が隣接装置から受信する LLDP の情報をリスト形式で表示します。

system-name *system-name*: システム名で指定された隣接装置からローカル装置が受信する LLDP の情報を表示します。設定範囲は 1～255 です。指定しない場合、リストのすべての隣接装置からローカル装置が受信する LLDP の情報を表示します。

説明

display lldp neighbor-information コマンドはローカル装置が隣接装置から受信する LLDP 情報を表示します。LLDP 情報は LLDP TLV として受信します。

例

隣接装置からすべてのポートのすべての LLDP エージェントが受信した LLDP の詳細情報を表示します。

<Switch> display lldp neighbor-information verbose

```
LLDP neighbor-information of port 48[GigabitEthernet1/0/48]:
LLDP agent nearest-bridge:
 LLDP neighbor index : 1
 Update time        : 0 days, 0 hours, 2 minutes, 5 seconds
 Chassis type       : MAC address
 Chassis ID         : 5cdd-70b1-81fe
 Port ID type       : Interface name
 Port ID           : GigabitEthernet1/0/23
 Time to live       : 121
 Port description    : GigabitEthernet1/0/23 Interface
 System name        : QX-S5124GT-4X
 System description  : Copyright (c) 2004-2016 Hangzhou H3C Tech. Co., Ltd. All
                   rights reserved.
 System capabilities supported : Bridge, Router, Customer Bridge, Service Bridge
 System capabilities enabled   : Bridge, Router, Customer Bridge
 Management address type          : All802
 Management address              : 5cdd-70b1-823d
 Management address interface type : IfIndex
 Management address interface ID   : Unknown
 Management address OID           : 0
 Port VLAN ID(PVID)  : 1
 Link aggregation supported : Yes
 Link aggregation enabled   : No
 Aggregation port ID       : 0
 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        : 9216
```

隣接装置からすべてのポートのすべての LLDP エージェントが受信した LLDP の概要情報を表示します。

<Switch> display lldp neighbor-information

```
LLDP neighbor-information of port 48[GigabitEthernet1/0/48]:
LLDP agent nearest-bridge:
 LLDP neighbor index : 1
 ChassisID/subtype   : 5cdd-70b1-81fe/MAC address
 PortID/subtype      : GigabitEthernet1/0/23/Interface name
 Capabilities        : Bridge, Router, Customer Bridge
```

隣接装置からすべての LLDP エージェントが受信した LLDP の概要情報をリスト形式で表示します。

<Switch> display lldp neighbor-information list

```
Chassis ID : * -- -- Nearest nontpmr bridge neighbor
           # -- -- Nearest customer bridge neighbor
           Default -- -- Nearest bridge neighbor
System Name         Local Interface Chassis ID     Port ID
QX-S5124GT-4X       GE1/0/48       5cdd-70b1-81fe  GigabitEthernet1/0/23
```

表 15-2 コマンド出力

フィールド	説明
LLDP neighbor-information of port 1	LLDP情報がポート1から受信されました。
Update time	隣接情報のLLDP情報が最後にアップデートされた時間です。
Chassis type	装置IDタイプです。 ● **Chassis component**ー装置構成です。 ● **Interface alias**ーインタフェースの通称です。 ● **Port component**ーポート構成です。 ● **MAC address**ーMACアドレスです。 ● **Network address (ipv4)**ーネットワークアドレスです。（IPv4） ● **Interface name**ーインタフェース名です。 ● **Locally assigned**–上記にリストされたタイプ以外のローカルで定義された装置タイプです。
Chassis ID	LLDPが送信する装置を識別するIDです。 MACアドレス、ネットワークアドレス、インタフェース、あるいはそれ以外の値を使用することができ、隣接装置の装置タイプに依存します。

フィールド	説明
Port ID type	ポートIDタイプです。 ● **Interface alias**－インタフェースの通称です。 ● **Port component**－ポート構成です。 ● **MAC address**－MACアドレスです。 ● **Network address (ipv4)**－ネットワークアドレスです。（IPv4） ● **Interface name**－インタフェース名です。 ● **Agent circuit ID**－エージェントcircuit IDです。 ● **Locally assigned**–上記にリストされたタイプ以外のローカルで定義されたポートIDタイプです。
Port ID	ポートIDのタイプの値です。
System name	隣接装置のシステム名です。
System description	隣接装置のシステムの説明です。
System capabilities supported	隣接装置でサポートされる機能です。 ● **Repeater**–信号のリピータがサポートされます。 ● **Bridge**–スイッチングがサポートされます。 ● **Router**–ルーティングがサポートされます。 ● **Telephone**–隣接装置が電話として動作できます。 ● **DocsisCableDevice**–隣接装置がDOCSIS準拠のケーブル装置として動作します。 ● **StationOnly**–隣接装置が基地局のみとして動作します。 ● **Customer Bridge**–カスタマブリッジ機能がサポートされます。 ● **Service Bridge**–サービスブリッジ機能がサポートされます。 ● **TPMR**– TPMR（The two-port MAC relay）機能がサポートされます。 ● **Other**–上記で記載されている以外の機能がサポートされます。

フィールド	説明
System capabilities enabled	隣接装置で有効な機能です。 ● **Repeater**–信号のリピータが有効です。 ● **Bridge**–スイッチングが有効です。 ● **Router**–ルーティングが有効です。 ● **Telephone**–隣接装置が電話として動作できます。 ● **DocsisCableDevice**–隣接装置がDOCSIS準拠のケーブル装置として動作しています。 ● **StationOnly**–隣接装置が基地局のみとして動作しています。 ● **Customer Bridge**–カスタマブリッジ機能が有効です。 ● **Service Bridge**–サービスブリッジ機能が有効です。**TPMR**–TPMR（The two-port MAC relay）機能が有効です。 ● **Other**–上記で記載されている以外の機能が有効です。
Management address OID	管理アドレスのオブジェクトIDです。
Port and protocol VLAN ID(PPVID)	ポートのプロトコルVLAN IDです。
Port and protocol VLAN supported	ポートのプロトコルVLANがサポートされているかどうかを示します。
Port and protocol VLAN enabled	ポートのプロトコルVLANが有効かどうかを示します。
VLAN name of VLAN 12	VLAN 12の名前です。
Link aggregation supported	リンクアグリゲーションがサポートされているかどうかを示します。
Link aggregation enabled	リンクアグリゲーションが有効かどうかを示します。
Aggregation port ID	メンバポートIDです。リンクアグリゲーションが無効である場合、0と表示されます。
Auto-negotiation supported	ポートでネゴシエーションがサポートされているかを示します。
Auto-negotiation enabled	ポートでネゴシエーションが有効かどうかを示します。
OperMau	ポートの通信速度と通信モードの状態です。
Power port class	PoEポートのクラスです。 ● **PSE**–電力供給装置です。 ● **PD**–電力が供給された装置です。
PSE power supported	装置がPSEとして動作可能かどうかを示します。
PSE power enabled	装置がPSEとして動作しているかどうかを示します。

フィールド	説明
PSE pairs control ability	PSE-PD間のPoE電力管理機能が有効かどうかを示します。
Power pairs	電力供給モードです。 ● **Signal**–データ転送と同時に電力を供給します。 ● **Spare**–データ転送と別の信号線で電力を供給します。
Port power classification	PDのポート供給電力のクラスです。 ● **Class 0**ークラス0です。 ● **Class 1**ークラス1です。 ● **Class 2**ークラス2です。 ● **Class 3**ークラス3です。 ● **Class 4**ークラス4です。
Power type	PoE装置タイプです。 ● Type 1 PD ● Type 2 PD ● Type 1 PSE ● Type 2 PSE
Power source	● PSE電力タイプです。 • **Unknown**–不明な電力供給です。 • **Primary**–プライマリ電力供給です。 • **Backup**–バックアップ電力供給です。 • **Reserved**ー予備です。 ● PoE装置タイプがPDの場合、パラメータを示します。 • **Unknown**–不明な電力供給です。 • **PSE**–PSE電力供給です。 • **Local**–ローカル電力供給です。 • **PSE and local**–PSE電力供給とローカル電力供給です。
Power priority	PSEポートのPoE電力供給のプライオリティです。 ● Unknown ● Critical ● High ● Low
PD requested power value	PDが要求する電力です。単位はWです。
PSE allocated power value	PSEがPDに供給する電力です。単位はWです。

フィールド	説明
PoE PSE power source	PSE電力供給タイプです。 ● **Unknown**–不明な電力供給です。 ● **Primary**–プライマリ電力供給です。 ● **Backup**–バックアップ電力供給です。
PoE PD power source	PD電力供給タイプです。 ● **Unknown**–不明な電力供給です。 ● **PSE**–PSE電力供給です。 ● **Local**–ローカル電力供給です。 ● **PSE and local**–PSE電力供給とローカル電力供給です。
Port PSE priority	PSEポートのPoE電力供給のプライオリティです。 ● Unknown ● Critical ● High ● Low
Port PD priority	PDポートのPoE電力を受信するプライオリティです。 ● Unknown ● Critical ● High ● Low
Port available power value	PSEポートのPoE電力あるいはPDポートで必要な電力です。単位はWです。
HardwareRev	ハードウェアバージョンです。
FirmwareRev	ファームウェアバージョンです。
SoftwareRev	ソフトウェアバージョンです。
SerialNum	シリアル番号です。
Manufacturer name	装置の製造メーカです。
Model name	装置モデルです。
TLV type	不明なbasic TLVタイプです。
TLV information	不明なbasic TLVタイプに含まれる情報です。
Unknown organizationally-defined TLV	不明な組織指定TLVです。
TLV OUI	不明な組織指定TLVのOUIです。

フィールド	説明
TLV subtype	不明な組織指定のTLVのサブタイプです。
Index	不明な組織指定のインデックスです。
Capabilities	隣接装置で有効な機能です。 ● **Repeater**–信号のリピータが有効です。 ● **Bridge**–スイッチングが有効です。 ● **Router**–ルーティングが有効です。 ● **Telephone**–隣接装置が電話として動作できます。 ● **DocsisCableDevice**–隣接装置がDOCSIS準拠のケーブル装置として動作しています。 ● **StationOnly**–隣接装置が基地局のみとして動作しています。 ● **Other**–上記で記載されている以外の機能が有効です。 ● **None**–隣接装置がTLVを通知しません。
Local Interface	LLDP情報を受信するローカルポートです。
Chassis ID : * -- -- Nearest nontpmr bridge neighbor #-- -- Nearest customer bridge neighbor	シャーシIDのフラグです。 ● （*）はnearest non-TPMR bridge neighborを示します。 ● （#）はnearest customer bridge neighborを示します。
Transmit Tw	ローカルクライアントのスリープ時間です。単位はμsです。
Receive Tw	ローカルクライアントによって予期されたピアのクライアントのスリープ時間です。単位はμsです。
Fallback Tw	ローカルクライアントによって予期されたピアのクライアント候補のスリープ時間です。単位はμsです。
Echo Transmit Tw	ピアのクライアントのスリープ時間です。単位はμsです。 このフィールドは以下の場合、0と表示されます。 ● ローカルクライアントがピアのクライアントのスリープ時間を受信していません。 ● ピアのクライアントのスリープ時間が0μsです。
Echo Receive Tw	ピアのクライアントによって予期されたローカルクライアントのスリープ時間です。単位はμsです。 このフィールドは以下の場合、0と表示されます。 ● ローカルクライアントがピアのクライアントから予期されたスリープ時間を受信していません。 ● ピアのクライアントによって予期されたローカルクライアントのスリープ時間が0μsです。

15.1.4 display lldp statistics

Syntax

display lldp statistics [**global** | [**interface** *interface-type interface-number*]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

global: グローバルの LLDP の統計情報を表示します。

interface *interface-type interface-number*: ポートのタイプと番号を指定します。

説明

display lldp statistics コマンドはグローバルあるいはポートの LLDP の統計情報を表示します。

キーワードを指定しない場合、グローバルの LLDP の統計情報とすべてのポートの LLDP の統計情報を表示します。

例

グローバルの LLDP の統計情報とすべてのポートの LLDP の統計情報を表示します。

<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
```

表 15-3 コマンド出力

フィールド	説明
LLDP statistics global information	グローバルのLLDPの統計情報です。
LLDP neighbor information last change time	隣接情報が最後にアップデートした時間です。
The number of LLDP neighbor information inserted	隣接情報が追加された回数です。
The number of LLDP neighbor information deleted	隣接情報が削除された回数です。
The number of LLDP neighbor information dropped	メモリ空き容量が足りないために隣接情報が廃棄された回数です。

15.1.5 display lldp status

Syntax

display lldp status [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: ポートのタイプと番号を指定します。指定しない場合、グローバルの LLDP の状態とすべてのポートの LLDP の状態を表示します。

説明

display lldp status コマンドは LLDP の状態を表示します。

例

グローバルの LLDP の状態と各ポートの LLDP の状態を表示します。

<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
```

表 15-4 コマンド出力

フィールド	説明
Bridge mode of LLDP	LLDPブリッジモードです。サービスブリッジあるいはカスタマブリッジがあります。
Global status of LLDP	LLDPがグローバルで有効かどうかを示します。
LLDP neighbor information last changed time	隣接情報が最後にアップデートされた時間です。
Transmit interval	LLDPフレームの転送間隔です。
Hold multiplier	TTL乗数です。
Reinit delay	LLDPを再初期化の遅延時間です。

フィールド	説明
Transmit max credit	LLDPフレームを送信するトークンバケットサイズです。
Trap interval	トラップを転送する間隔です。
Fast start times	新しい隣接装置が検出された際、連続して送信されるLLDPフレームの回数です。
Port 1	ポート1のLLDPの状態です。
Port status of LLDP	ポートのLLDPが有効かどうかを示します。
Admin status	ポートのLLDP動作モードです。 ● **Tx_Rx**–ポートはLLDPフレームの送受信ができます。 ● **Rx_Only**–ポートはLLDPフレームの受信のみができます。 ● **Tx_Only**–ポートはLLDPフレームの送信のみができます。 ● **Disable**–ポートはLLDPフレームの送受信ができません。
Trap Flag	トラップが有効かどうかを示します。
Polling interval	LLDPのポーリング間隔です。0はLLDPのポーリングが無効であることを示します。
Number of neighbors	ポートに接続しているLLDPの隣接数です。
Number of MED neighbors	ポートに接続しているMEDの隣接数です。
Number of CDP neighbors	ポートに接続しているCDPの隣接数です。
Number of sent optional TLV	LLDPフレームに含まれるオプションTLVがポートに送信された数です。
Number of received unknown TLV	受信されたLLDPフレームに含まれる不明なTLVの数です。

15.1.6 display lldp tlv-config

Syntax

display lldp tlv-config [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: ポートのタイプと番号を指定します。指定しない場合、すべてのポートで通知可能なオプション LLDP TLV のタイプを表示します。

説明

display lldp tlv-config コマンドはポートで通知可能なオプション LLDP TLV のタイプを表示します。

例

GigabitEthernet 1/0/1 で通知可能なオプションの LLDP TLV のタイプを表示します。

<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   YES       YES
 VLAN Name TLV                 YES       YES
 DCBX TLV                      NO        NO
 EVB TLV                       NO        NO
 Link Aggregation TLV           YES       YES
 Management VID TLV             YES       YES
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           YES       NO
```

```
 System Name TLV                YES      NO
 System Description TLV         YES      NO
 System Capabilities TLV        YES      NO
 Management Address TLV         YES      NO
IEEE 802.1 extend TLV:
 Port VLAN ID TLV               YES      NO
 Port And Protocol VLAN ID TLV   YES      NO
 VLAN Name TLV                  YES      NO
 DCBX TLV                       NO       NO
 EVB TLV                        YES      YES
 Link Aggregation TLV           YES      NO
 Management VID TLV             NO       NO
IEEE 802.3 extend TLV:
 MAC-Physic TLV                 YES      NO
 Power via MDI TLV              YES      NO
 Maximum Frame Size TLV         YES      NO
LLDP-MED extend TLV:
 Capabilities TLV               YES      NO
 Network Policy TLV             YES      NO
 Location Identification TLV    NO       NO
 Extended Power via MDI TLV     YES      NO
 Inventory TLV                  YES      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   YES      YES
 VLAN Name TLV                  YES      YES
 DCBX TLV                       NO       NO
 EVB TLV                        NO       NO
 Link Aggregation TLV           YES      NO
 Management VID TLV             YES      YES
IEEE 802.3 extend TLV:
 MAC-Physic TLV                 YES      NO
 Power via MDI TLV              YES      NO
 Maximum Frame Size TLV         YES      NO
```

```
LLDP-MED extend TLV:
 Capabilities TLV              YES       YES
 Network Policy TLV            YES       YES
 Location Identification TLV    NO        NO
 Extended Power via MDI TLV     YES       NO
 Inventory TLV                 YES       YES
```

表 15-5 コマンド出力

フィールド	説明
LLDP tlv-config of port 1	ポート1の通知可能なオプションTLVです。
NAME	TLVのタイプです。
STATUS	TLVのタイプがポートに送信されたかどうかを示します。
DEFAULT	デフォルトでTLVのタイプがポートに送信されたかどうかを示します。
Basic optional TLV	basic TLVのオプションTLVです。 ● **Port description TLV**－ポート説明TLVです。 ● **System name TLV**－システム名TLVです。 ● **System description TLV**－システム説明TLVです。 ● **System capabilities TLV**－システム機能TLVです。 ● **Management address TLV**－管理アドレスTLVです。
IEEE 802.1 extended TLV	IEEE802.1組織指定TLVです。 ● **Port VLAN ID TLV**－ポートVLAN ID TLVです。 ● **Port and protocol VLAN ID TLV**－ポートのプロトコルVLAN TLVです。 ● **VLAN name TLV**－VLAN名TLVです。 ● **DCBX TLV**－DCBX TLVです。DCBX TLVはサポートしていません。 ● **EVB TLV**－EVB TLVです。EVB TLVはサポートしていません。 ● **Management VID TLV**－管理VID TLVです。
IEEE 802.3 extended TLV	IEEE802.3組織指定TLVです。 ● **MAC-Physic TLV**－MAC物理TLVです。 ● **Power via MDI TLV**－MDI経由の電力TLVです。 ● **Link aggregation TLV**－リンクアグリゲーションTLVです。 ● **Maximum frame size TLV**－最大フレームサイズTLVです。

フィールド	説明
LLDP-MED extend TLV	LLDP-MED TLVです。 ● **Capabilities TLV**－機能TLVです。 ● **Network Policy TLV**－ネットワークポリシーTLVです。 ● **Extended Power-via-MDI TLV**－拡張MDI経由TLVです。 ● **Location Identification TLV**－位置識別TLVです。 ● **Inventory TLV**－インベントリTLVです。
Inventory TLV	インベントリTLVです。 ● **Hardware Revision TLV**－ハードウェアレビジョンTLVです。 ● **Firmware Revision TLV**－ファームウェアレビジョンTLVです。 ● **Software Revision TLV**－ソフトウェアバージョンTLVです。 ● **Serial Number TLV**－シリアル番号TLVです。 ● **Manufacturer Name TLV**－装置の製造メーカTLVです。 ● **Model name TLV**－装置名TLVです。 ● **Asset ID TLV**－Asset ID TLVです。

15.1.7 lldp admin-status

Syntax

Layer 2 Ethernet interface view :

lldp [**agent nearest-customer**] **admin-status** { **disable** | **rx** | **tx** | **txrx** }

undo lldp [**agent nearest-customer**] **admin-status**

Layer 2 aggregate interface view :

lldp agent nearest-customer admin-status { **disable** | **rx** | **tx** | **txrx** }

undo lldp agent nearest-customer admin-status

デフォルト

nearest bridge エージェントは txrx モード、nearest customer bridge エージェントは disable です。

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

agent: LLDP エージェントタイプを指定します。指定しない場合、nearest bridge エージェントの動作モードを設定します。

nearest-customer: nearest customer bridge エージェントを指定します。

disable: Disable モードを指定します。Disable モードのポートは LLDP フレームの送受信ができません。

rx: Rx モードを指定します。Rx モードのポートは LLDP フレームの受信のみができます。

ポートは LLDP フレームの送受信ができます。

tx: Tx モードを指定します。Tx モードのポートは LLDP フレームの送信のみができます。

ポートは LLDP フレームの送受信ができます。

txrx: TxRx モードを指定します。TxRx モードのポートは LLDP フレームの送受信ができます。

説明

lldp admin-status コマンドは LLDP の動作モードを指定します。

undo lldp admin-status コマンドはデフォルトに戻します。

例

GigabitEthernet 1/0/1 の nearest customer bridge エージェントの LLDP 動作モードを Rx に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] lldp agent nearest-customer admin-status rx

15.1.8 lldp check-change-interval

Syntax

Layer 2 Ethernet interface view :

lldp [**agent nearest-customer**] **check-change-interval** *interval*

undo lldp [**agent nearest-customer**] **check-change-interval**

Layer 2 aggregate interface view :

lldp agent nearest-customer check-change-interval *interval*

undo lldp agent nearest-customer check-change-interval

デフォルト

無効

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

agent: LLDP エージェントタイプを指定します。指定しない場合、nearest bridge エージェントの LLDP ポーリングを有効にし、ポーリング間隔を設定します。

nearest-customer: nearest customer bridge エージェントを指定します。

interval: LLDP ポーリング間隔を設定します。設定範囲は 1～30 秒です。

説明

lldp check-change-interval コマンドは LLDP ポーリングを有効にし、ポーリング間隔を設定します。

undo lldp check-change-interval コマンドはデフォルトに戻します。

例

GigabitEthernet 1/0/1 の nearest customer bridge エージェントの LLDP ポーリングを有効にし、ポーリング間隔を 30 秒に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] lldp agent nearest-customer check-change-interval 30

15.1.9 lldp compliance admin-status cdp

Syntax

lldp compliance admin-status cdp { **disable** | **txrx** }

undo lldp compliance admin-status cdp

デフォルト

disable

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

disable: Disable モードを指定します。Disable モードは CDP パケットの送受信を行うことができません。

txrx: TxRx モードを指定します。TxRx モードは CDP パケットの送受信を行うことができます。

説明

lldp compliance admin-status cdp コマンドは CDP 互換 LLDP モードの動作モードを設定します。

undo lldp compliance admin-status cdp コマンドはデフォルトに戻します。

Cisco の IP 電話を動作させるため以下の作業を行ってください。

- グローバルで CDP 互換 LLDP を有効にします。
- 指定したポートを TxRx モードで動作するように CDP 互換 LLDP を設定します。

例

グローバルで CDP 互換 LLDP を有効にし、GigabitEthernet 1/0/1 を TxRx モードで動作するように CDP 互換 LLDP を設定します。

<Switch> system-view

[Switch] lldp compliance cdp

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] lldp compliance admin-status cdp txrx

関連コマンド

lldp compliance cdp

15.1.10 lldp compliance cdp

Syntax

lldp compliance cdp

undo lldp compliance cdp

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

lldp compliance cdp コマンドは CDP 互換モードを有効にします。

undo lldp compliance cdp コマンドはデフォルトに戻します。

CDP で許可される最大 TTL は 255 秒です。Cisco の IP 電話と一緒に運用するため、CDP 互換 LLDP の送信間隔の設定は TTL 値の 1/3 以内にする必要があります。

例

CDP 互換モードを有効にします。

<Switch> system-view

[Switch] lldp compliance cdp

関連コマンド

- **lldp hold-multiplier**
- **lldp timer tx-interval**

15.1.11 lldp enable

Syntax

lldp enable

undo lldp enable

デフォルト

有効

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

lldp enable コマンドはポートで LLDP を有効にします。

undo lldp enable コマンドはポートで LLDP を無効にします。

LLDP はグローバルとポートの両方で有効にしたときのみ適用されます。

例

GigabitEthernet 1/0/1 で LLDP を無効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] undo lldp enable

関連コマンド

lldp global enable

15.1.12 lldp encapsulation snap

Syntax

Layer 2 Ethernet interface view :

lldp [**agent nearest-customer**] **encapsulation snap**

undo lldp [**agent nearest-customer**] **encapsulation**

Layer 2 aggregate interface view :

lldp agent nearest-customer encapsulation snap

undo lldp agent nearest-customer encapsulation

デフォルト

Ethernet II

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

agent: LLDP エージェントタイプを指定します。指定しない場合、nearest bridge エージェントの LLDP フレームのカプセル化フォーマットを設定します。

nearest-customer: nearest customer bridge エージェントを指定します。

説明

lldp encapsulation snap コマンドは LLDP フレームのカプセル化フォーマットを SNAP に設定します。

undo lldp encapsulation コマンドはデフォルトに戻します。

LLDP-CDP パケットは SNAP のカプセル化フォーマットのみ使用します。

例

GigabitEthernet 1/0/1 の LLDP フレームのカプセル化フォーマットを SNAP に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] lldp encapsulation snap

15.1.13 lldp fast-count

Syntax

lldp fast-count *count*

undo lldp fast-count

デフォルト

4

View

System view

定義済みユーザロール

network-admin

パラメータ

count: 新しい隣接装置が検出される際に連続して送信される LLDP フレームの数を指定します。設定範囲は 1～8 です。

説明

lldp fast-count コマンドは新しい隣接装置が検出される際に連続して送信される LLDP フレームの数を指定します。

undo lldp fast-count コマンドはデフォルトに戻します。

例

新しい隣接装置が検出される際に連続して送信される LLDP フレームの数を 5 に設定します。

<Switch> system-view

[Switch] lldp fast-count 5

15.1.14 lldp global enable

Syntax

lldp global enable

undo lldp global enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

lldp global enable コマンドはグローバルで LLDP を有効にします。

undo lldp global enable コマンドはグローバルで LLDP を無効にします。

LLDP はグローバルとポートの両方で有効にしたときのみ適用されます。

例

グローバルで LLDP を無効にします。

<Switch> system-view

[Switch] undo lldp global enable

関連コマンド

lldp enable

15.1.15 lldp hold-multiplier

Syntax

lldp hold-multiplier *value*

undo lldp hold-multiplier

デフォルト

4

View

System view

定義済みユーザロール

network-admin

パラメータ

value: TTL の乗数を設定します。設定範囲は 2～10 です。

説明

lldp hold-multiplier コマンドは TTL の乗数を設定します。

undo lldp hold-multiplier コマンドはデフォルトに戻します。

LLDPDU で送信される TTL TLV は、受信装置で保存される装置情報の保存期間を決定します。

TTL の乗数を設定することにより、隣接装置に送信する TTL の設定を行うことができます。隣接装置についての情報の TTL は以下の式によって定義されます。

TTL ＝min（65535, （TTL の乗数 x LLDP フレームの送信間隔 ＋ 1））

TTL は最大 65535 秒です。65535 より大きい場合、65535 秒に丸められます。

例

TTL の乗数を 6 に設定します。

<Switch> system-view

[Switch] lldp hold-multiplier 6

関連コマンド

lldp timer tx-interval

15.1.16 lldp ignore-pvid-inconsistency

Syntax

lldp ignore-pvid-inconsistency

undo lldp ignore-pvid-inconsistency

デフォルト

有効

View

System view

デフォルトのコマンド・レベル

network-admin

説明

lldp ignore-pvid-inconsistency コマンドは LLDP PVID 不一致チェックを無効にします。

undo lldp ignore-pvid-inconsistency コマンドは LLDP PVID 不一致チェックを有効にします。

デフォルトでは、システムは LLDP パケットを受信すると、パケットに含まれる PVID 値を受信側インタフェースで設定された PVID と比較します。両方の PVID が一致しない場合は、ユーザに通知するためのログメッセージが出力されます。

リンクで異なる PVID が必要な場合は、PVID 不一致チェックを無効にできます。

例

LLDP PVID 不一致チェックを無効にします。

<Switch> system-view

[Switch] lldp ignore-pvid-inconsistency

15.1.17 lldp management-address-format string

Syntax

Layer 2 Ethernet interface view :

lldp [**agent nearest-customer**] **management-address-format string**

undo lldp [**agent nearest-customer**] **management-address-format**

Layer 2 aggregate interface view :

lldp agent nearest-customer management-address-format string

undo lldp agent nearest-customer management-address-format

デフォルト

numeric 形式

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

agent: LLDP エージェントタイプを指定します。指定しない場合、nearest bridge エージェントの管理アドレスのカプセル化フォーマットを設定します。

nearest-customer: nearest customer bridge エージェントを指定します。

説明

lldp management-address-format string コマンドは管理アドレスの TLV のカプセル化フォーマットを string 形式に設定します。

undo lldp management-address-format コマンドはデフォルトに戻します。

管理アドレスの LLDP 隣接は同じカプセル化フォーマットを使用する必要があります。

IPv6 管理アドレスでは numeric 形式のみサポートします。

例

GigabitEthernet 1/0/1 の nearest customer bridge エージェントで管理アドレスの TLV のカプセル化フォーマットを string 形式に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] lldp agent nearest-customer management-address-format string

15.1.18 lldp notification remote-change enable

Syntax

Layer 2 Ethernet interface view :

lldp [**agent nearest-customer**] **notification remote-change enable**

undo lldp [**agent nearest-customer**] **notification remote-change enable**

Layer 2 aggregate interface view :

lldp agent nearest-customer notification remote-change enable

undo lldp agent nearest-customer notification remote-change enable

デフォルト

無効

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

agent: LLDP エージェントタイプを指定します。指定しない場合、nearest bridge エージェントの LLDP トラップを有効にします。

nearest-customer: nearest customer bridge エージェントを指定します。

説明

lldp notification remote-change enable コマンドは LLDP トラップを有効にします。

undo lldp notification remote-change enable コマンドは LLDP トラップを無効にします。

例

GigabitEthernet 1/0/1 の nearest customer bridge エージェントの LLDP トラップを有効にします。

<Switch> system-view

[Switch] interface GigabitEthernet 1/0/1

[Switch-GigabitEthernet1/0/1] lldp agent nearest-customer notification remote-change enable

15.1.19 lldp timer notification-interval

Syntax

lldp timer notification-interval *interval*

undo lldp timer notification-interval

デフォルト

30 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

interval: LLDP トラップと LLDP-MED トラップの送信間隔を指定します。設定範囲は 5 ～3600 秒です。

説明

lldp timer notification-interval コマンドは LLDP トラップと LLDP-MED トラップの送信間隔を設定します。

undo lldp timer notification-interval コマンドはデフォルトに戻します。

例

LLDP トラップと LLDP-MED トラップの送信間隔を 8 秒に設定します。

<Switch> system-view

[Switch] lldp timer notification-interval 8

15.1.20 lldp timer reinit-delay

Syntax

lldp timer reinit-delay *delay*

undo lldp timer reinit-delay

デフォルト

2 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

delay: LLDP の再初期化の遅延時間を設定します。設定範囲は 1～10 秒です。

説明

lldp timer reinit-delay コマンドは LLDP の再初期化の遅延時間を設定します。

undo lldp timer reinit-delay コマンドはデフォルトに戻します。

例

LLDP の再初期化の遅延時間を 4 秒に設定します。

<Switch> system-view

[Switch] lldp timer reinit-delay 4

15.1.21 lldp timer tx-interval

Syntax

lldp timer tx-interval *interval*

undo lldp timer tx-interval

デフォルト

30 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

interval: LLDP フレームの送信間隔を設定します。設定範囲は 5～32768 秒です。

説明

lldp timer tx-interval コマンドは LLDP フレームの送信間隔を設定します。

undo lldp timer tx-interval コマンドはデフォルトに戻します。

例

LLDP フレームの送信間隔を 20 秒に設定します。

<Switch> system-view

[Switch] lldp timer tx-interval 20

15.1.22 lldp tlv-enable

Syntax

Layer 2 Ethernet interface view :

- nearest bridge エージェント

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** } }

- nearest customer bridge エージェント

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** } }

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** }

デフォルト

Ethernet インタフェースのデフォルトを以下に示します。

- nearest bridge エージェントは以下のタイプの LLDP TLV を除いたすべての LLDP TLV を送信します。
  - 位置識別 TLV
  - ポートのプロトコル VLAN ID TLV
  - VLAN 名 TLV
  - 管理 VLAN ID TLV
- nearest customer bridge エージェントは basic TLV と IEEE802.1 組織指定 TLV を送信します。

レイヤ 2 アグリゲートインタフェースのデフォルトを以下に示します。

nearest customer bridge エージェントは basic TLV と IEEE802.1 組織指定 TLV（ポートのプロトコル VLAN ID TLV、VLAN 名 TLV、管理 VLAN ID TLV のみ）を送信します。

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

agent: LLDP エージェントタイプを指定します。Ethernet インタフェースでパラメータを指定しない場合、nearest bridge エージェントの通知可能な TLV のタイプを設定します。

nearest-customer: nearest customer bridge エージェントを指定します。

all: 指定したタイプのすべての TLV を送信します。

- 以下の TLV を送信するインタフェースを有効にします。
  - **basic-tlv** で **all** が指定された場合、すべての basic LLDP TLV を送信します。
  - **dot1-tlv** で **all** が指定された場合、すべての 802.1 組織指定 LLDP TLV を送信します。
  - **dot3-tlv** で **all** が指定された場合、すべての 802.3 組織指定 LLDP TLV を送信します。
- **med-tlv** で **all** が指定された場合、位置識別 TLV を除くすべての LLDP-MED TLV を送信します。

basic-tlv: basic LLDP TLV を送信します。

management-address-tlv [*ip-address* | **interface loopback** *interface-number*]:

管理アドレス TLV を送信します。*ip-address* は送信される管理アドレスを指定します。デフォルトを以下に示します。**loopback** *interface-number* パラメータはループバックインタフェースの IP アドレスを指定します。デフォルトを以下に示します。

- レイヤ 2 Ethernet インタフェースあるいはアグリゲートインタフェースで、管理アドレスは以下の要件に一致する VLAN インタフェースのプライマリ IP アドレスです。
  - up 状態のインタフェースです。
  - 一致する VLAN ID がポートで許可された VLAN でもっとも小さい値です。

  許可された VLAN の VLAN インタフェースに IP アドレスが設定されていない、あるいはすべての VLAN インタフェースが down している場合、ポートの MAC アドレスが送信されます。

undo コマンドを実行するとき、以下の処理を行います。

- *ip-address* を指定した場合、指定した IP アドレスの送信を無効にします。
- *ip-address* を指定しない場合、管理アドレス TLV の送信を無効にします。

port-description: ポート説明 TLV を送信します。

system-capability: システム機能 TLV を送信します。

system-description: システム説明 TLV を送信します。

system-name: システム名 TLV を送信します。

dot1-tlv: IEEE 802.1 組織指定 LLDP TLV を送信します。

port-vlan-id: ポート VLAN ID TLV を送信します。

protocol-vlan-id [*vlan-id*]: ポートとプロトコル VLAN ID TLV を送信します。*vlan-id* は送信される TLV の VLAN ID を指定します。VLAN ID の設定範囲は 1～4094 です。デフォルトはポートでもっとも小さい VLAN ID です。

vlan-name [*vlan-id*]: VLAN 名 TLV を送信します。*vlan-id* は送信される TLV の VLAN ID を指定します。VLAN ID の設定範囲は 1～4094 です。デフォルトはポートでもっとも小さい VLAN ID です。

management-vid [*mvlan-id*]: 管理 LAN ID TLV を送信します。*mvlan-id* は送信される TLV の管理 VLAN ID を指定します。管理 VLAN ID の設定範囲は 1～4094 です。管理 VLAN ID が指定されない場合、0 が送信されます。0 は LLDP エージェントが管理 VLAN ID で設定されないことを示します。

dot3-tlv: IEEE802.3 組織指定 LLDP TLV を送信します。

link-aggregation: リンクアグリゲーション TLV を送信します。

mac-physic: MAC/PHY の設定/状態 TLV（MAC/PHY configuration/status TLV）を送信します。

max-frame-size: 最大フレームサイズ TLV を送信します。

power: MDI TLV の電力と電力ステートフル制御 TLV を送信します。

med-tlv: LLDP-MED TLV を送信します。

capability: LLDP-MED 機能 TLV を送信します。

inventory: ハードウェアレビジョン、ファームウェアレビジョン、ソフトウェアバージョン、シリアル番号、装置名、製品名、assert ID の TLV を送信します。

location-id: 位置識別 TLV を送信します。

civic-address: 位置識別 TLV のネットワーク装置に関する一般的なアドレス情報を挿入します。

device-type: 装置タイプを設定します。設定範囲は 0～2 です。

- 0 は DHCP サーバを指定します。
- 1 はスイッチを指定します。
- 2 は LLDP-MED エンドポイントを指定します。

country-code: ISO 3166 で定義された国別コードを設定します。

{ *ca-type ca-value* }&<1-10>: アドレス情報を設定します。*ca-type* はアドレス情報タイプを示します。設定範囲は 0～255 です。*ca-value* はアドレス情報を示します。設定範囲は 1～250 文字です。&<1-10>は *ca-type ca-value* を最大 10 まで指定できることを示します。

elin-address: 位置識別 TLV に緊急用電話番号を挿入します。

tel-number: 緊急用電話番号を設定します。設定範囲は 10～25 です。

network-policy [*vlan-id*]: ネットワークポリシーTLV を送信します。VLAN ID の設定範囲は 1～4094 です。

power-over-ethernet: 拡張 MDI 経由の電力 TLV（power-via-MDI TLV）を送信します。

説明

lldp tlv-enable コマンドは通知可能な TLV のタイプを設定します。

undo lldp tlv-enable コマンドは TLV の指定されたタイプの送信を無効にします。

nearest bridge エージェントはアグリゲートインタフェースでサポートしていません。

all パラメータを指定しないで、TLV の複数のタイプを送信することができます。

MAC/PHY 設定/状態 TLV が送信されない場合、通知可能であるにも関わらず、LLDP-MED TLV が送信されません。LLDP-MEDTLV が送信されない場合、通知可能であるにも関わらず、他の LLDP-MED TLV が送信されません。

IEEE802.1 組織指定 LLDP TLV のプロトコル VLAN ID、VLAN 名 TLV、管理 VLAN ID TLV は nearest bridge エージェントでのみ設定できます。

例

GigabitEthernet 1/0/1 の IEEE802.1 組織指定 TLV のリンクアグリゲーション TLV を送信するため、GigabitEthernet 1/0/1 の nearest customer bridge エージェントを有効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] lldp agent nearest-customer tlv-enable dot1-tlv link-aggregation

目次

このセクションのページは **3-x-x** です。

16 章 L2PT 16-1
16.1 L2PT設定コマンド 16-1
16.1.1 display l2protocol statistics 16-1
16.1.2 l2protocol tunnel dot1q 16-3
16.1.3 l2protocol tunnel-dmac 16-5
16.1.4 reset l2protocol statistics 16-5

16章 L2PT

16.1 L2PT設定コマンド

16.1.1 display l2protocol statistics

Syntax

display l2protocol statistics [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: Ethernet インタフェースあるいはアグリゲートインタフェースを指定します。指定しない場合、すべての Ethernet インタフェースとアグリゲートインタフェースの L2PT の統計情報を表示します。

説明

display l2protocol statistics コマンドは L2PT（Layer 2 Protocol Tunneling）の統計情報を表示します。

例

すべての Ethernet インタフェースとアグリゲートインタフェースの L2PT の統計情報を表示します。

<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
```

表 16-1 コマンド出力

フィールド	説明
Encapsulated	カプセル化したパケット数です。 インタフェースがカスタマネットワークからプロトコルパケットを受信し、カプセル化したとき、1つずつ数が増えます。 **Tunnel**プロトコルの場合、**N/A**と表示されます。**Tunnel**プロトコルはトンネルパケットを示します。
Decapsulated	復号化したパケット数です。 インタフェースがサービスプロバイダネットワークからプロトコルパケットを受信し、トンネルパケットを復号化したとき、1つずつ数が増えます。 **Tunnel**プロトコルの場合、**N/A**と表示されます。**Tunnel**プロトコルはトンネルパケットを示します。
Forwarded	転送されたパケット数です。 インタフェースがプロトコルパケットを受信し、転送したとき、1つずつ数が増えます。 **Tunnel**プロトコルの場合、インタフェースがプロトコルパケットを受信し、転送したとき、1つずつ数が増えます。PEのインタフェースがカスタマネットワークに接続されていない場合、値は増加しません。

フィールド	説明
Dropped	廃棄されたパケット数です。 インタフェースがプロトコルパケットを受信し、廃棄したとき、1つずつ数が増えます。ハードウェアによって廃棄されたプロトコルパケットはカウントされません。 Tunnelプロトコルの場合、インタフェースがプロトコルパケットを受信し、廃棄したとき、1つずつ数が増えます。

16.1.2 l2protocol tunnel dot1q

Syntax

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**

Layer 2 aggregate interface view :

l2protocol { **gvrp** | **mvrp** | **pvst** | **stp** | **vtp** | **cdp** | **lacp** | **lldp** | **pagp** | **udld**} **tunnel dot1q**

undo l2protocol { **gvrp** | **mvrp** | **pvst** | **stp** | **vtp** | **cdp** | **lacp** | **lldp** | **pagp** | **udld**} **tunnel dot1q**

デフォルト

無効

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

cdp: CDP を指定します。

dldp: DLDP を指定します。

eoam: EOAM を指定します。

gvrp: GVRP を指定します。

lacp: LACP を指定します。

lldp: LLDP を指定します。LLDP の L2PT は nearest bridge エージェントからのパケットのみサポートします。

mvrp: MVRP を指定します。

pagp: PAgP を指定します。

pvst: PVST を指定します。

stp: STP を指定します。

udld: UDLD を指定します。

vtp: VTP を指定します。

説明

l2protocol tunnel dot1q コマンドはプロトコルの L2PT を有効にします。

undo l2protocol tunnel dot1q コマンドはデフォルトに戻します。

ポートでプロトコルの L2PT を有効にする前に、以下の処理を行ってください。

- CE でプロトコルを有効にし、ポートでプロトコルを無効にしてください。
- カスタマ側の PE ポートでのみ L2PT を有効にしてください。サービスプロバイダネットワークに接続されているポートで L2PT を有効にした場合、L2PT はポートがカスタマネットワーク接続されていると認識します。
- 以下の条件に該当する環境では、CE のアグリゲーションインタフェースと接続している PE ポートのプロトコル(例えば STP)を無効にしてください。
  - □ プロトコルは CE のアグリゲーションインタフェースで動作します。
  - □ CE のアグリゲーションインタフェースは PE の L2PT 対応のポートと接続します。

アグリゲーショングループのメンバポートで L2PT を有効にするコマンドを入力することができますが、設定は適用されません。

例

STP を無効にします。GigabitEthernet 1/0/1 で STP の L2PT を有効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] undo stp enable

[Switch-GigabitEthernet1/0/1] l2protocol stp tunnel dot1q

STP を無効にします。アグリゲートインタフェース Bridge-Aggregation 1 で STP の L2PT を有効にします。

<Switch> system-view

[Switch] interface bridge-aggregation 1

[Switch-Bridge-Aggregation1] undo stp enable

[Switch-Bridge-Aggregation1] l2protocol stp tunnel dot1q

16.1.3 l2protocol tunnel-dmac

Syntax

l2protocol tunnel-dmac *mac-address*

undo l2protocol tunnel-dmac

デフォルト

010f-e200-0003

View

System view

定義済みユーザロール

network-admin

パラメータ

mac-address: 宛先マルチキャスト MAC アドレスを指定します。有効なアドレスは 0100-0ccd-cdd0、0100-0ccd-cdd1、0100-0ccd-cdd2、010f-e200-0003 です。

説明

l2protocol tunnel-dmac コマンドはトンネルパケットの宛先マルチキャスト MAC アドレスを設定します。

undo l2protocol tunnel-dmac コマンドはデフォルトに戻します。

例

トンネルパケットの宛先マルチキャスト MAC アドレスを 0100-0ccd-cdd0 に設定します。

<Switch> system-view

[Switch] l2protocol tunnel-dmac 0100-0ccd-cdd0

16.1.4 reset l2protocol statistics

Syntax

reset l2protocol statistics [**interface** *interface-type interface-number*]

View

User view

定義済みユーザロール

network-admin

パラメータ

interface *interface-type interface-number*: Ethernet インタフェースあるいはアグリゲートインタフェースを指定します。指定しない場合、すべての Ethernet インタフェースとアグリゲートインタフェースの L2PT の統計情報を削除します。

説明

reset l2protocol statistics コマンドは L2PT の統計情報を削除します。

例

すべての Ethernet インタフェースとアグリゲートインタフェースの L2PT の統計情報を削除します。

<Switch> reset l2protocol statistics

QX-S5100G シリーズ Ethernet スイッチ

コマンドマニュアル

4. IP サービス

本マニュアルは以下に示す章で構成されています。

01-ARP

02-Gratuitous ARP

03-Proxy ARP

04-ARP スヌーピング

05-IP アドレス

06-DHCP

07-DHCP サーバ

08-DHCP リレーエージェント

09-DHCP クライアント

10-DHCP スヌーピング

11-BOOTP クライアント

12-DNS

13-IP フォワーディングの基本

14-IP パフォーマンスの最適化

15-UDP ヘルパー

16-IPv6 の基本

17-DHCPv6

18-DHCPv6 リレーエージェント

19-DHCPv6 クライアント

20-HTTP リダイレクト

目次

このセクションのページは **4-x-x** です。

1 章 ARP 1-1
1.1 ARP 設定コマンド 1-1
1.1.1 arp check enable 1-1
1.1.2 arp check log enable 1-2
1.1.3 arp mac-interface-consistency check enable 1-3
1.1.4 arp max-learning-num 1-3
1.1.5 arp max-learning-number 1-5
1.1.6 arp multiport 1-6
1.1.7 arp static 1-7
1.1.8 arp timer aging 1-9
1.1.9 display arp 1-10
1.1.10 display arp *ip-address* 1-13
1.1.11 display arp timer aging 1-14
1.1.12 display arp vpn-instance 1-14
1.1.13 reset arp 1-15

1章 ARP

1.1 ARP設定コマンド

1.1.1 arp check enable

Syntax

arp check enable

undo arp check enable

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

arp check enable コマンドはダイナミック ARP エントリチェックを有効にします。

undo arp check enable コマンドはダイナミック ARP エントリチェックを無効にします。

ダイナミック ARP エントリチェック機能は、装置がマルチキャスト MAC アドレスを含むダイナミック ARP エントリをサポートしているかどうかを管理することができます。ARP エントリチェック機能を有効にすると、装置がマルチキャスト MAC アドレスから ARP エントリを作成するのを無効にします。ARP エントリチェックが有効な場合、装置はマルチキャスト MAC アドレスの ARP エントリを学習することはできません。

ARP エントリチェックを無効にした場合、装置はマルチキャスト MAC アドレスの ARP エントリを学習することができます。手動でマルチキャスト MAC アドレスを含むスタティック ARP エントリを追加することができます。

例

ダイナミック ARP エントリチェックを有効にします。

<Switch> system-view

[Switch] arp check enable

1.1.2 arp check log enable

Syntax

arp check log enable

undo arp check log enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

arp check log enable コマンドは ARP ロギング機能を有効にします。

undo arp check log enable コマンドは ARP ロギング機能を無効にします。

ARP が IP アドレスを正常に解決できないとき、装置で ARP イベントをロギングします。以下の ARP イベントをロギングできます。

- インタフェースで proxy ARP が無効な場合、受信した ARP パケットの宛先 IP アドレスは受信インタフェースの IP アドレスのいずれでもありません。
- 受信した ARP エントリの送信元 IP アドレスが受信インタフェースの IP アドレスの 1 つと重複しています。

装置は Information Center に ARP ログメッセージを送信します。Information Center のログ出力ルールを設定するため、**info-center source** コマンドを使用します。Information Center の詳細は、オペレーションマニュアルのセクション 11 *システム管理*“*Information Center*”を参照してください。

装置は非常に多くの ARP ログを作成することができます。システムリソースを保護するため、ARP イベントの調査、トラブルシューティングを行っているときのみ、ARP ロギング機能を有効にしてください。

例

ARP ロギング機能を有効にします。

<Switch> system-view

[Switch] arp check log enable

1.1.3 arp mac-interface-consistency check enable

Syntax

arp mac-interface-consistency check enable

undo arp mac-interface-consistency check enable

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

arp mac-interface-consistency check enable コマンドはインタフェースで ARP エントリと MAC アドレスエントリの整合性のチェックを有効にします。

undo arp mac-interface-consistency check enable コマンドはインタフェースで ARP エントリと MAC アドレスエントリの整合性のチェックを無効にします。

不安定なネットワークでは、ユーザからのパケットの受信側インタフェースが変更されることがあります。MAC アドレスエントリのインタフェースはすぐに更新できますが、ARP エントリのインタフェースは更新できません。この場合、ARP エントリに一致するパケットは、正しくないインタフェースから送信されます。この問題を解決するには、この機能を使用して、エントリの ARP および MAC アドレスユーザのインタフェース整合性を定期的にチェックします。インタフェースが同じでない場合、ARP は ARP エントリの VLAN に ARP 要求を送信し、ARP 応答を受信したインタフェースでエントリを更新します。

MAC アドレスエントリを表示する場合、**display mac-address** コマンドを使用します。

例

インタフェースで ARP エントリと MAC アドレスエントリの整合性のチェックを有効にします。

<Switch> system-view

[Switch] arp mac-interface-consistency check enable

1.1.4 arp max-learning-num

Syntax

arp max-learning-num *number*

undo arp max-learning-num

デフォルト

1024

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

VLAN interface view

定義済みユーザロール

network-admin

パラメータ

number: インタフェースが学習できるダイナミック ARP エントリの最大数を指定します。設定範囲は 0〜1024 です。

説明

arp max-learning-num コマンドはインタフェースが学習できるダイナミック ARP エントリの最大数を設定します。

undo arp max-learning-num コマンドはデフォルトに戻します。

多くの ARP エントリを保持することを防ぐため、インタフェースが学習できるダイナミック ARP エントリの最大数を設定することができます。設定した最大数に到達すると、インタフェースは ARP エントリの学習を停止します。

0 に設定した場合、ダイナミック ARP エントリの学習を無効にします。

例

VLAN インタフェース 40 が学習できるダイナミック ARP エントリの最大数を 10 に設定します。

<Switch> system-view

[Switch] interface vlan-interface 40

[Switch-Vlan-interface40] arp max-learning-num 10

GigabitEthernet 1/0/1 が学習できるダイナミック ARP エントリの最大数を 10 に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] arp max-learning-num 10

Bridge-aggregation 1 が学習できるダイナミック ARP エントリの最大数を 10 に設定します。

<Switch> system-view

[Switch] interface bridge-aggregation 1

[Switch-Bridge-Aggregation1] arp max-learning-num 10

1.1.5 arp max-learning-number

Syntax

arp max-learning-number *max-number* **slot** *slot-number*

undo arp max-learning-number slot *slot-number*

デフォルト

4096

View

System view

定義済みユーザロール

network-admin

パラメータ

max-number: 装置が学習できるダイナミック ARP エントリの最大数を指定します。設定範囲は 0～4096 です。1024 をこえるばあいは安定動作ができなくなる可能性があります。

slot *slot-number:* メンバ ID によって IRF スタックメンバ装置を指定します。

説明

arp max-learning-number コマンドは装置のダイナミック ARP 学習制限を設定します。

undo arp max-learning-number コマンドはデフォルトに戻します。

装置は ARP エントリを動的に学習できます。装置が多くの ARP エントリを保持しすぎるのを防ぐために、装置が学習できるダイナミック ARP エントリの最大数を設定できます。最大数に達すると、装置は ARP エントリの学習を停止します。

number を 0 に設定すると、装置はダイナミック ARP エントリの学習を無効になります。

例

スロット 1 の ARP 学習制限を 64 に設定します。

<Switch> system-view

[Switch] arp max-learning-number 64 slot 1

1.1.6 arp multiport

Syntax

arp multiport *ip-address mac-address vlan-id* [**vpn-instance** *vpn-instance-name*]

undo arp *ip-address* [*vpn-instance-name*]

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

ip-address: マルチポート ARP エントリの IP アドレスを指定します。

mac-address:マルチポート ARP エントリの MAC アドレスを指定します。形式は H-H-H です。

vlan-id: マルチポート ARP エントリの VLAN を指定します。設定範囲は 1～4094 です。指定した VLAN がすでに存在している必要があります。

vpn-instance *vpn-instance-name*: マルチポート ARP エントリが属する VPN インスタンスを指定します。*vpn-instance-name* は、VPN インスタンス名を表します。大文字、小文字を区別します。設定範囲は 1～31 文字です。指定する VPN インスタンスはすでに存在している必要があります。指定しない場合、マルチポート ARP エントリはパブリックネットワークに所属します。

説明

arp multiport コマンドはマルチポート ARP エントリを設定します。

undo arp コマンドは ARP エントリを削除します。

VLAN あるいは対応する VLAN インタフェースが削除された場合、マルチポート ARP エントリも削除されます。

マルチポート ARP エントリをパケット転送に対して有効にするには、マルチキャストまたはマルチポートユニキャストのエントリアドレスを設定して、複数の出力インタフェースを指定する必要があります。MAC アドレスエントリは、マルチポート ARP エントリと同じ MAC アドレスおよび VLAN ID を持つ必要があります。また、マルチポート ARP エントリ内の IP アドレスは、指定された VLAN の VLAN インタフェースと同じサブネット上に存在する必要があります。

例

VLAN10 の IP アドレス 202.38.10.2 および MAC アドレス 0000-0001-0000 を含むマルチポート ARP エントリを設定します。

<Switch> system-view

[Switch] arp multiport 202.38.10.2 0000-0001-0000 10

関連コマンド

- **display arp multiport**
- **reset arp multiport**

1.1.7 arp static

Syntax

arp static *ip-address mac-address* [*vlan-id interface-type interface-number*] [**vpn-instance** *vpn-instance-name*]

undo arp *ip-address* [*vpn-instance-name*]

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

ip-address: スタティック ARP エントリの IP アドレスを指定します。

mac-address: スタティック ARP エントリの MAC アドレスを指定します。形式は H-H-H です。

vlan-id: ARP エントリが所属する VLAN の ID を指定します。設定範囲は 1～4094 です。VLAN と VLAN インタフェースはあらかじめ作成する必要があります。

interface-type interface-number: インタフェースのタイプと番号を指定します。インタフェースが指定された VLAN に所属していることを確認してください。

vpn-instance *vpn-instance-name*: スタティック ARP エントリの VPN インスタンスを指定します。大文字、小文字を区別します。設定範囲は 1～31 文字で指定します。VPN インスタンスがすでに存在していなければなりません。パブリックネットワークでスタティック ARP エントリを指定するには、このオプションは指定しないでください。

説明

arp static コマンドはスタティック ARP エントリを設定します。

undo arp コマンドはスタティック ARP エントリを削除します。

スタティック ARP エントリは手動で設定し維持します。スタティック ARP エントリはエージアウトしません。またダイナミック ARP エントリに上書きされることはありません。

スタティック ARP エントリはロングスタティック ARP エントリとショートスタティック ARP エントリに分類されます。

ショートスタティック ARP エントリは IP-MAC マッピングが含まれます。解決済みのショートスタティック ARP エントリは特定のイベントで未解決になります。たとえば、出力インタフェースがダウンしたとき、あるいは対応する VLAN や VLAN インタフェースが削除されたとき、未解決になります。

ロングスタティック ARP エントリは IP-MAC マッピング、VLAN、出力インタフェースが含まれます。ロングスタティック ARP エントリは以下の状態にある場合、未解決となり、パケットの転送に使用することができません。

- 対応する VLAN インタフェースあるいは出力インタフェースがダウンしています。
- エントリの IP アドレスがローカル IP アドレスと競合します。
- ローカルインタフェースに、ARP エントリの IP アドレスと同一のサブネットの IP アドレスがありません。

vlan-id interface-type interface-number を指定した場合、以下の制限とガイドラインに従ってください。

- インタフェースは Ethernet インタフェースあるいはアグリゲートインタフェースにする必要があります。
- VLAN、VLAN インタフェースはすでに作成されている必要があります。Ethernet インタフェースは VLAN に属している必要があります。
- VLAN インタフェースの IP アドレスと *ip-address* パラメータで指定された IP アドレスは同一ネットワークにする必要があります。
- VLAN あるいは VLAN インタフェースが削除された場合、VLAN のロングスタティック ARP エントリは削除されます。

例

IP アドレス 202.38.10.2、MAC アドレス f474-8801-0000、VLAN 10 の出力インタフェース GigabitEthernet 1/0/1 に対応するスタティック ARP エントリを設定します。

<Switch> system-view

[Switch] arp static 202.38.10.2 f474-8801-0000 10 gigabitethernet 1/0/1

関連コマンド

- **display arp**
- **reset arp**

1.1.8 arp timer aging

Syntax

arp timer aging *aging-time*

undo arp timer aging

デフォルト

20 分

View

System view

定義済みユーザロール

network-admin

パラメータ

aging-time: ダイナミック ARP エントリのエージングタイマを設定します。設定範囲は 1～1440 分です。

説明

arp timer aging コマンドはダイナミック ARP エントリのエージングタイマを設定します。

undo arp timer aging コマンドはデフォルトに戻します。

ARP テーブル上の各ダイナミック ARP エントリは有効期限を持っています。有効期限はエージングタイマと呼ばれ、有効期限内にダイナミック ARP エントリがアップデートされるたびに、エージングタイマはリセットされます。有効期限切れになる前に更新されなかったダイナミック ARP エントリは、ARP テーブルから削除されます。

必要に応じてダイナミック ARP エントリのエージングタイマを設定してください。たとえば proxy ARP を設定するとき、不正なダイナミック ARP エントリが時間内に削除されるようにエージングタイマを短い値に設定してください。

例

ダイナミック ARP エントリのエージングタイマを 10 分に設定します。

<Switch> system-view

[Switch] arp timer aging 10

関連コマンド

display arp timer aging

1.1.9 display arp

Syntax

display arp [[**all** | **dynamic** | **multiport** | **static**] [**slot** *slot-number*] | **vlan** *vlan-id* | **interface** *interface-type interface-number*] [**count** | **verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all: すべての ARP エントリを表示します。

dynamic: ダイナミック ARP エントリを表示します。

multiport: マルチポート ARP エントリを表示します。

static: スタティック ARP エントリを表示します。

slot *slot-number*: IRF スタックメンバ装置の ARP エントリを表示します。*slot-number* は IRF スタックメンバ装置の ID を指定します。

vlan *vlan-id*: 指定した VLAN の ARP エントリを表示します。設定範囲は 1～4094 です。

interface *interface-type interface-number*: *interface-type interface-number* で指定されたインタフェースの ARP エントリを表示します。

count: ARP エントリ数を表示します。

verbose: ARP エントリの詳細情報を表示します。

説明

display arp コマンドは ARP エントリを表示します。

このコマンドは IP アドレス、MAC アドレス、VLAN ID、出力インタフェース、エントリタイプ、エージングタイマを含む ARP エントリの情報を表示します。

パラメータを指定しない場合、すべての ARP エントリを表示します。

例

すべての ARP エントリを表示します。

<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              16    D
1.1.1.3         00e0-fe50-6503 12     Tunnel1              15    D
```

```
1.1.1.4         000d-88f7-9f7d  12      0x1                 16    D
```

すべての ARP エントリの詳細情報を表示します。

<Switch> display arp all verbose

```
  Type: S-Static   D-Dynamic   O-Openflow   R-Rule   M-Multiport  I-Invalid
IP Address      : 1.1.1.1         VID : 1          Aging   : N/A
MAC Address     : 02e0-f102-0023   Type: S          Nickname: 0x0000
Interface/Link ID: GE1/0/1
VPN Instance    : [No Vrf]
VSI Name        : N/A
VSI Interface   : N/A

IP Address      : 1.1.1.2         VID : 12         Aging   : 16
MAC Address     : 0015-e944-adc5   Type: D          Nickname: 0x0000
Interface/Link ID: GE1/0/2
VPN Instance    : [No Vrf]
VSI Name        : N/A
VSI Interface   : N/A

IP Address      : 1.1.1.3        VID : 12         Aging   : 15
MAC Address     : 0013-1234-0001  Type: D          Nickname: 0x0000
Interface/Link ID: Tunnel1
VPN Instance    : [No Vrf]
VSI Name        : vpna
VSI Interface   : Vsi1

IP Address      : 1.1.1.4        VID : 12         Aging   : 16
MAC Address     : 0012-1234-0002  Type: D          Nickname: 0x0000
Interface/Link ID: 0x1
VPN Instance    : [No Vrf]
VSI Name        : vpna
VSI Interface   : Vsi1
```

すべての ARP エントリの数を表示します。

<Switch> display arp all count

```
 Total number of entries : 4
```

表 1-1 コマンド出力

フィールド	説明
IP Address	ARPエントリのIPアドレスです。
MAC Address	ARPエントリのMACアドレスです。

フィールド	説明
VID	ARPエントリが所属するVLAN IDです。以下のどちらかの状態である場合、**N/A**と表示されます。 • ARPエントリが未解決のショートスタティックARPエントリです。 • ARPエントリの出力インタフェースがVLANに所属していません。
Interface/Link ID	ARPエントリの出力インタフェースです。ARPエントリが未解決のショートスタティックARPエントリである場合、マルチポートARPエントリで出力インタフェース情報がない場合、**N/A**と表示されます。 マルチポートARPエントリの出力インタフェース情報を取得するには、ARPエントリのMACアドレスに従ってMACアドレステーブルを検索します。
Aging	ダイナミックARPエントリのエージングタイマです。単位は分です。**N/A**はエージングタイマが不明あるいはエージングタイマが有効期限切れであることを示します。
Type	ARPエントリのタイプです。 • **D**–ダイナミックARPエントリです。 • **S**–スタティックARPエントリです。 • **M**—マルチポートARPエントリです。 • **I**–無効なARPエントリです。
VPN Instance	VPNインスタンスの名前です。ARPエントリにVPNインスタンスが設定されていない場合、**[No Vrf]**と表示されます。 このフィールドは現在のソフトウェアバージョンではサポートしていません。
VSI Name	ARPエントリが属しているVSIの名前です。ARPエントリがVSIに所属していない場合、**N/A**と表示されます。 このフィールドは現在のソフトウェアバージョンではサポートしていません。
VSI Interface	VSIのゲートウェイインタフェースです。VSIでゲートウェイインタフェースが指定されていない場合、**N/A**と表示されます。 このフィールドは現在のソフトウェアバージョンではサポートしていません。
Total number of entries	ARPエントリ数です。

関連コマンド

- **arp static**

- **reset arp**

1.1.10 display arp *ip-address*

Syntax

display arp *ip-address* [**slot** *slot-number*] [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ip-address: 指定した IP アドレスの ARP エントリを表示します。

slot *slot-number*: IRF スタックメンバ装置の ARP エントリを表示します。*slot-number* は IRF スタックメンバ装置の ID を指定します。

verbose: ARP エントリの詳細情報を表示します。

説明

display arp ip-address コマンドは IP アドレスの ARP エントリを表示します。

ARP エントリの情報は IP アドレス、MAC アドレス、VLAN ID、出力インタフェース、エントリタイプ、エージングタイマを含みます。

例

IP アドレス 20.1.1.1 の ARP エントリを表示します。

<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
```

関連コマンド

- **arp static**
- **reset arp**

1.1.11 display arp timer aging

Syntax

display arp timer aging

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display arp timer aging コマンドはダイナミック ARP エントリのエージングタイマを表示します。

例

ダイナミック ARP エントリのエージングタイマを表示します。

<Switch> display arp timer aging

```
Current ARP aging time is 20 minute(s)(default)
```

関連コマンド

arp timer aging

1.1.12 display arp vpn-instance

Syntax

display arp vpn-instance *vpn-instance-name* [**count**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

vpn-instance-name: 名前で VPN インスタンスを指定します。大文字、小文字を区別し 1～31 文字で指定します。VPN インスタンス名にスペースを含めることはできません。

count: ARP エントリの数を表示します。

説明

display arp vpn-instance コマンドは、VPN インスタンスの ARP エントリを表示します。

このコマンドは、IP アドレス、MAC アドレス、VLAN ID、出力インタフェース、エントリタイプやエージングタイマを含め、VPN インスタンスの ARP エントリの情報を表示します。

例

VPN インスタンス **test** の ARP エントリを表示します。

<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        0000-0001-0001 N/A    N/A                N/A   S
```

関連コマンド

- **arp static**
- **reset arp**

1.1.13 reset arp

Syntax

reset arp { **all** | **dynamic** | **interface** *interface-type interface-number* | **multiport** | **slot** *slot-number* | **static** }

View

User view

定義済みユーザロール

network-admin

パラメータ

all: すべての ARP エントリを削除します。

dynamic: すべてのダイナミック ARP エントリを削除します。

multiport: マルチポート ARP エントリを削除します。

static: すべてのスタティック ARP エントリを削除します。

slot *slot-number*: IRF スタックメンバ装置の ARP エントリを削除します。*slot-number* は IRF スタックメンバ装置の ID を指定します。指定しない場合、マスタ装置の ARP エントリを削除します。

interface *interface-type interface-number*: *interface-type interface-number* で指定されたインタフェースの ARP エントリを削除します。指定しない場合、すべてのインタフェースの ARP エントリを削除します。

説明

reset arp コマンドは ARP テーブルから ARP エントリを削除します。

例

すべてのスタティック ARP エントリを削除します。

<Switch> reset arp static

関連コマンド

- **arp static**
- **display arp**

目次

このセクションのページは **4-x-x** です。

2 章 Gratuitous ARP 2-1
2.1 Gratuitous ARP 設定コマンド 2-1
2.1.1 arp ip-conflict log prompt 2-1
2.1.2 arp send-gratuitous-arp 2-2
2.1.3 gratuitous-arp mac-change retransmit 2-3
2.1.4 gratuitous-arp-learning enable 2-4
2.1.5 gratuitous-arp-sending enable 2-5

2章 Gratuitous ARP

2.1 Gratuitous ARP設定コマンド

2.1.1 arp ip-conflict log prompt

Syntax

arp ip-conflict log prompt

undo arp ip-conflict log prompt

デフォルト

無効

受信した ARP パケットの送信元 IP アドレスを使用する場合、装置は以下のように動作します。

- gratuitous ARP 要求を送信します。
- 重複に関する ARP 応答を装置が受信した後に、エラーメッセージを表示します。

View

System view

定義済みユーザロール

network-admin

説明

arp ip-conflict log prompt コマンドは重複の確認を行わず、IP 重複の通知を有効にします。

undo arp ip-conflict log prompt コマンドはデフォルトに戻します。

コマンドは、重複に関する ARP 応答を装置が受信、あるいは ARP 要求を送信する前に、エラーメッセージを表示することができます。

例

装置で IP 重複の通知を有効にします。

<Switch> system-view

[Switch] arp ip-conflict log prompt

2.1.2 arp send-gratuitous-arp

Syntax

arp send-gratuitous-arp [**interval** *interval*]

undo arp send-gratuitous-arp

デフォルト

無効

ARP パケットを送信する送信間隔のデフォルトは 2000 ミリ秒です。

View

VLAN interface view

定義済みユーザロール

network-admin

パラメータ

interval *interval*: gratuitous ARP パケットを送信する送信間隔を設定します。設定範囲は 200～200000 ミリ秒です。

説明

arp send-gratuitous-arp コマンドはインタフェースで gratuitous ARP パケットの定期送信を有効にし、送信間隔を設定します。

undo arp send-gratuitous-arp コマンドはインタフェースで gratuitous ARP パケットを定期的に送信することを無効にします。

このコマンドは有効にしたインタフェースが up で IP アドレスが設定されているときのみ、適用されます。

この機能はインタフェースのプライマリ IP アドレス、あるいは手動で設定されたセカンダリ IP アドレスの gratuitous ARP 要求のみ送信することができます。プライマリ IP アドレスは手動または自動で設定することができますが、セカンダリ IP アドレスは手動で設定する必要があります。

gratuitous ARP パケットの送信間隔を変更すると、次の送信間隔から設定が適用されます。

gratuitous ARP パケットの送信間隔は以下の状況によって、設定した値よりも短くなります。

- 複数のインタフェースで有効にされた場合
- 各インタフェースで複数のセカンダリ IP アドレスが設定された場合
- 優先する状況で短い送信間隔を設定した場合

例

VLAN インタフェース 2 で gratuitous ARP パケットの定期送信を有効にし、送信間隔を 300 ミリ秒に設定します。

<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

Syntax

gratuitous-arp mac-change retransmit *times* **interval** *seconds*

undo gratuitous-arp mac-change retransmit

デフォルト

MAC アドレスが変更された時に gratuitous ARP パケットを 1 回送信します。

View

System view

定義済みユーザロール

network-admin

パラメータ

times: gratuitous ARP パケットを再送信する回数を設定します。設定範囲は 1 から 10 です。

interval *seconds*: gratuitous ARP パケットを再送信する送信間隔を設定します。設定範囲は 1 秒から 10 秒です。

説明

gratuitous-arp mac-change retransmit コマンドは MAC アドレス変更による gratuitous ARP パケットの複数送信を有効にし、送信間隔を設定します。

undo gratuitous-arp mac-change retransmit コマンドは MAC アドレス変更による gratuitous ARP パケットの送信を 1 回にします。

この機能は、装置の MAC アドレスが変更にされたときに送信する gratuitous ARP パケットを、指定された間隔で指定された時間再送信します。

装置は、MAC アドレスの変更を他のデバイスに通知するために、gratuitous ARP パケットを送信します。ただし、装置はデフォルトで 1 回だけ gratuitous ARP パケットを送信するため、他の装置はパケットの受信に失敗する可能性があります。この機能を使用し

て、他の装置がパケットを受信できるように、gratuitous ARP パケットを再送信するパラメータを設定します。

例

MAC アドレス変更による gratuitous ARP パケットの再送信を有効にし、送信数を 3 回、間隔を 5 秒に設定します。

<Switch> system-view

[Switch] gratuitous-arp mac-change retransmit 3 interval 5

2.1.4 gratuitous-arp-learning enable

Syntax

gratuitous-arp-learning enable

undo gratuitous-arp-learning enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

gratuitous-arp-learning enable コマンドは gratuitous ARP パケットの学習機能を有効にします。

undo gratuitous-arp-learning enable コマンドは gratuitous ARP パケットの学習機能を無効にします。

gratuitous ARP パケットの学習機能は、装置が受信した gratuitous ARP パケットをもとに ARP エントリを作成あるいはアップデートすることで ARP テーブルを維持することができます。

学習機能が無効であるとき、装置は既存の ARP エントリのみをアップデートするため受信した gratuitous ARP パケットを使用します。ARP エントリは受信した gratuitous ARP パケットをもとに作成されません。これは ARP テーブルの空き容量を節約します。

例

gratuitous ARP パケットの学習機能を有効にします。

<Switch> system-view

[Switch] gratuitous-arp-learning enable

2.1.5 gratuitous-arp-sending enable

Syntax

gratuitous-arp-sending enable

undo gratuitous-arp-sending enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

gratuitous-arp-sending enable コマンドは異なるサブネットから ARP 要求を受信した際に、gratuitous ARP パケットの送信を有効にします。

undo gratuitous-arp-sending enable コマンドはデフォルトに戻します。

例

異なるサブネットから ARP 要求を受信した際に、gratuitous ARP パケットの送信を無効にします。

<Switch> system-view

[Switch] undo gratuitous-arp-sending enable

目次

このセクションのページは **4-x-x** です。

3 章 Proxy ARP 3-1
3.1 Proxy ARP 設定コマンド 3-1
3.1.1 display local-proxy-arp 3-1
3.1.2 display proxy-arp 3-2
3.1.3 local-proxy-arp enable 3-2
3.1.4 proxy-arp enable 3-4

3章 Proxy ARP

3.1 Proxy ARP設定コマンド

3.1.1 display local-proxy-arp

Syntax

display local-proxy-arp [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: 指定したインタフェースのローカル Proxy ARP の状態を表示します。

説明

display local-proxy-arp コマンドはローカル Proxy ARP の状態を表示します。

ローカル Proxy ARP の状態は有効あるいは無効にすることができます。

インタフェースを指定した場合、指定したインタフェースのローカル Proxy ARP の状態を表示します。

インタフェースを指定しない場合、すべてのインタフェースのローカル Proxy ARP の状態を表示します。

例

VLAN インタフェース 2 のローカル Proxy ARP の状態を表示します。

<Switch> display local-proxy-arp interface vlan-interface 2

```
Interface Vlan-interface2
 Local Proxy ARP status: enabled
```

関連コマンド

local-proxy-arp enable

3.1.2 display proxy-arp

Syntax

display proxy-arp [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: 指定したインタフェースの Proxy ARP の状態を表示します。

説明

display proxy-arp コマンドは Proxy ARP の状態を表示します。

Proxy ARP の状態は有効あるいは無効にすることができます。

インタフェースを指定した場合、指定したインタフェースの Proxy ARP の状態を表示します。

インタフェースを指定しない場合、すべてのインタフェースの Proxy ARP の状態を表示します。

例

VLAN インタフェース 1 の Proxy ARP の状態を表示します。

<Switch> display proxy-arp interface Vlan-interface 1

```
Interface Vlan-interface1
 Proxy ARP status: disabled
```

関連コマンド

proxy-arp enable

3.1.3 local-proxy-arp enable

Syntax

local-proxy-arp enable [**ip-range** *startIP* **to** *endIP*]

undo local-proxy-arp enable

デフォルト

無効

View

VLAN interface view

定義済みユーザロール

network-admin

パラメータ

ip-range *startIP* **to** *endIP*: ローカル Proxy ARP を有効にする IP アドレスの範囲を指定します。*startIP* は *endIP* 以下の値にしてください。

説明

local-proxy-arp enable コマンドはローカル Proxy ARP を有効にします。

undo local-proxy-arp enable コマンドはローカル Proxy ARP を無効にします。

Proxy ARP は異なるネットワークの IP アドレスの ARP 要求に応答するため、ネットワークの装置で有効にします。Proxy ARP を有効にすることで、異なるブロードキャストドメインのホストが同一のブロードキャストドメインにいるように互いに通信できるようにします。

Proxy ARP は一般的な Proxy ARP とローカル Proxy ARP があります。

一般的な Proxy ARP は異なるレイヤ 3 インタフェースに接続され、異なるブロードキャストドメインに存在するホスト間で通信することができます。

ローカル Proxy ARP は同一のレイヤ 3 インタフェースに接続され、異なるブロードキャストドメインに存在するホスト間で通信することができます。

ip-range を指定することで 1 つの IP アドレス範囲を設定することができます。

例

VLAN インタフェース 2 でローカル Proxy ARP を有効にします。

<Switch> system-view

[Switch] interface vlan-interface 2

[Switch-Vlan-interface2] local-proxy-arp enable

VLAN インタフェース 2 で IP アドレス範囲 1.1.1.1～1.1.1.20 のローカル Proxy ARP を有効にします。

<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

関連コマンド

display local-proxy-arp

3.1.4 proxy-arp enable

Syntax

proxy-arp enable

undo proxy-arp enable

デフォルト

無効

View

VLAN interface view

定義済みユーザロール

network-admin

説明

proxy-arp enable コマンドは Proxy ARP を有効にします。

undo proxy-arp enable コマンドは Proxy ARP を無効にします。

Proxy ARP は異なるネットワークの IP アドレスの ARP 要求に応答するため、ネットワークの装置で有効にします。Proxy ARP を有効にすることで、異なるブロードキャストドメインのホストが同一のブロードキャストドメインにいるように互いに通信できるようにします。

Proxy ARP は一般的な Proxy ARP とローカル Proxy ARP があります。

一般的な Proxy ARP は異なるレイヤ 3 インタフェースに接続され、異なるブロードキャストドメインに存在するホスト間で通信することができます。

ローカル Proxy ARP は同一のレイヤ 3 インタフェースに接続され、異なるブロードキャストドメインに存在するホスト間で通信することができます。

例

VLAN インタフェース 2 で Proxy ARP を有効にします。

<Switch> system-view

[Switch] interface vlan-interface 2

[Switch-Vlan-interface2] proxy-arp enable

関連コマンド

display proxy-arp

目次

このセクションのページは **4-x-x** です。

4 章 ARP スヌーピング 4-1
4.1 ARP snooping 設定コマンド 4-1
4.1.1 arp snooping enable 4-1
4.1.2 display arp snooping 4-1
4.1.3 reset arp snooping 4-3

4章 ARP スヌーピング

4.1 ARP snooping設定コマンド

4.1.1 arp snooping enable

Syntax

arp snooping enable

undo arp snooping enable

デフォルト

無効

View

VLAN view

定義済みユーザロール

network-admin

説明

arp snooping enable コマンドは ARP snooping を有効にします。

undo arp snooping enable コマンドはデフォルトに戻します。

例

VLAN 2 で ARP snooping を有効にします。

<Switch> system-view

[Switch] vlan 2

[Switch-vlan2] arp snooping enable

4.1.2 display arp snooping

Syntax

display arp snooping [**vlan** *vlan-id*] [**slot** *slot-number*] [**count**]

display arp snooping ip *ip-address* [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

vlan *vlan-id*: VLAN の ARP snooping エントリを表示します。設定範囲は 1～4094 です。

count: 現在の ARP snooping エントリの数を表示します。

ip *ip-address*: 指定されたインタフェースの ARP snooping エントリを表示します。

slot *slot-number*: IRF スタックメンバ装置を指定します。*slot-number* は IRF スタックユニットのメンバ装置 ID です。

説明

display arp snooping コマンドは ARP snooping エントリを表示します。

パラメータを指定しない場合、すべての ARP snooping エントリを表示します。

例

VLAN 2 の snooping エントリを表示します。

<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
```

現在の ARP snooping エントリの数を表示します。

<Switch> display arp snooping count

```
Total entries: 2
```

表 4-1 コマンド出力

フィールド	説明
IP Address	ARP snoopingエントリのIPアドレスです。
MAC Address	ARP snoopingエントリのMACアドレスです。
VLAN ID	ARP snoopingエントリが所属するVLAN IDです。
Interface	ARP snoopingエントリの入力インタフェースです。
Aging	ARP snoopingエントリのエージングタイマです。単位は分です。

フィールド	説明
Status	ARP snoopingエントリの状態です。 ● **Valid**－正常なARP snoopingエントリです。 ● **Invalid**－不正なARP snoopingエントリです。 ● **Collision**－ARP snoopingエントリが重複しています。
Total entries	ARP snoopingエントリの数です。

関連コマンド

reset arp snooping

4.1.3 reset arp snooping

Syntax

reset arp snooping [**ip** *ip-address* | **vlan** *vlan-id*]

View

User view

定義済みユーザロール

network-admin

パラメータ

ip *ip-address*: 指定した IP アドレスの ARP snooping エントリを削除します。

vlan *vlan-id*: 指定した VLAN の ARP snooping エントリを削除します。設定範囲は 1～4094 です。

説明

reset arp snooping コマンドは ARP snooping エントリを削除します。

パラメータを指定しない場合、すべての ARP snooping エントリを削除します。

例

VLAN 2 の ARP snooping エントリを削除します。

<Switch> reset arp snooping vlan 2

関連コマンド

display arp snooping

目次

このセクションのページは **4-x-x** です。

5 章 IP アドレス 5-1
5.1 IP アドレス設定コマンド 5-1
5.1.1 display ip interface 5-1
5.1.2 display ip interface brief 5-4
5.1.3 ip address 5-7
5.1.4 ip address unnumbered 5-8

5章 IP アドレス

5.1 IPアドレス設定コマンド

5.1.1 display ip interface

Syntax

display ip interface [*interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface-type interface-number: インタフェースのタイプと番号を指定します。指定しない場合、すべてのレイヤ 3 インタフェースの IP の設定と統計情報を表示します。

説明

display ip interface コマンドは指定したレイヤ 3 インタフェースあるいはすべてのレイヤ 3 インタフェースの IP の設定と統計情報を表示します。

統計情報には以下の情報が含まれます。

- ユニキャストパケットの数、バイト、インタフェースが送受信したマルチキャストパケットが含まれます。
- TTL 無効のパケットの数、インタフェースが受信した ICMP パケットの数が含まれます。

例

VLAN インタフェース 10 の IP の設定と統計情報を表示します。

<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
```

表 5-1 コマンド出力

フィールド	説明
current state	インタフェースの現在の物理状態です。 ● **Administrative DOWN**—インタフェースが**shutdown**コマンドでシャットダウンしています。 ● **DOWN**—インタフェースが管理上upとなっていますが、物理的にdownしています。ケーブル接続あるいはリンク障害によって引き起こされる可能性があります。 ● **UP**—インタフェースが管理上および物理的にupとなっています。
Line protocol current state	リンクレイヤプロトコルの現在の状態です。 ● **DOWN**—インタフェースのプロトコル状態がdownしています。 ● **UP**—インタフェースのプロトコル状態がupしています。 ● **UP (spoofing)**—インタフェースのプロトコル状態がUpしているように見せかけていることを示します。対応するリンクが存在しない、あるいはリンクがオンデマンドでのみ設定されることを示します。

フィールド	説明
Internet Address	インタフェースのIPアドレスです。 ● **Primary**—プライマリIPアドレスです。 ● **Sub**—セカンダリIPアドレスです。 ● **DHCP-Allocated**—DHCPによって取得したIPアドレスです。 ● **BOOTP-Allocated**—BOOTPによって取得したIPアドレスです。 ● **Mad**—MADのIPアドレスです。
Broadcast address	インタフェースに接続されたサブネットのブロードキャストアドレスです。
The Maximum Transmit Unit	インタフェースのMTU（最大転送ユニット）です。単位はバイトです。
input packets, bytes, multicasts output packets, bytes, multicasts	インタフェースで受信したユニキャストパケット、バイト、マルチキャストパケットです。（装置起動時に統計情報の取得が開始されます。）
TTL invalid packet number	インタフェースで受信したTTL無効のパケット数です。（装置起動時に統計情報の取得が開始されます。）

フィールド	説明
ICMP packet input number: Echo reply: 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:	インタフェースで受信したICMPパケットの総数です。（装置起動時に統計情報の取得が開始されます。） ● **Echo reply packets**－エコー応答パケットです。 ● **Unreachable packets**－到達不能パケットです。 ● **Source quench packets**－送信元抑制パケットです。 ● **Routing redirect packets**－ルーティングリダイレクトパケットです。 ● **Echo request packets**－エコー要求パケットです。 ● **Router advertisement packets**－ルータ通知パケットです。 ● **Router solicitation packets**－ルータ選択要求パケットです。 ● **Time exceeded packets**－時間超過パケットです。 ● **IP header bad packets**－IPヘッダ不良パケットです。 ● **Timestamp request packets**－タイムスタンプ要求パケットです。 ● **Timestamp reply packets**－タイムスタンプ応答パケットです。 ● **Information request packets**－情報要求パケットです。 ● **Information reply packets**－情報応答パケットです。 ● **Netmask request packets**－ネットマスク要求パケットです。 ● **Netmask reply packets**－ネットマスク応答パケットです。 ● **Unknown type packets**－不明なタイプのパケットです。

関連コマンド

- **display ip interface brief**
- **ip address**

5.1.2 display ip interface brief

Syntax

display ip interface [*interface-type* [*interface-number*]] **brief**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface-type: インタフェースタイプを指定します。指定しない場合、すべてのレイヤ 3 インタフェースの IP 設定の概要情報を表示します。

interface-number: インタフェース番号を指定します。指定しない場合、指定したタイプのすべてのレイヤ 3 インタフェースの IP 設定の概要情報を表示します。

説明

display ip interface brief コマンドはレイヤ 3 インタフェースの IP 設定の概要情報を表示します。物理リンクの状態、リンクレイヤプロトコルの状態、IP アドレス、インタフェースの説明が含まれます。

例

VLAN インタフェースの IP 設定の概要情報を表示します。

<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...
<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
```

表 5-2 コマンド出力

フィールド	説明
*down: administratively down	インタフェースが**shutdown**コマンドでシャットダウンしています。
(s) : spoofing	インタフェースのスプーフィング属性です。リンクレイヤプロトコルがUp表示されているインタフェースにリンクがない、あるいはリンクがオンデマンドでのみ設定されることを示します。
Interface	インタフェース名です。

フィールド	説明
Physical	インタフェースの物理状態です。 ● ***down**—インタフェースが**shutdown**コマンドでシャットダウンしています。 ● **down**—インタフェースが管理上upとなっていますが、物理的にdownしています。ケーブル接続あるいはリンク障害によって引き起こされる可能性があります。 ● **up**—インタフェースが管理上および物理的にupとなっています。
Protocol	インタフェースのリンクレイヤプロトコルの状態です。 ● **down**—インタフェースのプロトコル状態がdownしています。(一般的にインタフェースにIPアドレスが設定されていない時に起こります。) ● **down(l)**—ループバックインタフェースのプロトコル状態がdownしています。 ● **up**—インタフェースのリンクレイヤプロトコルがupです。 ● **up(l)**—ループバックインタフェースのリンクレイヤプロトコルがupです。 ● **up(s)**—インタフェースのプロトコル状態がup（spoofing）です。
IP Address	インタフェースのIPアドレスです。設定されていない場合、（--）と表示されます。
VPN instance	インタフェースが属しているVPNインスタンスの名前です。最大12文字です。名前が12文字より長い場合、最初の9文字が表示され、（...）が続きます。インタフェースがVPNインスタンスに所属していない場合、（--）と表示されます。 このフィールドは現在のソフトウェアバージョンでサポートしていません。
Description	インタフェースの説明の情報です。 最大12文字が表示されます。12文字より多い場合、最初の9文字が表示され、（...）が続きます。説明が設定されていない場合、（--）と表示されます。

関連コマンド

- **display ip interface**
- **ip address**

5.1.3 ip address

Syntax

ip address *ip-address* { *mask-length* | *mask* } [**sub**]

undo ip address [*ip-address* { *mask-length* | *mask* } [**sub**]

デフォルト

設定なし

View

Interface view

定義済みユーザロール

network-admin

パラメータ

ip-address: インタフェースの IP アドレスを指定します。ドットで区切り、10 進数で指定します。

mask-length: サブネットマスクの長さを指定します。設定範囲は 1～31 です。ループバックインタフェースの設定範囲は 1～32 です。

mask: サブネットマスクを指定します。ドットで区切り、10 進数で指定します。

sub: インタフェースにセカンダリ IP アドレスを割り当てます。

説明

ip address コマンドはインタフェースに IP アドレスを割り当てます。

undo ip address コマンドはインタフェースから IP アドレスを削除します。

インタフェースのプライマリ IP アドレスあるいはセカンダリ IP アドレスを設定するために、このコマンドを使用します。

インタフェースは 1 つのプライマリ IP アドレスのみ設定することができます。新しく設定されたプライマリ IP アドレスは、古いアドレスを上書きします。インタフェースが複数のサブネットに接続されている場合、サブネットがインタフェースを通して通信できるように、プライマリ IP アドレスとサブネットを設定します。

BOOTP、DHCP、PPP を通して IP アドレスを取得するインタフェースはセカンダリ IP アドレスを設定することができません。

undo ip address コマンドはインタフェースからすべての IP アドレスを削除します。

undo ip address *ip-address* { *mask* | *mask-length* }コマンドはプライマリ IP アドレスを削除します。**undo ip address** *ip-address* { *mask* | *mask-length* } **sub** コマンドはセカンダリ IP アドレスを削除します。

インタフェースに割り当てたプライマリ IP アドレスとセカンダリ IP アドレスは同一ネットワークセグメント上に設定することができますが、装置の異なるインタフェースは異なるネットワークセグメント上に存在する必要があります。

例

VLAN インタフェース 10 にプライマリ IP アドレスを 129.12.0.1、セカンダリ IP アドレスを 202.38.160.1、サブネットマスクを 255.255.255.0 に設定します。

<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

関連コマンド

- **display ip interface**
- **display ip interface brief**

5.1.4 ip address unnumbered

Syntax

ip address unnumbered interface *interface-type interface-number*

undo ip address unnumbered

デフォルト

設定なし

View

Interface view

定義済みユーザロール

network-admin

パラメータ

interface *interface-type interface-number*: 現在のインタフェースが IP アドレスを借用できるインタフェースを指定します。

説明

ip address unnumbered コマンドは現在のインタフェースを IP unnumbered として設定し、指定したインタフェースから IP アドレスを借用します。

undo ip address unnumbered コマンドはデフォルトに戻します。

通常、IP アドレスは手動または DHCP を使用してインタフェースに割り当てます。IP アドレスが十分でない場合、またはインタフェースがごくたまにしか使用されない場合は、他のインタフェースから IP アドレスを借りるようにインタフェースを設定できます。これは IP アンナンバードと呼ばれ、IP アドレスを借用するインタフェースは IP アンナンバードインタフェースと呼ばれます。

ループバックインタフェースは他のインタフェースの IP アドレスを借用できませんが、他のインタフェースはループバックインタフェースの IP アドレスを借用できます。

複数のインタフェースが同じ番号なし IP アドレスを使用できます。インタフェースに手動で設定された IP アドレスが複数ある場合は、手動で設定されたプライマリ IP アドレスのみを借用できます。

IP アドレスが設定されていないインタフェースでダイナミックルーティングプロトコルを有効にすることはできません。インタフェースが他の装置と通信できるようにするには、インタフェースのピア装置へのスタティックルートを設定する必要があります。

例

VLAN インタフェース 100 の IP アドレスを借用するように VLAN インタフェース 10 を設定します。

```
<Switch> system-view
[Switch] interface vlan-interface 10
[Switch-Vlan-interface10] ip address unnumbered interface vlan-interface 100
```

目次

このセクションのページは **4-x-x** です。

6 章 DHCP 6-1
6.1 DHCP 設定コマンド 6-1
6.1.1 dhcp dscp 6-1
6.1.2 dhcp enable 6-2
6.1.3 dhcp select 6-2

6章 DHCP

6.1 DHCP設定コマンド

6.1.1 dhcp dscp

Syntax

dhcp dscp *dscp-value*

undo dhcp dscp

デフォルト

56

View

System view

定義済みユーザロール

network-admin

パラメータ

dscp-value: DHCP パケットの DSCP を設定します。設定範囲は 0～63 です。

説明

dhcp dscp コマンドは DHCP サーバあるいは DHCP リレーエージェントに送信される DHCP パケットの DSCP を設定します。

undo dhcp dscp コマンドはデフォルトに戻します。

DHCP パケットの DSCP の値はパケットのプライオリティを指定します。パケットを送信するプライオリティに影響します。DSCP の値が大きくなると、プライオリティが高くなります。

例

DHCP パケットの DSCP を 30 に設定します。

<Switch> system-view

[Switch] dhcp dscp 30

6.1.2 dhcp enable

Syntax

dhcp enable

undo dhcp enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

dhcp enable コマンドは DHCP を有効にします。

undo dhcp enable コマンドは DHCP を無効にします。

DHCP に関する設定は DHCP を有効にしたのち適用されます。

DHCP サーバあるいは DHCP リレーエージェントの設定を実行する前に、DHCP を有効にしてください。

例

DHCP を有効にします。

<Switch> system-view

[Switch] dhcp enable

6.1.3 dhcp select

Syntax

dhcp select { **relay** | **server** }

undo dhcp select { **relay** | **server** }

デフォルト

インタフェースは DHCP サーバモードで動作し、設定パラメータの DHCP 要求に応答します。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

relay: インタフェースで DHCP リレーエージェントを有効にします。

server: インタフェースで DHCP サーバを有効にします。

説明

dhcp select コマンドはインタフェースで DHCP サーバあるいは DHCP リレーエージェントを有効にします。

undo dhcp select コマンドはインタフェースで DHCP サーバあるいは DHCP リレーエージェントを無効にします。

インタフェースは DHCP パケットを廃棄します。

インタフェースで DHCP サーバモードを DHCP リレーエージェントモードに変更する前に、**reset dhcp server ip-in-use** コマンドでアドレスの割り当てと許可された ARP エントリを削除してください。これらの割り当ては、DHCP リレーエージェントが有効になったのち、作成される ARP エントリと重複する可能性があります。

例

VLAN インタフェース 2 で DHCP リレーエージェントを有効にします。

<Switch> system-view

[Switch] interface vlan-interface 2

[Switch-Vlan-interface2] dhcp select relay

関連コマンド

dhcp relay server-address

目次

このセクションのページは **4-x-x** です。

7 章 DHCP サーバ 7-1
7.1 DHCP サーバ設定コマンド 7-1
7.1.1 address range 7-1
7.1.2 bims-server 7-2
7.1.3 bootfile-name 7-3
7.1.4 class option-group 7-4
7.1.5 dhcp class 7-5
7.1.6 dhcp option group 7-6
7.1.7 dhcp server apply ip-pool 7-7
7.1.8 dhcp server forbidden-ip 7-8
7.1.9 dhcp server ip-pool 7-9
7.1.10 dhcp server ping packets 7-10
7.1.11 dhcp server ping timeout 7-11
7.1.12 dhcp server relay information enable 7-12
7.1.13 display dhcp server conflict 7-13
7.1.14 display dhcp server expired 7-14
7.1.15 display dhcp server free-ip 7-15
7.1.16 display dhcp server ip-in-use 7-17
7.1.17 display dhcp server pool 7-18
7.1.18 display dhcp server statistics 7-21
7.1.19 dns-list 7-23
7.1.20 domain-name 7-24
7.1.21 expired 7-25
7.1.22 forbidden-ip 7-26
7.1.23 gateway-list 7-27
7.1.24 if-match 7-28
7.1.25 nbns-list 7-31
7.1.26 netbios-type 7-32
7.1.27 network 7-33
7.1.28 next-server 7-34
7.1.29 option 7-35
7.1.30 reset dhcp server conflict 7-37
7.1.31 reset dhcp server expired 7-37
7.1.32 reset dhcp server ip-in-use 7-38
7.1.33 reset dhcp server statistics 7-39
7.1.34 static-bind 7-39

7.1.35 tftp-server domain-name 7-41
7.1.36 tftp-server ip-address 7-42
7.1.37 voice-config 7-43

7章 DHCP サーバ

7.1 DHCPサーバ設定コマンド

7.1.1 address range

Syntax

address range *start-ip-address end-ip-address*

undo address range

デフォルト

設定なし

View

DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

start-ip-address: 開始 IP アドレスを指定します。

end-ip-address: 終了 IP アドレスを指定します。

説明

address range コマンドはダイナミックの割り当てを行うため DHCP アドレスプールの IP アドレス範囲を設定します。

undo address range コマンドは DHCP アドレスプールの IP アドレス範囲を削除します。

IP アドレス範囲が指定されていない場合、address pool view で **network** コマンドを使用してサブネットのすべての IP アドレスを割り当てることができます。IP アドレス範囲が指定されている場合、IP アドレス範囲の IP アドレスのみを割り当てることができます。

address range コマンドを使用した後、アドレスプールのセカンダリサブネットを指定するため、**network secondary** コマンドを使用することができません。

コマンドを複数回設定した場合、最後に行った設定が適用されます。

address range で指定されたアドレス範囲は **network** コマンドで指定されたサブネット内にある必要があります。範囲外のアドレスを割り当てることはできません。

例

アドレスプール 1 の 192.168.8.1～192.168.8.150 のアドレス範囲を指定します。

<Switch> system-view

[Switch] dhcp server ip-pool 1

[Switch-dhcp-pool-1] address range 192.168.8.1 192.168.8.150

関連コマンド

- **display dhcp server pool**
- **network**

7.1.2 bims-server

Syntax

bims-server ip *ip-address* [**port** *port-number*] **sharekey** { **cipher** | **simple** } *string*

undo bims-server

デフォルト

設定なし

View

DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

ip *ip-address*: BIMS サーバの IP アドレスを指定します。

port *port-number*: BIMS サーバのポート番号を指定します。設定範囲は 1～65534 です。
cipher: 暗号テキストキーを設定します。

simple: プレーンテキストキーを設定します。

string: キーの文字列を設定します。大文字小文字を区別します。**simple** を指定した場合、プレーンテキストで 1～16 の文字列でなくてはなりません。**cipher** を設定した場合、1～53 文字の暗号テキストでなければなりません。BIMS サーバに送られたパケットを暗号化するために DHCP クライアントは共有キーを使用します。

説明

bims-server コマンドは、DHCP アドレスプールの BIMS サーバの IP アドレス、ポート番号、共有キーを指定します。

undo bims-server コマンドは、指定された BIMS サーバ情報を削除します。

コマンドを複数回、設定した場合、最後に行った設定が適用されます。

セキュリティ目的のため、プレーンで設定されたパスワードも含め、すべてのパスワードは暗号文で保存されます。

例

BIMS サーバの IP アドレス 1.1.1.1、ポート番号 80、共有キーaabbcc アドレスプール 0 に指定します。

<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

関連コマンド

display dhcp server pool

7.1.3 bootfile-name

Syntax

bootfile-name *bootfile-name*

undo bootfile-name

デフォルト

設定なし

View

DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

bootfile-name: コンフィグレーションファイル名を指定します。設定範囲は 1～63 文字です。大文字、小文字を区別します。

説明

bootfile-name コマンドはコンフィグレーションファイル名を指定します。

undo bootfile-name コマンドはコンフィグレーションファイル名を削除します。

コマンドを複数回設定した場合、最後に行った設定が適用されます。

コンフィグレーションファイルが TFTP サーバにある場合、TFTP サーバのコンフィグレーションファイル名を指定します。

例

DHCP アドレスプール 0 のブートファイル名 boot.cfg を指定します。

<Switch> system-view

[Switch] dhcp server ip-pool 0

[Switch-dhcp-pool-0] bootfile-name boot.cfg

関連コマンド

- **display dhcp server pool**
- **next-server**
- **tftp-server domain-name**
- **tftp-server ip-address**

7.1.4 class option-group

Syntax

class *class-name* **option-group** *option-group-number*

undo class *class-name* **option-group**

デフォルト

設定なし

View

DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

class-name: DHCP ユーザクラスの名前を指定します。設定範囲は 1～63 文字で、大文字と小文字は区別しません。

option-group-number: DHCP オプショングループに 1 から 32768 までの番号を割り当てます。

説明

class option-group コマンドは DHCP ユーザクラスの DHCP オプショングループを指定します。

undo class option-group コマンドは DHCP ユーザクラスの DHCP オプショングループ設定を削除します。

DHCP-DISCOVER メッセージを受信すると、サーバはこのコマンドで指定された順序で DHCP クライアントと DHCP ユーザクラスを比較します。一致する DHCP ユーザクラスが見つかった場合、サーバはクライアントにオプショングループの DHCP オプションを割り当てます。複数の DHCP ユーザクラスと一致した場合、サーバは次のようにオプショングループを選択します。

·オプショングループに共通のオプションがある場合、サーバは最初に一致したユーザクラスに指定されたオプショングループを選択します。

·オプショングループのオプションが異なる場合、サーバは一致するオプショングループをすべて選択します。

DHCP アドレスプール内の DHCP ユーザクラスに指定できるオプショングループは 1 つだけです。ユーザクラスに対してこのコマンドを複数回実行すると、最新の設定が有効になります。

例

DHCP アドレスプール 0 の DHCP ユーザクラス user に、DHCP オプショングループ 1 を指定します。

```
<Switch> system-view
[Switch] dhcp server ip-pool 0
[Switch-dhcp-pool-0] class user option-group 1
```

関連コマンド

dhcp option-group

7.1.5 dhcp class

Syntax

dhcp class *class-name*

undo dhcp class *class-name*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

class-name: DHCP ユーザクラスの名前を指定します。設定範囲は 1～63 文字で、大文字と小文字は区別しません。

説明

dhcp class コマンドは DHCP ユーザクラスを作成し、その view に移行します。

undo dhcp class コマンドは指定した DHCP ユーザクラスを削除します。

またコマンドを使用して既存の DHCP ユーザクラス View に移行することができます。

DHCP ユーザクラス View では、if-match コマンドを使用して、DHCP クライアントを DHCP ユーザクラスに紐付ける一致ルールを設定できます。

例

DHCP ユーザクラス test を作成し、その View に移行します。

<Switch> system-view

[Switch] dhcp class test

[Switch-dhcp-class-test]

関連コマンド

- **class option-group**
- **if-match**

7.1.6 dhcp option group

Syntax

dhcp option-group *option-group-number*

undo dhcp option-group *option-group-number*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

option-group-number: DHCP オプショングループに 1 から 32768 までの番号を割り当てます。

説明

dhcp option group コマンドは DHCP オプショングループを作成し、その view に移行します。

undo dhcp option group コマンドは指定した DHCP オプショングループを削除します。

またコマンドを使用して既存の DHCP オプショングループ View に移行することができます。

例

DHCP オプショングループ 1 を作成し、その View に移行します。

<Switch> system-view

[Switch] dhcp option-group 1

[Switch-dhcp-option-group-1]

関連コマンド

- **class option-group**
- **option**

7.1.7 dhcp server apply ip-pool

Syntax

dhcp server apply ip-pool *pool-name*

undo dhcp server apply ip-pool

デフォルト

設定なし

View

Interface view

定義済みユーザロール

network-admin

パラメータ

pool-name: DHCP アドレスプールの名前を指定します。設定範囲は 1～63 文字です。大文字、小文字を区別します。

説明

dhcp server apply ip-pool コマンドはインタフェースにアドレスプールを適用します。

undo dhcp server apply ip-pool コマンドは設定を削除します。

インタフェースから DHCP 要求を受信すると、DHCP サーバはすべてのアドレスプールからクライアントのスタティックの割り当てを検索します。スタティックの割り当てがない場合、サーバはインタフェースに適用されたアドレスプールから設定パラメータをクライアントに割り当てます。アドレスプールに割り当て可能な IP アドレスがない、あるいはアドレスプールが存在しない場合、DHCP クライアントは IP アドレスを取得することができません。

コマンドを複数回設定した場合、最後に行った設定が適用されます。

例

VLAN インタフェース 2 に DHCP アドレスプール 0 を適用します。

<Switch> system-view

[Switch] interface vlan-interface 2

[Switch-Vlan-interface2] dhcp server apply ip-pool 0

関連コマンド

dhcp server ip-pool

7.1.8 dhcp server forbidden-ip

Syntax

dhcp server forbidden-ip *start-ip-address* [*end-ip-address*]

undo dhcp server forbidden-ip *start-ip-address* [*end-ip-address*]

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

start-ip-address: 開始 IP アドレスを指定します。

end-ip-address: 終了 IP アドレスを指定します。*end-ip-address* は *start-ip-address* より小さい値にすることができません。指定されない場合、*start-ip-address* のみがダイナミック割り当てから除外されます。

説明

dhcp server forbidden-ip コマンドはダイナミック割り当てから指定した IP アドレスを除外します。

undo dhcp server forbidden-ip コマンドは設定を削除します。

ゲートウェイと FTP サーバのような装置の IP アドレスはクライアントに割り当てることができません。このコマンドはダイナミック割り当てからそのようなアドレスを除外します。

除外された IP アドレスがスタティックの割り当てにある場合、クライアントに割り当てることができます。

undo dhcp server forbidden-ip コマンドでアドレスあるいはアドレス範囲を削除する場合、**dhcp server forbidden-ip** コマンドで指定したアドレスあるいはアドレス範囲と同一にしてください。

アドレス範囲の一部の IP アドレスを削除する場合、アドレス範囲全体を削除する必要があります。

ダイナミック割り当てから複数の IP アドレス範囲を除外することができます。

例

ダイナミック割り当てから IP アドレス 10.110.1.1～10.110.1.63 を除外します。

<Switch> system-view

[Switch] dhcp server forbidden-ip 10.110.1.1 10.110.1.63

関連コマンド

- **forbidden-ip**
- **static-bind**

7.1.9 dhcp server ip-pool

Syntax

dhcp server ip-pool *pool-name*

undo dhcp server ip-pool *pool-name*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

pool-name: アドレスプールを固有に識別するため DHCP アドレスプールの名前を指定します。設定範囲は 1～63 文字です。大文字、小文字を区別しません。

説明

dhcp server ip-pool コマンドは DHCP アドレスプールを作成し、その view に移行します。

undo dhcp server ip-pool コマンドは指定した DHCP アドレスプールを削除します。

またコマンドを使用して既存の DHCP アドレスプールに移行することができます。

DHCP アドレスプールは DHCP クライアントに割り当てられる設定パラメータを記録するために使用されます。

例

DHCP アドレスプール pool1 を作成します。

<Switch> system-view

[Switch] dhcp server ip-pool pool1

[Switch-dhcp-pool-pool1]

関連コマンド

- **dhcp server apply ip-pool**
- **display dhcp server pool**

7.1.10 dhcp server ping packets

Syntax

dhcp server ping packets *number*

undo dhcp server ping packets

デフォルト

1

View

System view

定義済みユーザロール

network-admin

パラメータ

number: ping パケットの最大数を指定します。設定範囲は 0～10 です。0 は DHCP サーバがアドレス競合の検出を行わないことを示します。

説明

dhcp server ping packets コマンドは ping パケットの最大数を指定します。

undo dhcp server ping packets コマンドはデフォルトに戻します。

IP アドレスの競合を防ぐため、DHCP サーバは DHCP クライアントに IP アドレスを割り当てる前に IP アドレス宛に ping を実行します。

ping が成功した場合、サーバは IP アドレスが競合していると認識し、新しい IP アドレスを選択します。すべての ping が失敗すると、サーバは DHCP クライアントに IP アドレスを割り当てます。

例

ping パケットの最大数を 10 に指定します。

<Switch> system-view

[Switch] dhcp server ping packets 10

関連コマンド

- **dhcp server ping timeout**
- **display dhcp server conflict**
- **reset dhcp server conflict**

7.1.11 dhcp server ping timeout

Syntax

dhcp server ping timeout *milliseconds*

undo dhcp server ping timeout

デフォルト

500 ミリ秒

View

System view

定義済みユーザロール

network-admin

パラメータ

milliseconds: ping 応答に対するタイムアウト時間を指定します。設定範囲は 0～10000 ミリ秒です。アドレス競合の検出を無効にする場合、0 を指定します。

説明

dhcp server ping timeout コマンドは DHCP サーバで ping 応答に対するタイムアウト時間を設定します。

undo dhcp server ping timeout コマンドはデフォルトに戻します。

IP アドレスの競合を防ぐため、DHCP サーバは DHCP クライアントに IP アドレスを割り当てる前に IP アドレス宛に ping を実行します。

ping が成功した場合、サーバは IP アドレスが競合していると認識し、新しい IP アドレスを選択します。すべての ping が失敗すると、サーバは DHCP クライアントに IP アドレスを割り当てます。

例

ping 応答に対するタイムアウト時間を 1000 ミリ秒に設定します。

<Switch> system-view

[Switch] dhcp server ping timeout 1000

関連コマンド

- **dhcp server ping packets**
- **display dhcp server conflict**
- **reset dhcp server conflict**

7.1.12 dhcp server relay information enable

Syntax

dhcp server relay information enable

undo dhcp server relay information enable

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

dhcp server relay information enable コマンドは DHCP サーバのオプション 82 を有効にします。

undo dhcp server relay information enable コマンドは DHCP サーバのオプション 82 を無効にします。

DHCP サーバがオプション 82 を処理するように設定されている場合、オプション 82 のメッセージを受信すると、DHCP サーバはオプション 82 を DHCP 応答メッセージに追加します。DHCP サーバがオプション 82 を無効するように設定されている場合、DHCP 応答メッセージにオプション 82 を追加しません。

例

DHCP サーバのオプション 82 を無効にします。

<Switch> system-view

[Switch] undo dhcp server relay information enable

7.1.13 display dhcp server conflict

Syntax

display dhcp server conflict [**ip** *ip-address*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ip *ip-address*: 指定した IP アドレスの競合情報を表示します。指定しない場合、すべての IP アドレスの競合情報を表示します。

説明

display dhcp server conflict コマンドは IP アドレス競合の情報を表示します。

DHCP サーバは以下の状況で IP アドレス競合の情報を作成します。

- DHCP クライアントに IP アドレスを割り当てる前、DHCP サーバは ping を行い、が他のホストで IP アドレスを使用しているかどうかを検出します。
- DHCP クライアントは IP アドレス競合をサーバに通知するため、DHCP サーバに DECLINE パケットを送信します。

- DHCP サーバはアドレスプールの割り当て可能なアドレスが自身の IP アドレスであることを検出します。

例

すべての IP アドレスの競合情報を表示します。

<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
```

表 7-1 コマンド出力

フィールド	説明
IP address	競合したIPアドレスです。
Detect time	競合が検出された時間です。

関連コマンド

reset dhcp server conflict

7.1.14 display dhcp server expired

Syntax

display dhcp server expired [**ip** *ip-address* | **pool** *pool-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ip *ip-address*: 指定した IP アドレスのリース期限の終了に関する情報を表示します。指定しない場合、すべての IP アドレスのリース期限の終了に関する情報を表示します。

pool *pool-name*: 指定したアドレスプールのリース期限の終了に関する情報を表示します。設定範囲は 1～63 です。大文字、小文字を区別しません。指定しない場合、すべてのアドレスプールのリース期限の終了に関する情報を表示します。

説明

display dhcp server expired コマンドはリース期限の終了に関する情報を表示します。

有効なアドレスがすべて割り当てられてとき、DHCP サーバは DHCP クライアントにリース期限が終了した IP アドレスを割り当てます。

例

すべてのリース期限の終了に関する情報を表示します。

<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
```

表 7-2 コマンド出力

フィールド	説明
IP address	リース期限が終了するIPアドレスです。
Client-identifier/Hardware address	クライアントIDあるいはMACアドレスです。
Lease expiration	リース期限が終了する時間です。

関連コマンド

reset dhcp server expired

7.1.15 display dhcp server free-ip

Syntax

display dhcp server free-ip [**pool** *pool-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

pool *pool-name*: 指定したアドレスプールの割り当て可能な IP アドレスを表示します。設定範囲は 1～63 文字です。大文字、小文字を区別しません。指定しない場合、すべてのアドレスプールの割り当て可能なすべての IP アドレスを表示します。

説明

display dhcp server free-ip コマンドは割り当て可能な IP アドレスを表示します。

例

すべてのアドレスプールの割り当て可能な IP アドレスを表示します。

<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
```

表 7-3 コマンド出力

フィールド	説明
Pool name	アドレスプールの名前です。
Network	割り当て可能なネットワークです。
IP ranges	割り当て可能なIPアドレス範囲です。
Secondary networks	割り当て可能なセカンダリネットワークです。

関連コマンド

- **address range**
- **dhcp server ip-pool**
- **network**

7.1.16 display dhcp server ip-in-use

Syntax

display dhcp server ip-in-use [**ip** *ip-address* | **pool** *pool-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ip *ip-address*: 指定した IP アドレスの割り当て情報を表示します。指定しない場合、すべての割り当てられた IP アドレスの情報を表示します。

pool *pool-name*: 指定した IP アドレスプールの割り当て情報を表示します。設定範囲は 1～63 です。大文字、小文字を区別しません。指定しない場合、すべての割り当てられた IP アドレスプールの IP アドレスの情報を表示します。

説明

display dhcp server ip-in-use コマンドは割り当てられた IP アドレスの情報を表示します。

クライアントの割り当て情報は、DHCP サーバに DHCP クライアントのゲートウェイが設定されているときのみ、IP ソースガードのような他のセキュリティモジュールで使用することができます。

リース期限が 2100 年を超過する場合、リース期限は After 2100 と表示されます。

例

すべての割り当てられた DHCP アドレスの情報を表示します。

<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)
```

表 7-4 コマンド出力

フィールド	説明
IP address	割り当てられたIPアドレスです。
Client identifier/Hardware address	クライアントIDあるいはハードウェアアドレスです。
Lease expiration	リース期間です。 • **Exact time (May 1 14:02:49 2015)**—リース期間が終了する時間です。 • **Not used**—スタティック割り当てのIPアドレスがクライアントに割り当てられていません。 • **Unlimited**—期限なしのリースです。 • **After 2100**—リース期間の終了が2100年以降です。
Type	割り当てタイプです。 • **Static(F)**— IPアドレスが割り当てられていない空きのスタティック割り当てです。 • **Static(O)**—IPアドレスが選択され、提供されたスタティック割り当てです。DHCPサーバによってDHCP-OFFERパケットにIPアドレスが記載されDHCPクライアントに送信されます。 • **Static(C)**—IPアドレスがDHCPクライアントに割り当てられ、コミットされたスタティック割り当てです。 • **Auto(O)**—IPアドレスが選択され、一時的に提供されたダイナミック割り当てです。DHCPサーバによってDHCP-OFFERパケットにIPアドレスが記載されDHCPクライアントに送信されます。 • **Auto(C)**— IPアドレスがDHCPクライアントに割り当てられ、コミットされたダイナミック割り当てです。

関連コマンド

reset dhcp server ip-in-use

7.1.17 display dhcp server pool

Syntax

display dhcp server pool [*pool-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

pool-name: 指定したアドレスプールの情報を表示します。設定範囲は 1～63 文字です。大文字、小文字を区別しません。指定しない場合、すべてのアドレスプールの情報を表示します。

説明

display dhcp server pool コマンドは DHCP アドレスプールの情報を表示します。

例

すべての DHCP アドレスプールの情報を表示します。

<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 20.1.1.0 mask 255.255.255.0
  secondary networks:
    20.1.2.0 mask 255.255.255.0
    20.1.3.0 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 1.1.1.1 2.2.2.2 4.4.4.4
  nbns-list 5.5.5.5 6.6.6.6 7.7.7.7
  netbios-type m-node
  option 2 ip-address 1.1.1.1
  expired 1 0 0 0

Pool name: 2
  Network 20.1.1.0 mask 255.255.255.0
```

```
  address range 20.1.1.1 to 20.1.1.15
  class departmentA range 20.1.1.20 to 20.1.1.29
  class departmentB range 20.1.1.30 to 20.1.1.40
  next-server 20.1.1.33
  tftp-server domain-name www.dian.org.cn
  tftp-server ip-address 192.168.0.120
  voice-config ncp-ip 10.1.1.2
  voice-config as-ip 10.1.1.5
  voice-config voice-vlan 3 enable
  voice-config fail-over 10.1.1.1 123*
  option 2 ip-address 1.1.1.3
  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
```

表 7-5 コマンド出力

フィールド	説明
Pool name	アドレスプールの名前です。
Network	割り当て可能なネットワークです。
secondary networks	割り当て可能なセカンダリネットワークです。
address range	割り当て可能なアドレス範囲です。
class *class-name* range	DHCPユーザクラスとアドレス範囲です。
static bindings	スタティックIP-MAC/クライアントIDバインディングです。
option	カスタマイズされたDHCPオプションです。
expired	リース期限です。この例の1 2 3 4は1日2時間3分4秒を示します。
bootfile-name	ブートファイル名です。
dns-list	DNSサーバのIPアドレスです。
domain-name	ドメイン名サフィックスです。

フィールド	説明
bims-server	BIMSサーバの情報です。
forbidden-ip	ダイナミックの割り当てから除外されたIPアドレスです。
gateway-list	ゲートウェイアドレスです。
nbns-list	WINSサーバのアドレスです。
netbios-type	NetBIOSノードタイプです。
next-server	次のサーバのIPアドレスです。
tftp-server domain-name	TFTPサーバ名です。
tftp-server ip-address	TFTPサーバのアドレスです。
voice-config ncp-ip	プライマリのネットワークコーリングプロセッサのアドレスです。
voice-config as-ip	バックアップのネットワークコーリングプロセッサのアドレスです。
voice-config voice-vlan	Voice VLANです。
voice-config fail-over	フェイルオーバルートです。

7.1.18 display dhcp server statistics

Syntax

display dhcp server statistics [**pool** *pool-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

pool *pool-name*: アドレスプールを指定します。設定範囲は 1～63 文字です。大文字、小文字を区別しません。指定しない場合、すべてのアドレスプールの情報を表示します。

説明

display dhcp server statistics コマンドは DHCP サーバの統計情報を表示します。

例

DHCP サーバの統計情報を表示します。

<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
```

表 7-6 コマンド出力

フィールド	説明
Pool number	アドレスプールの総数です。このフィールドは指定したアドレスプールの統計情報を表示する場合、表示されません。
Pool utilization	プール使用率です。 ● すべてのアドレスプールの統計情報を表示する場合、すべてのアドレスプールの使用率を表示します。 ● アドレスプールの統計情報を表示する場合、指定したアドレスプールの使用率を表示します。
Bindings	以下のタイプの割り当てです。 ● **Automatic**—ダイナミック割り当て数です。 ● **Manual**—スタティック割り当て数です。 ● **Expired**—除外された割り当て数です。

フィールド	説明
Conflict	競合アドレスの総数です。このフィールドは指定したアドレスプールの統計情報を表示する場合、表示されません。
Messages received	クライアントから受信されたDHCPパケットです。 ● DHCPDISCOVER ● DHCPREQUEST ● DHCPDECLINE ● DHCPRELEASE ● DHCPINFORM ● BOOTPREQUEST このフィールドは指定したアドレスプールの統計情報を表示する場合、表示されません。
Messages sent	クライアントに送信されたDHCPパケットです。 ● DHCPOFFER ● DHCPACK ● DHCPNAK ● BOOTPREPLY このフィールドは指定したアドレスプールの統計情報を表示する場合、表示されません。
Bad Messages	BADメッセージ数です。 このフィールドは指定したアドレスプールの統計情報を表示する場合、表示されません。

関連コマンド

reset dhcp server statistics

7.1.19 dns-list

Syntax

dns-list *ip-address*&<1-8>

undo dns-list [*ip-address*&<1-8>]

デフォルト

設定なし

View

DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

ip-address&<1-8>: DNS サーバを指定します。&<1-8>は DNS サーバのアドレスを半角スペースで区切り最大 8 つまで指定できることを示します。

説明

dns-list コマンドは DHCP アドレスプールの DNS サーバアドレスを指定します。

undo dns-list コマンドは DHCP アドレスプールの DNS サーバアドレスを削除します。

コマンドを複数回設定した場合、最後に行った設定が適用されます。

パラメータを指定しない場合、**undo dns-list** コマンドは DHCP アドレスプールのすべての DNS サーバのアドレスを削除します。

例

DHCP アドレスプール 0 の DNS サーバアドレス 10.1.1.254 を指定します。

<Switch> system-view

[Switch] dhcp server ip-pool 0

[Switch-dhcp-pool-0] dns-list 10.1.1.254

関連コマンド

display dhcp server pool

7.1.20 domain-name

Syntax

domain-name *domain-name*

undo domain-name

デフォルト

設定なし

View

DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

domain-name: ドメイン名を指定します。設定範囲は 1～50 です。大文字、小文字を区別します。

説明

domain-name コマンドは DHCP アドレスプールのドメイン名を指定します。

undo domain-name コマンドは DHCP アドレスプールのドメイン名を削除します。

コマンドを複数回設定した場合、最後に行った設定が適用されます。

例

DHCP アドレスプール 0 のドメイン名 company.com を指定します。

<Switch> system-view

[Switch] dhcp server ip-pool 0

[Switch-dhcp-pool-0] domain-name company.com

関連コマンド

display dhcp server pool

7.1.21 expired

Syntax

expired { **day** *day* [**hour** *hour* [**minute** *minute* [**second** *second*]]] | **unlimited** }

undo expired

デフォルト

1 日

View

DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

day *day*: 日数を指定します。設定範囲は 0～365 日です。

hour *hour*: 時間を指定します。設定範囲は 0～23 時間です。デフォルトは 0 時間です。

minute *minute*: 分を指定します。設定範囲は 0～59 分です。デフォルトは 0 分です。

second *second*: 秒を指定します。設定範囲は 0～59 秒です。デフォルトは 0 秒です。

unlimited: リース期間を指定しません。正確には 136 年のリース期間です。

説明

expired コマンドは DHCP アドレスプールのリース期間を指定します。

undo expired コマンドは DHCP アドレスプールのリース期間をデフォルトに戻します。

DHCP サーバは DHCP クライアントにリース期間と共に IP アドレスを割り当てます。リース期間が終了する前に、DHCP クライアントはリース期間を延長する必要があります。

- リース期間の延長が成功した場合、DHCP クライアントは IP アドレスを使用し続けることができます。
- リース期間の延長が失敗したとき、以下のイベントの両方が発生します。
  - □ リース期間が終了した後 DHCP クライアントは IP アドレスを使用することができません。
  - □ DHCP サーバは終了したアドレスとして IP アドレスにラベルをつけます。

例

DHCP アドレスプール 0 のリース期間を 1 日、2 時間、3 分、4 秒に指定します。

<Switch> system-view

[Switch] dhcp server ip-pool 0

[Switch-dhcp-pool-0] expired day 1 hour 2 minute 3 second 4

関連コマンド

- **display dhcp server expired**
- **display dhcp server pool**
- **reset dhcp server expired**

7.1.22 forbidden-ip

Syntax

forbidden-ip *ip-address*&<1-8>

undo forbidden-ip [*ip-address*&<1-8>]

デフォルト

設定なし

View

DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

ip-address&<1-8>: 除外する IP アドレスを指定します。&<1-8>は IP アドレスを半角スペースで区切り最大 8 つまで指定できることを示します。

説明

forbidden-ip コマンドはアドレスプールのダイナミック割り当てから IP アドレスを除外します。

undo forbidden-ip コマンドは設定を削除します。

アドレスプールの除外された IP アドレスは他のアドレスプールで割り当て可能です。

アドレスプールで最大 4096 の IP アドレスを除外することができます。

パラメータを指定しない場合、**undo forbidden-ip** コマンドはすべての除外した IP アドレスを削除します。

例

DHCP アドレスプール 0 のダイナミック割り当てから 192.168.1.3 と 192.168.1.10 を除外します。

<Switch> system-view

[Switch] dhcp server ip-pool 0

[Switch-dhcp-pool-0] forbidden-ip 192.168.1.3 192.168.1.10

関連コマンド

- **dhcp server forbidden-ip**
- **display dhcp server pool**

7.1.23 gateway-list

Syntax

gateway-list *ip-address*&<1-64>

undo gateway-list [*ip-address*&<1-64>]

デフォルト

設定なし

View

DHCP address pool view

DHCP secondary subnet view

定義済みユーザロール

network-admin

パラメータ

ip-address&<1-64>: ゲートウェイを指定します。&<1-64>はゲートウェイアドレスを半角スペースで区切り最大 64 つまで指定できることを示します。ゲートウェイアドレスは割り当て可能な IP アドレスと同一のサブネットに存在する必要があります。

説明

gateway-list コマンドは DHCP アドレスプールあるいは DHCP セカンダリサブネットのゲートウェイアドレスを指定します。

undo gateway-list コマンドは DHCP アドレスプールあるいは DHCP セカンダリサブネットからゲートウェイアドレスを削除します。

DHCP サーバは以下の方法でセカンダリサブネットのクライアントにゲートウェイアドレスを割り当てます。

- address pool view と secondary subnet view の両方でゲートウェイを指定する場合、DHCP は secondary subnet view のゲートウェイアドレスをセカンダリサブネットのクライアントに割り当てます。
- address pool view でゲートウェイを指定し、secondary subnet view でゲートウェイを指定しない場合、DHCP は address pool view のゲートウェイアドレスをセカンダリサブネットのクライアントに割り当てます。

パラメータを指定しない場合、**undo gateway-list** コマンドはすべてのゲートウェイアドレスを削除します。

例

DHCP アドレスプール 0 のゲートウェイアドレス 10.1.1.1 を指定します。

<Switch> system-view

[Switch] dhcp server ip-pool 0

[Switch-dhcp-pool-0] gateway-list 10.1.1.1

関連コマンド

display dhcp server pool

7.1.24 if-match

Syntax

if-match rule *rule-number* **{ hardware-address** *hardware-address* **mask** *hardware-address-mask* **| option** *option-code* **[ascii** *ascii-string* **[offset** *offset* **| partial] | hex** *hex-string* **[mask** *mask* **| offset** *offset* **length** *length* **| partial]] | relay-agent** *gateway-address* **}**

undo if-match rule *rule-number*

デフォルト

設定なし

View

DHCP user class view

定義済みユーザロール

network-admin

パラメータ

rule *rule-number*: ルールに割り当てる ID を指定します。値の範囲は 1～128 までで、ID が小さいほど、一致の優先度が高くなります。

hardware-address *hardware-address*: ハードウェアアドレスをハイフンで区切られた 16 進数の文字列で指定します。値の範囲は 4～39 文字です。最後の 16 進数は 2 桁または 4 桁で、その他の 16 進数は 4 桁である必要があります。たとえば、aabb-ccdd-ee は有効で、aabb-c-dddd または aabb-cc-dddd は無効です。

mask *hardware-address-mask*: *hardware-address* と AND 演算するマスクを指定します。マスクの長さはハードウェアアドレスと同じである必要があります。

option *option-code*: DHCP オプションの番号を指定します。1～254 の数値で指定します。

ascii *ascii-string*: ASCII 文字列を指定します。1～128 文字の文字列で指定します。

offset *offset*: 一致操作が開始されるまでのオフセットをバイト単位で指定します。値の範囲は 0～254 です。オフセット値を指定しない場合は、オプション内容の先頭バイトから照合が開始されます。ASCII 文字列を指定した場合、オフセット後のオプションの内容が ASCII 文字列と同じであれば、パケットはルールに一致します。16 進数を指定した場合、オフセット後の指定した長さのオプション内容が 16 進数と同じであれば、パケットはルールに一致します。

partial: 部分一致を有効にします。パケット内の指定されたオプションに、ルールで指定された ASCII 文字列または 16 進数が含まれている場合、パケットはルールに一致します。たとえば、ルールで abc を指定した場合、オプションの内容 xabc、xyzabca、xabcyz、および abcxyz はすべてルールに一致します。

hex *hex-string*: 16 進数の文字列を指定します。16 進数の文字列の長さは 2～256 までの偶数である必要があります。

mask *mask*: 一致操作の 16 進数マスクを指定します。マスク長は 2～256 までの偶数で、*hex-string* の文字列長と同じである必要があります。DHCP サーバは、マスク長のオプション内容を先頭から選択し、選択したオプション内容と指定した 16 進数をマスクと AND 演算します。2 つの AND 演算結果が同じ場合、パケットはルールと一致します。

length *length*: 照合するオプション内容の長さをバイト単位で指定します。値の範囲は 1～128 です。長さは、16 進文字列の長さと同じである必要があります。

relay-agent *gateway-address*: giaddr フィールドの値を指定します。値はドット付き 10 進表記の IPv4 アドレスです。パケットの giaddr フィールド値がルールの値と同じ場合、パケットはルールに一致します。

説明

if-match コマンドは DHCP ユーザクラスの一致ルールを設定します。

undo if-match コマンドは DHCP ユーザクラスの一致ルールを削除します。

DHCP クライアントから送信された DHCP-DISCOVER パケットが DHCP ユーザクラスのルールと一致する場合、DHCP クライアントはユーザクラスと一致します。

1 つの DHCP ユーザクラスに対して複数の一致ルールを設定できます。

各一致ルールは、そのタイプ内のルール ID によって一意に識別されます(ハードウェアアドレス、オプション、またはリレーエージェントアドレス)。

- 設定しているルールの ID とタイプが既存のルールと同じ場合、新しいルールによって既存のルールが上書きされます。
- 設定するルールの ID が既存のルールと同じで、タイプが異なる場合は、新しいルールが有効になり、既存のルールと共存します。ベストプラクティスとして、異なるタイプのルールに同じ ID を割り当てないでください。
- 異なる ID のルールが同じルール内容を持つことはできません。

if-match hardware-address ルールを設定する場合は、次の注意事項に従ってください。

- ハードウェアアドレスタイプは、MAC アドレスのみをサポートします。他のタイプのハードウェアアドレスを持つクライアントでは、ルール一致となりません。
- 指定されたハードウェアアドレスは、クライアントハードウェアアドレスと同じ長さである必要があります。MAC アドレスと一致させるには、指定するハードウェアアドレスの長さを 6 バイトにする必要があります。
- ハードウェアアドレスのマスク内の、f と 0 は不連続にすることができます。たとえば、if-match rule 1 hardware-address 0094-0000-1100 mask ffff-0000-ff00 は、最初の 2 バイトが 0094 で、5 バイトが 11 のハードウェアアドレスと一致します。

if-match オプションルールを設定する場合は、次の注意事項に従ってください。

- オプションを含むパケットを照合するには、*option-code* の引数だけを指定します。
- AND 演算で 16 進数を一致させるには、option-code hex-string mask オプションを指定します。
- 16 進数を直接照合するには、オプション *option-code hex-string* [**offset** *offset* **length** *length* [**partial**] オプションを指定します。offset、length、または partial パラメータを指定しない場合、オプションの内容が 16 進数で始まると、パケットはルールに一致します。
- ASCII 文字列と一致させるには、*option-code* **ascii** *ascii-string* [**offset** *offset* [partial] オプションを指定します。offset または partial パラメータを指定しない場合、オプションの内容が ASCII 文字列で始まると、パケットはルールに一致します。

例

DHCP ユーザクラス test を作成し、その View に移行します。

<Switch> system-view

[Switch] dhcp class test

[Switch-dhcp-class-test]

関連コマンド

- **class option-group**

if-match

7.1.25 nbns-list

Syntax

nbns-list *ip-address*&<1-8>

undo nbns-list [*ip-address*&<1-8>]

デフォルト

設定なし

View

DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

ip-address&<1-8>: WINS サーバの IP アドレスを指定します。&<1-8>は WINS サーバアドレスを半角スペースで区切り最大 8 つまで指定できることを示します。

説明

nbns-list コマンドは DHCP アドレスプールの WINS サーバアドレスを指定します。

undo nbns-list コマンドは指定した WINS サーバアドレスを削除します。

コマンドを複数回設定した場合、最後に行った設定が適用されます。

パラメータを指定しない場合、**undo nbns-list** コマンドはすべての WINS サーバアドレスを削除します。

例

DHCP アドレスプール 0 の WINS サーバアドレス 10.1.1.1 を指定します。

<Switch> system-view

[Switch] dhcp server ip-pool 0

[Switch-dhcp-pool-0] nbns-list 10.1.1.1

関連コマンド

- **display dhcp server pool**
- **netbios-type**

7.1.26 netbios-type

Syntax

netbios-type { **b-node** | **h-node** | **m-node** | **p-node** }

undo netbios-type

デフォルト

設定なし

View

DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

b-node: ブロードキャストノードを指定します。b-node クライアントはサーバから名前-IP マッピングを取得するため、ブロードキャストメッセージで宛先名を送信します。

h-node: ハイブリッドノードを指定します。h-node クライアントは WINS サーバに宛先名をユニキャストします。応答を受信しない場合、h-node クライアントはサーバからマッピングを取得するため宛先名をブロードキャストします。

m-node: ミックスノードを指定します。m-node クライアントは宛先名をブロードキャストします。応答を受信しない場合、m-node クライアントはサーバからマッピングを取得するため宛先名をユニキャストします。

p-node: ピアツーピアノードを指定します。p-node クライアントは WINS サーバから WINS サーバを取得するため、ユニキャストメッセージの宛先アドレスを送信します。

説明

netbios-type コマンドは DHCP アドレスプールの NetBIOS ノードタイプを指定します。

undo netbios-type コマンドは指定した NetBIOS ノードタイプを削除します。

コマンドを複数回設定した場合、最後に行った設定が適用されます。

例

DHCP アドレスプール 0 の NetBIOS ノードタイプを p-node に指定します。

<Switch> system-view

[Switch] dhcp server ip-pool 0

[Switch-dhcp-pool-0] netbios-type p-node

関連コマンド

- **display dhcp server pool**
- **nbns-list**

7.1.27 network

Syntax

network *network-address* [*mask-length* | **mask** *mask*] [**secondary**]

undo network *network-address* [*mask-length* | **mask** *mask*] [**secondary**]

デフォルト

設定なし

View

DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

network-address: ダイナミック割り当てのサブネットを指定します。マスク長やマスクが指定されない場合、ナチュラルマスクが使用されます。

mask-length: マスク長を指定します。設定範囲は 1～30 です。

mask *mask*: ドットで区切られた形式でマスクを指定します。

secondary: セカンダリサブネットを指定します。指定しない場合、プライマリサブネットを指定します。プライマリサブネットのアドレスが使い果たされている場合、DHCP サーバはクライアントのためにセカンダリサブネットからアドレスを選択します。

説明

network コマンドは DHCP アドレスプールのダイナミック割り当てのサブネットを指定します。

undo network コマンドは指定されたサブネットを削除します。

セカンダリサブネットを指定し、その view に移行するため、**secondary** を使用することができます。**gateway-list** コマンドを使用して DHCP クライアントのためにセカンダリサブネットのゲートウェイを指定することができます。

DHCP アドレスプールで 1 つのプライマリサブネットのみを指定することができます。コマンドを複数回設定した場合、最後に行った設定が適用されます。

DHCP アドレスプールで最大 32 のセカンダリサブネットを指定することができます。

DHCP アドレスプールのプライマリサブネットとセカンダリサブネットは同一ネットワークアドレス、マスクにすることができません。

アドレスプールで **address range** コマンドあるいは **class** コマンドを使用した場合、同一のアドレスプールのセカンダリサブネットを指定することができません。

ネットワークの設定の変更あるいは削除を行うと現在のアドレスプールから割り当てられたアドレスを削除します。

例

DHCP アドレスプール 0 のプライマリサブネット 192.168.8.0/24 とセカンダリサブネット 192.168.10.0/24 を指定します。

<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]

関連コマンド

- **display dhcp server pool**
- **gateway-list**

7.1.28 next-server

Syntax

next-server *ip-address*

undo next-server

デフォルト

設定なし

View

DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

ip-address: サーバの IP アドレスを指定します。

説明

next-server コマンドは DHCP アドレスプールのサーバの IP アドレスを指定します。

undo next-server コマンドは DHCP アドレスプールからサーバの IP アドレスを削除します。

起動時、DHCP クライアントは IP アドレス、指定されたサーバの IP アドレスを取得します。他のブート情報を取得するため TFTP サーバのような指定されたサーバと連絡をとります。

コマンドを複数回設定した場合、最後に行った設定が適用されます。

例

DHCP アドレスプール 0 のサーバの IP アドレス 10.1.1.254 を指定します。

<Switch> system-view

[Switch] dhcp server ip-pool 0

[Switch-dhcp-pool-0] next-server 10.1.1.254

関連コマンド

display dhcp server pool

7.1.29 option

Syntax

option *code* { **ascii** *ascii-string* | **hex** *hex-string* | **ip-address** *ip-address*&<1-8> }

undo option *code*

デフォルト

設定なし

View

DHCP address pool view

DHCP option group view

定義済みユーザロール

network-admin

パラメータ

code: 自己定義されたオプション数を指定します。設定範囲は 2～254 です。50～54、56、58、59、61、62、82 を除きます。

ascii *ascii-string*: ASCII の文字列を指定します。設定範囲は 1～255 です。

hex *hex-string*: 16 進数の偶数番号を指定します。設定範囲は 2～256 です。

ip-address *ip-address*&<1-8>: 自己定義されたオプションの IP アドレスを指定します。&<1-8>は IP アドレスを半角スペースで区切り最大 8 つまで指定できることを示します。

説明

option コマンドは自己定義された DHCP オプションを設定します。

undo option コマンドは自己定義された DHCP オプションを削除します。

DHCP サーバは ASCII 文字列、16 進数文字列、IP アドレスで自己定義されたオプションを記載し、DHCP 応答の自己定義されたオプションをクライアントに送信します。

以下の目的のためにオプションを定義することができます。

- 新しくリリースされたオプションを追加します。
- オプション 43 のようなベンダ指定のオプションを追加します。
- CLI によって設定できない、専用の設定コマンドのオプションを追加します。たとえば **option** *4* **ip-address** *1.1.1.1* コマンドで DHCP クライアントにタイムサーバアドレス 1.1.1.1 を定義することができます。
- DHCP オプションでは正確な要件を満たすことができない場合、既存の DHCP オプションを拡張します。たとえば、**dns-list** コマンドは 8 つの DNS サーバアドレスを設定することができます。8 つを超える DNS サーバを指定する場合、すべての DNS サーバで **option** *6* コマンドを使用する必要があります。

専用のコマンドと **option** コマンドの両方を使用して DHCP オプションを指定する場合、DHCP サーバは専用のコマンドで指定された内容を割り当てます。たとえば、DHCP サーバのアドレスが **dns-list** コマンドと **option** *6* コマンドで指定された場合、サーバは **dns-list** コマンドで指定されたアドレスを使用します。

DHCP オプショングループで設定された DHCP オプションは DHCP アドレスプールで設定された DHCP オプションより優先されます。

option コマンドで同じコードが指定された場合、最後に行った設定が適用されます。

例

アドレスプール 0 のログサーバアドレス 2.2.2.2 を指定するためオプション 7 を設定します。

<Switch> system-view

[Switch] dhcp server ip-pool 0

[Switch-dhcp-pool-0] option 7 ip-address 2.2.2.2

関連コマンド

display dhcp server pool

7.1.30 reset dhcp server conflict

Syntax

reset dhcp server conflict [**ip** *ip-address*]

View

User view

定義済みユーザロール

network-admin

パラメータ

ip *ip-address*: 指定された IP アドレスの競合に関する情報を削除します。指定しない場合、すべてのアドレスの競合に関する情報を削除します。

説明

reset dhcp server conflict コマンドは IP アドレスの競合に関する情報を削除します。

ダイナミックに割り当てられた IP アドレスが他のホストでスタティックに設定されたとき、アドレスの競合が発生します。アドレスプールの設定を修正した後、競合したアドレスは割り当て可能になります。これらのアドレスを割り当てるため、最初に競合に関する情報を削除するため、**reset dhcp server conflict** コマンドを使用します。

例

すべてのアドレスの競合に関する情報を削除します。

<Switch> reset dhcp server conflict

関連コマンド

display dhcp server conflict

7.1.31 reset dhcp server expired

Syntax

reset dhcp server expired [**ip** *ip-address* | **pool** *pool-name*]

View

User view

定義済みユーザロール

network-admin

パラメータ

ip *ip-address*: 期限が終了した IP アドレスを指定し、IP アドレスに関する割り当て情報を削除します。指定しない場合、すべてのアドレスの競合に関する情報を削除します。

pool *pool-name*: 指定したアドレスプールの期限が終了した IP アドレスの割り当て情報を削除します。設定範囲は 1～63 です。大文字、小文字は区別しません。指定しない場合､すべてのアドレスプールの期限が終了した IP アドレスの割り当て情報を削除します。

説明

reset dhcp server expired コマンドは期限が終了した IP アドレスの割り当て情報を削除します。

例

すべての期限が終了した IP アドレスの割り当て情報を削除します。

<Switch> reset dhcp server expired

関連コマンド

display dhcp server expired

7.1.32 reset dhcp server ip-in-use

Syntax

reset dhcp server ip-in-use [**ip** *ip-address* | **pool** *pool-name*]

View

User view

定義済みユーザロール

network-admin

パラメータ

ip *ip-address*: 指定した IP アドレスの割り当て情報を削除します。指定しない場合、すべての IP アドレスの割り当て情報を削除します。

pool *pool-name*: 指定したアドレスプールの割り当て情報を削除します。設定範囲は 1～63 です。大文字、小文字を区別しません。指定しない場合、すべてのアドレスプールの割り当て情報を削除します。

説明

reset dhcp server ip-in-use コマンドは IP アドレスプールの割り当て情報を削除します。

reset dhcp server ip-in-use コマンドで割り当てられたスタティック割り当て情報を削除すると、スタティック割り当て情報は未割り当てのスタティック割り当て情報となります。

例

IP アドレス 10.110.1.1 の割り当て情報を削除します。

<Switch> reset dhcp server ip-in-use ip 10.110.1.1

関連コマンド

display dhcp server ip-in-use

7.1.33 reset dhcp server statistics

Syntax

reset dhcp server statistics

View

User view

定義済みユーザロール

network-admin

説明

reset dhcp server statistics コマンドは DHCP サーバの統計情報を削除します。

例

DHCP サーバの統計情報を削除します。

<Switch> reset dhcp server statistics

関連コマンド

display dhcp server statistics

7.1.34 static-bind

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*

デフォルト

設定なし

View

DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

ip-address *ip-address*: スタティック割り当ての IP アドレスを指定します。マスク長あるいはマスクが指定されない場合、ナチュラルマスクが使用されます。

mask-length: マスク長を指定します。設定範囲は 1～30 です。

mask *mask*: ドットで区切られた形式でマスクを指定します。

client-identifier *client-identifier*: スタティック割り当てのクライアント ID を指定します。設定範囲は 4～254 文字です。形式は H-H-H で、16 進数の数字とハイフン（-）で構成されます。最後の H は 2 桁あるいは 4 桁の 16 進数にすることができますが、それ以外の H は 4 桁の 16 進数の文字にする必要があります。たとえば、aabb-cccc-dd は有効な ID ですが、aabb-c-dddd や aabb-cc-dddd は無効な ID です。

hardware-address *hardware-address*: スタティック割り当てのクライアントのハードウェアアドレスを指定します。設定範囲は 4～39 文字です。形式は H-H-H で、16 進数の数字とハイフン（-）で構成されます。最後の H は 2 桁あるいは 4 桁の 16 進数にすることができますが、それ以外の H は 4 桁の 16 進数の文字にする必要があります。たとえば、aabb-cccc-dd は有効なハードウェアアドレスですが、aabb-c-dddd や aabb-cc-dddd は無効なハードウェアアドレスです。

ethernet: クライアントのハードウェアアドレスのタイプを Ethernet に指定します。デフォルトタイプは Ethernet です。

token-ring: クライアントのハードウェアアドレスのタイプを Token Ring に指定します。

説明

static-bind コマンドはクライアント ID あるいは MAC アドレスを IP アドレスにスタティックに割り当てます。

undo static-bind コマンドはスタティックの割り当てを削除します。

スタティック割り当ての IP アドレスは DHCP サーバのインタフェースのアドレスにすることはできません。そうでなければ、IP アドレスの競合が発生すると、境界のクライアントは IP アドレスを取得することができません。

アドレスプールのスタティック割り当てを複数指定することができます。アドレスプールのスタティック割り当ては最大 8192 です。

スタティックの割り当てを修正することはできません。DHCP クライアントの割り当てを変更する場合、最初に既存の割り当てを削除し、新しい割り当てを作成してください。

例

DHCP アドレスプール 0 の IP アドレス 10.1.1.1/24 をクライアント ID が 00aa-aabb のクライアント ID に割り当てます。

<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

関連コマンド

display dhcp server pool

7.1.35 tftp-server domain-name

Syntax

tftp-server domain-name *domain-name*

undo tftp-server domain-name

デフォルト

設定なし

View

DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

domain-name: TFTP サーバ名を指定します。設定範囲は 1～63 です。大文字、小文字を区別します。

説明

tftp-server domain-name コマンドは DHCP アドレスプールの TFTP サーバ名を指定します。

undo tftp-server domain-name コマンドは DHCP アドレスプールの TFTP サーバ名を削除します。

コマンドを複数回設定した場合、最後に行った設定が適用されます。

例

DHCP アドレスプール 0 の TFTP サーバ aaa を指定します。

<Switch> system-view

[Switch] dhcp server ip-pool 0

[Switch-dhcp-pool-0] tftp-server domain-name aaa

関連コマンド

- **display dhcp server pool**
- **tftp-server ip-address**

7.1.36 tftp-server ip-address

Syntax

tftp-server ip-address *ip-address*

undo tftp-server ip-address

デフォルト

設定なし

View

DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

ip-address: TFTP サーバの IP アドレスを指定します。

説明

tftp-server ip-addressコマンドは DHCP アドレスプールの TFTP サーバアドレスを指定します。

undo tftp-server ip-addressコマンドは DHCP アドレスプールの TFTP サーバアドレスを削除します。

コマンドを複数回設定した場合、最後に行った設定が適用されます。

例

DHCP アドレスプール 0 の TFTP サーバアドレス 10.1.1.1 を指定します。

<Switch> system-view

[Switch] dhcp server ip-pool 0

[Switch-dhcp-pool-0] tftp-server ip-address 10.1.1.1

関連コマンド

- **display dhcp server pool**
- **tftp-server domain-name**

7.1.37 voice-config

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**]

デフォルト

設定なし

View

DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

as-ip *ip-address*: バックアップのネットワークコーリングプロセッサの IP アドレスを指定します。

fail-over *ip-address dialer-string*: フェイルオーバ IP アドレスとダイヤル文字列を指定します。設定範囲は 1～39 です。0～9 の数字、アスタリスク（*）が含まれます。

ncp-ip *ip-address*: プライマリのネットワークコーリングプロセッサの IP アドレスを指定します。

voice-vlan *vlan-id*: voice VLAN ID を指定します。設定範囲は 2～4094 です。

- **disable**: 指定された VLAN を無効にします。DHCP クライアントは VLAN を voice VLAN として適用しません。
- **enable**: 指定された VLAN を有効にします。DHCP クライアントは VLAN を voice VLAN として適用します。

説明

voice-config コマンドは DHCP アドレスプールのオプション 184 の内容を設定します。

undo voice-config コマンドは DHCP アドレスプールのオプション 184 の内容を削除します。

コマンドを複数回設定した場合、最後に行った設定が適用されます。

例

DHCP アドレスプール 0 のオプション 184 を設定します。プライマリのネットワークコーリングプロセッサの IP アドレスを 10.1.1.1、セカンダリのネットワークコーリングプロセッサの IP アドレスを 10.2.2.2 に設定します。voice VLAN 3 が有効です。フェイルオーバ IP アドレスは 10.3.3.3 です。ダイヤル文字列は 99*です。

```
<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*
```

関連コマンド

display dhcp server pool

目次

このセクションのページは **4-x-x** です。

8 章 DHCP リレーエージェント 8-1
8.1 DHCP リレーエージェント設定コマンド 8-1
8.1.1 dhcp relay client-information record 8-1
8.1.2 dhcp relay client-information refresh enable 8-2
8.1.3 dhcp relay information circuit-id 8-3
8.1.4 dhcp relay information enable 8-5
8.1.5 dhcp relay information remote-id 8-6
8.1.6 dhcp relay information strategy 8-7
8.1.7 dhcp relay release ip 8-8
8.1.8 dhcp relay server-address 8-9
8.1.9 dhcp relay source-address 8-10
8.1.10 dhcp smart-relay enable 8-11
8.1.11 display dhcp relay client-information 8-12
8.1.12 display dhcp relay information 8-14
8.1.13 display dhcp relay server-address 8-16
8.1.14 display dhcp relay statistics 8-17
8.1.15 reset dhcp relay client-information 8-18
8.1.16 reset dhcp relay statistics 8-19

8章 DHCP リレーエージェント

8.1 DHCPリレーエージェント設定コマンド

8.1.1 dhcp relay client-information record

Syntax

dhcp relay client-information record

undo dhcp relay client-information record

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

dhcp relay client-information record コマンドはリレーエントリのクライアント情報の記録を有効にします。

undo dhcp relay client-information コマンドはリレーエントリのクライアント情報の記録を無効にします。

DHCP リレーエージェントが DHCP クライアントのゲートウェイで設定されたときのみクライアント情報が記録されます。

リレーエントリはクライアントの IP アドレス、MAC アドレスのようなクライアントの情報が含まれます。

リレーエントリのクライアント情報の記録を無効にすると、記録されたすべてのリレーエントリを削除します。

例

リレーエントリのクライアント情報の記録を有効にします。

<Switch> system-view

[Switch] dhcp relay client-information record

関連コマンド

- **dhcp relay client-information refresh**
- **dhcp relay client-information refresh enable**

8.1.2 dhcp relay client-information refresh enable

Syntax

dhcp relay client-information refresh enable

undo dhcp relay client-information refresh enable

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

dhcp relay client-information refresh enable コマンドは DHCP リレーエージェントでダイナミックリレーエントリの定期的な更新を有効にします。

undo dhcp relay client-information refresh enable コマンドは DHCP リレーエージェントでダイナミックリレーエントリの定期的な更新を無効にします。

DHCP クライアントは DHCP サーバに IP アドレスをリリースするため、DHCP-RELEASE メッセージをユニキャストします。

DHCP リレーエージェントは DHCP サーバにメッセージを送信し、クライアントの IP-MAC アドレスエントリを削除しません。

この機能で、DHCP リレーエージェントは DHCP サーバに DHCP-REQUEST メッセージを定期的に送信するため、クライアントの IP アドレス、リレーインタフェースの MAC アドレスを使用します。

- サーバが DHCP-ACK メッセージを送信する、あるいは時間以内にメッセージを返信しない場合、DHCP リレーエージェントは以下の処理を行います。
  - □ リレーエントリを削除します。
  - □ IP アドレスをリリースするため、DHCP サーバに DHCP-RELEASE メッセージを送信します。
- サーバが DHCP-NAK メッセージを返信する場合、リレーエージェントはエントリを保持します。

この機能が無効である場合、DHCP リレーエージェントは自動でリレーエントリを削除しません。DHCP クライアントが IP アドレスをリリースしたのち、対応するリレーエントリを削除するため、リレーエージェントで **reset dhcp relay client-information** コマンドを使用する必要があります。

例

DHCP リレーエージェントでダイナミックリレーエントリの定期的な更新を無効にします。

<Switch> system-view

[Switch] undo dhcp relay client-information refresh enable

関連コマンド

- **dhcp relay client-information record**
- **reset dhcp relay client-information**

8.1.3 dhcp relay information circuit-id

Syntax

dhcp relay information circuit-id { **string** *circuit-id* | { **normal** | **verbose** [**node-identifier** { **mac** | **sysname** | **user-defined** *node-identifier* }] } [**format** { **ascii** | **hex** }] }

undo dhcp relay information circuit-id

デフォルト

コードモードは normal で、パディング形式は hex です。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

string *circuit-id*: circuit ID サブオプションの内容を指定します。設定範囲は 3～63 です。大文字、小文字を区別します。

normal: コードモードを normal モードに指定します。このパディングの内容は VLAN ID とポート番号から構成されます。

verbose: コードモードを verbose モードに指定します。このパディングの内容はノード識別子、インタフェース情報、VLAN ID が含まれます。デフォルトのノード識別子はアクセスノードの MAC アドレスです。デフォルトのインタフェース情報は Ethernet タイプ（eth で固定です）、シャーシ番号、サブスロット番号、インタフェース番号が含まれます。

node-identifier { **mac** | **sysname** | **user-defined** *node-identifier* }: アクセスノードの識別子を指定します。

- **mac**: ノード識別子として MAC アドレスを使用します。
- **sysname**: ノード識別子として装置名を使用します。装置名は system view の **sysname** コマンドを使用して設定することができます。装置名のパディング形式は指定したパディング形式に関わらず、常に ASCII です。

🕮 **メモ**：

ノード識別子として **sysname** を指定した場合、装置名を設定するときに半角スペースを含むことができません。そうでなければ、DHCP リレーエージェントはオプション 82 の追加あるいは置き換えに失敗します。

- **user-defined** *node-identifier*: ユーザ定義のノード識別子を使用します。設定範囲は 1～50 です。大文字、小文字を区別します。指定された文字列のパディング形式は指定したパディング形式に関われず、常に ASCII になります。

format: circuit ID サブオプションのコードタイプを指定します。

ascii: ASCII コードタイプを指定します。

hex: hex のコードタイプを指定します。

説明

dhcp relay information circuit-id コマンドはオプション 82 の circuit ID サブオプションのパディング内容とパディング形式を設定します。

undo dhcp relay information circuit-id コマンドはデフォルトに戻します。

コマンドを複数回設定した場合、最後に行った設定が適用されます。

ユーザ定義、normal モード、verbose モードのパディング形式はコマンドの設定によって変わります。表 8-1 に異なるモードのパディング形式を示します。

表 8-1 異なるモードのパディング形式

キーワード（モード）	パディング形式が指定されていない場合	パディング形式が ASCII	パディング形式が hex
string *circuit-id*	パディング形式を指定できません。常にASCIIになります。	ー	ー
normal	hexです。	ASCIIです。	hexです。
verbose	VLAN IDはhexです。 ノード識別子、Ethernetタイプ、インタフェース番号はASCIIです。	ASCIIです。	ノード識別子とEthernetタイプはASCIIです。 インタフェース番号とVLAN IDはhexです。

例

circuit ID サブオプションのコードモードが verbose、ノード識別子が装置名、パディング形式が ASCII に指定します。

<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

関連コマンド

- **dhcp relay information enable**
- **dhcp relay information strategy**
- **display dhcp relay information**

8.1.4 dhcp relay information enable

Syntax

dhcp relay information enable

undo dhcp relay information enable

デフォルト

無効

View

Interface view

定義済みユーザロール

network-admin

説明

dhcp relay information enable コマンドはリレーエージェントでオプション 82 のサポートを有効にします。

undo dhcp relay information enable コマンドはオプション 82 のサポートを無効にします。

このコマンドによって DHCP リレーエージェントが DHCP サーバに要求を転送する前に、オプション 82 が含まれない DHCP 要求にオプション 82 を追加します。オプション 82 の内容は **dhcp relay information circuit-id** コマンド、**dhcp relay information remote-id** コマンドによって決まります。DHCP 要求にオプション 82 が含まれる場合、

リレーエージェントは **dhcp relay information strategy** コマンドで設定された方法にしたがって DHCP 要求を処理します。

この機能が無効である場合、リレーエージェントはオプション 82 を含む DHCP 要求とオプション 82 を含まない DHCP 要求を DHCP サーバに転送します。

例

オプション 82 のサポートを有効にします。

<Switch> system-view

[Switch] interface vlan-interface 10

[Switch-Vlan-interface10] dhcp relay information enable

関連コマンド

- **dhcp relay information circuit-id**
- **dhcp relay information remote-id**
- **dhcp relay information strategy**
- **display dhcp relay information**

8.1.5 dhcp relay information remote-id

Syntax

dhcp relay information remote-id { **normal** [**format** { **ascii** | **hex** }] | **string** *remote-id* | **sysname** }

undo dhcp relay information remote-id

デフォルト

コードモードは normal で、パディング形式は hex です。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

normal: コードモードを normal モードに指定します。このパディングの内容は受信インタフェースの MAC アドレスです。

format: remote ID サブオプションのコードタイプを指定します。デフォルトコードタイプは hex です。

ascii: ASCII コードタイプを指定します。

hex: hex のコードタイプを指定します。

string *remote-id*: remote ID サブオプションの内容を指定します。設定範囲は 1～63 です。大文字、小文字を区別します。

sysname: リモート ID サブオプションの内容として装置名を指定します。装置名は **sysname** コマンドを使用して設定することができます。

説明

dhcp relay information remote-id コマンドはオプション 82 の remote ID サブオプションのパディング内容とパディング形式を設定します。

undo dhcp relay information remote-id コマンドはデフォルトに戻します。

指定した文字列（**string**）あるいは装置名（**sysname**）は常に ASCII です。normal モードのパディング形式はコマンドの設定によって変わります。

コマンドを複数回設定した場合、最後に行った設定が適用されます。

例

オプション 82 の remote ID サブオプションのパディング内容を device001 に指定します。

<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

関連コマンド

- **dhcp relay information enable**
- **dhcp relay information strategy**
- **display dhcp relay information**

8.1.6 dhcp relay information strategy

Syntax

dhcp relay information strategy { **drop** | **keep** | **replace** }

undo dhcp relay information strategy

デフォルト

replace

View

Interface view

定義済みユーザロール

network-admin

パラメータ

drop: オプション 82 メッセージが含まれる DHCP メッセージを廃棄します。

keep: オプション 82 を含むメッセージをそのまま転送するよう指定します。

replace: 元のオプション 82 のメッセージを設定されたオプション 82 のメッセージに置き換えします。

説明

dhcp relay information strategy コマンドは DHCP リレーエージェントでオプション 82 が含まれるメッセージの処理方法を設定します。

undo dhcp relay information strategy コマンドはデフォルトに戻します。

このコマンドは DHCP 要求にオプション 82 が含まれるときのみ適用します。

DHCP 要求にオプション 82 が含まれない場合、DHCP リレーエージェントは DHCP サーバに DHCP 要求を転送する前、常に DHCP 要求にオプション 82 を追加します。

replace パラメータを指定した場合、オプション 82 のパディングモード、パディング形式を設定してください。

keep パラメータあるいは **drop** パラメータを指定した場合､オプション 82 のパディングモード、パディング形式を設定する必要はありません。設定しても適用されません。

例

DHCP リレーエージェントでオプション 82 が含まれるメッセージの処理方法を keep に設定します。

<Switch> system-view

[Switch] interface vlan-interface 10

[Switch-Vlan-interface10] dhcp relay information enable

[Switch-Vlan-interface10] dhcp relay information strategy keep

関連コマンド

- **dhcp relay information enable**
- **display dhcp relay information**

8.1.7 dhcp relay release ip

Syntax

dhcp relay release ip *ip-address*

View

System view

定義済みユーザロール

network-admin

パラメータ

ip-address: リリースされる IP アドレスを指定します。

説明

dhcp relay release ip コマンドは指定したクライアントの IP アドレスをリリースします。

このコマンドを実行した後、リレーエージェントは DHCP サーバに DHCP-RELEASE パケットを送信し、IP アドレスのリレーエントリを削除します。パケットを受信するとサーバは、IP アドレスをリリースするため、指定された IP アドレスの割り当て情報を削除します。

例

IP アドレス 1.1.1.1 をリリースします。

<Switch> system-view

[Switch] dhcp relay release ip 1.1.1.1

8.1.8 dhcp relay server-address

Syntax

dhcp relay server-address *ip-address*

undo dhcp relay server-address [*ip-address*]

デフォルト

設定なし

View

Interface view

定義済みユーザロール

network-admin

パラメータ

ip-address: DHCP サーバの IP アドレスを指定します。DHCP リレーエージェントは DHCP クライアントから受信した DHCP パケットを DHCP サーバに転送します。

説明

dhcp relay server-address コマンドは DHCP リレーエージェントの DHCP サーバを指定します。

undo dhcp relay server-address コマンドは DHCP サーバを削除します。

DHCP サーバを指定する IP アドレスは、DHCP リレーエージェントインタフェースの IP アドレスと同一のサブネット上にすることはできません。そうでなければ、DHCP クライアントは IP アドレスの取得に失敗します。

インタフェースで最大 8 つの DHCP サーバを指定することができます。DHCP リレーエージェントはクライアントからのパケットをすべての指定された DHCP サーバに転送します。

IP アドレスを指定しない場合、**undo dhcp relay server-address** コマンドはインタフェースのすべての DHCP サーバを削除します。

例

リレーエージェントの VLAN インタフェース 10 で DHCP サーバ 1.1.1.1 を指定します。

<Switch> system-view

[Switch] interface vlan-interface 10

[Switch-Vlan-interface10] dhcp relay server-address 1.1.1.1

関連コマンド

- **dhcp select relay**
- **display dhcp relay interface**

8.1.9 dhcp relay source-address

Syntax

dhcp relay source-address *{ ip-address* | **interface** *interface-type interface-number }*

undo dhcp relay source-address

デフォルト

DHCP リレーエージェントは、リレーされた DHCP 要求の送信元 IP アドレスとして、DHCP サーバに接続するインタフェースの IP アドレスを使用します。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

ip-address: 送信元 IP アドレスを指定します。

interface *interface-type interface-number*: インタフェースの IP アドレスを送信元 IP アドレスとして使用します。*interface-type interface-numbe*r 引数は、インタフェースタイプとインタフェース番号を指定します。

説明

複数のリレーインタフェースが同じ IP アドレスを共有している場合、またはリレーインタフェースに DHCP サーバへのルートがない場合、このコマンドが必要です。

このコマンドを使用すると DHCP リレー エージェント上の別のインタフェース（通常はループバック インタフェース）の IP アドレスを、DHCP 要求の送信元 IP アドレスとして指定できます。

リレー インタフェースは、DHCP 要求の送信元 IP アドレス フィールドと **giaddr** フィールドに送信元 IP アドレスを挿入します。

複数のリレーインタフェースが同じ IP アドレスを共有している場合は、リレーインタフェースがオプション 82 をサポートするように設定する必要もあります。DHCP 要求を受信すると、リレーインタフェースはオプション 82 のサブオプション 5 にサブネット情報を挿入します。DHCP サーバは、サブオプション 5 に従って IP アドレスを割り当てます。DHCP リレーエージェントは、MAC アドレステーブルで出力インタフェースを検索し、DHCP 応答を転送します。

このコマンドを複数回実行した場合、最新の設定が有効になります。

例

VLAN インタフェース 2 で中継された DHCP 要求の送信元 IP アドレスとして 1.1.1.1 を指定する

<Switch> system-view

[Switch] interface vlan-interface 2

[Switch-Vlan-interface10] dhcp relay source-address 1.1.1.1

関連コマンド

- **dhcp select relay**

8.1.10 dhcp smart-relay enable

Syntax

dhcp smart-relay enable

undo dhcp smart-relay enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

dhcp smart-relay enable コマンドは DHCP スマートリレー機能を有効にします。

undo dhcp smart-relay enable コマンドは DHCP スマートリレー機能を無効にします。

スマートリレー機能を使用すると、DHCP サーバが DHCP-OFFER メッセージに応答しないときに、リレーエージェントはセカンダリ IP アドレスをゲートウェイアドレスとして使用できます。リレーエージェントは、DHCP サーバに要求を転送する前に、最初に **giaddr** フィールドにプライマリ IP アドレスを挿入します。2 回再試行しても DHCP-OFFER が返されない場合、リレーエージェントはセカンダリ IP アドレスに切り替えます。

この機能がない場合、リレーエージェントは常にプライマリ IP アドレスをゲートウェイアドレスとして使用します。

例

DHCP スマートリレー機能を有効にします。

<Switch> system-view

[Switch] dhcp smart-relay enable

関連コマンド

- **dhcp select**
- **gateway-list**

8.1.11 display dhcp relay client-information

Syntax

display dhcp relay client-information [**interface** *interface-type interface-number* | **ip** *ip-address*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: 指定されたインタフェースのリレーエントリを表示します。指定しない場合、リレーエージェントのすべてのインタフェースのリレーエントリを表示します。

ip *ip-address*: 指定された IP アドレスのリレーエントリを表示します。指定しない場合、リレーエージェントのすべての IP アドレスのリレーエントリを表示します。

説明

display dhcp relay client-information コマンドはリレーエージェントのリレーエントリを表示します。

dhcp relay client-information record コマンドが設定されているときのみ、DHCP リレーエージェントはリレーエントリを記録します。

例

リレーエージェントのすべてのリレーエントリを表示します。

<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
```

表 8-2 コマンド出力

フィールド	説明
Total number of client-information items	リレーエントリの総数です。
Total number of dynamic items	ダイナミックリレーエントリの総数です。
Total number of temporary items	一時的なリレーエントリの総数です。
IP address	DHCPクライアントのIPアドレスです。
MAC address	DHCPクライアントのMACアドレスです。

フィールド	説明
Type	リレーエントリタイプです。 • **Dynamic**—リレーエージェントはDHCPサーバからAck応答を受信した際にダイナミックリレーエントリを作成します。 • **Temporary**—リレーエージェントはDHCPクライアントらREQUESTパケットを受信した際に一時的なリレーエントリを作成します。
Interface	DHCPクライアントに接続されたレイヤ3インタフェースです。リレーエージェントにインタフェース情報がない場合、**N/A**と表示されます。
VPN name	DHCPクライアントが所属しているVPNインスタンスの名前です。DHCPクライアントがVPNに所属していない場合、**N/A**と表示されます。 このフィールドは現在のソフトウェアバージョンでサポートしていません。

関連コマンド

- **dhcp relay client-information record**
- **reset dhcp relay client-information**

8.1.12 display dhcp relay information

Syntax

display dhcp relay information [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: 指定したインタフェースのオプション 82 の設定情報を表示します。インタフェースを指定しない場合、すべてのインタフェースのオプション 82 の設定情報を表示します。

説明

display dhcp relay information コマンドは DHCP リレーエージェントのオプション 82 の設定情報を表示します。

例

すべてのインタフェースのオプション 82 の設定情報を表示します。

<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
```

表 8-3 コマンド出力

フィールド	説明
Interface	インタフェース名です。
Status	オプション82の状態です。 ● **Enable**—DHCPリレーエージェントはオプション82のサポートが有効です。 ● **Disable**—DHCPリレーエージェントはオプション82のサポートが無効です。
Strategy	要求メッセージの処理方法です。 **Option 82**、**Drop**、**Keep**、**Replace**が含まれます。
Circuit ID Pattern	circuit IDサブオプションのパディングモードです。**Verbose**、**Normal**、**User Defined**があります。
Remote ID Pattern	remote IDサブオプションのパディングモードです。**Sysname**、**Normal**、**User Defined**があります。

フィールド	説明
Circuit ID format-type	circuit IDサブオプションのパディング形式です。**ASCII**、**Hex**、**Undefined**があります。
Remote ID format-type	remote IDサブオプションのパディング形式です。**ASCII**、**Hex**、**Undefined**があります。
Node identifier	アクセスノード識別子です。
User defined	ユーザ定義サブオプションの内容です。
Circuit ID	circuit IDサブオプションのユーザ定義の内容です。
Remote ID	remote IDサブオプションのユーザ定義の内容です。

8.1.13 display dhcp relay server-address

Syntax

display dhcp relay server-address [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: 指定されたインタフェースの DHCP サーバのアドレスを表示します。指定しない場合、DHCP リレーエージェントで動作するすべてのインタフェースの DHCP サーバのアドレスを表示します。

説明

display dhcp relay server-address コマンドはインタフェースに設定された DHCP サーバのアドレスを表示します。

例

すべてのインタフェースの DHCP サーバのアドレスを表示します。

<Switch> display dhcp relay server-address

```
Interface name              Server IP address
Vlan2                       2.2.2.2
```

表 8-4 コマンド出力

フィールド	説明
Interface name	インタフェース名です。
Server IP address	DHCPサーバのIPアドレスです。

関連コマンド

dhcp relay server-address

8.1.14 display dhcp relay statistics

Syntax

display dhcp relay statistics [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: 指定したインタフェースの DHCP パケットの統計情報を表示します。指定しない場合、DHCP リレーエージェントのすべての DHCP パケットの統計情報を表示します。

説明

display dhcp relay statistics コマンドは DHCP リレーエージェントの DHCP パケットの統計情報を表示します。

例

DHCP リレーエージェントのすべての DHCP パケットの統計情報を表示します。

<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
```

関連コマンド

reset dhcp relay statistics

8.1.15 reset dhcp relay client-information

Syntax

reset dhcp relay client-information [**interface** *interface-type interface-number* | **ip** *ip-address*]

View

User view

定義済みユーザロール

network-admin

パラメータ

interface *interface-type interface-number*: 指定されたインタフェースのリレーエントリを削除します。指定しない場合、すべてのインタフェースのリレーエントリを削除します。

ip *ip-address*: 指定された IP アドレスのリレーエントリを削除します。指定しない場合、すべての IP アドレスのリレーエントリを削除します。

説明

reset dhcp relay client-information コマンドは DHCP リレーエージェントのリレーエントリを削除します。

例

DHCP リレーエージェントのすべてのリレーエントリを削除します。

<Switch> reset dhcp relay client-information

関連コマンド

display dhcp relay client-information

8.1.16 reset dhcp relay statistics

Syntax

reset dhcp relay statistics [**interface** *interface-type interface-number*]

View

User view

定義済みユーザロール

network-admin

パラメータ

interface *interface-type interface-number*: 指定されたインタフェースの DHCP リレーエージェントの統計情報を削除します。指定しない場合、すべての DHCP リレーエージェントの統計情報を削除します。

説明

reset dhcp relay statistics コマンドは DHCP リレーエージェントの統計情報を削除します。

例

すべての DHCP リレーエージェントの統計情報を削除します。

<Switch> reset dhcp relay statistics

関連コマンド

display dhcp relay statistics

目次

このセクションのページは **4-x-x** です。

9 章 DHCP クライアント 9-1
9.1 DHCP クライアント設定コマンド 9-1
9.1.1 dhcp client dad enable 9-1
9.1.2 dhcp client dscp 9-1
9.1.3 display dhcp client 9-2
9.1.4 ip address dhcp-alloc 9-5

9章 DHCP クライアント

9.1 DHCPクライアント設定コマンド

9.1.1 dhcp client dad enable

Syntax

dhcp client dad enable

undo dhcp client dad enable

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

dhcp client dad enable コマンドはアドレス重複の検出を有効にします。

undo dhcp client dad enable コマンドはアドレス重複の検出を無効にします。

DHCP クライアントは、ARP パケットを使用して IP アドレスの重複があるかどうかを検出します。攻撃者は、サーバが割り当てた IP アドレスを使用できなくさせるため、ARP 応答を送信し、IP アドレスのオーナーとして動作します。ARP 攻撃がネットワークに存在する場合、アドレス重複検出機能を無効にすることを推奨します。

例

アドレス重複の検出を無効にします。

<Switch> system-view

[Switch] undo dhcp client dad enable

9.1.2 dhcp client dscp

Syntax

dhcp client dscp *dscp-value*

undo dhcp client dscp

デフォルト

56

View

System view

定義済みユーザロール

network-admin

パラメータ

dscp-value: DHCP パケットの DSCP を設定します。設定範囲は 0～63 です。

説明

dhcp client dscp コマンドは DHCP クライアントによって送信される DHCP パケットの DSCP を設定します。

undo dhcp client dscp コマンドはデフォルトに戻します。

DHCP パケットの DSCP の値はパケットのプライオリティを指定します。パケットを送信するプライオリティに影響します。DSCP の値が大きくなると、プライオリティが高くなります。

例

DHCP クライアントによって送信される DHCP パケットの DSCP を 30 に設定します。

<Switch> system-view

[Switch] dhcp client dscp 30

9.1.3 display dhcp client

Syntax

display dhcp client [**verbose**] [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

verbose: DHCP クライアントの詳細情報を表示します。指定しない場合、DHCP クライアントの概要情報を表示します。

interface *interface-type interface-number*: インタフェースのタイプと番号を指定します。指定しない場合、すべてのインタフェースの DHCP クライアントの情報を表示します。

説明

display dhcp client コマンドは DHCP クライアントの情報を表示します。

例

すべてのインタフェースの DHCP クライアントの情報を表示します。

<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
```

インタフェースの DHCP クライアントの詳細情報を表示します。

<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.
```

表 9-1 コマンド出力

フィールド	説明
DHCP client information	DHCPクライアントを提供するインタフェースの情報です。
Current state	DHCPクライアントの現在の状態です。 ● **HALT**—クライアントがIPサービスの適用を停止します。 ● **INIT**—初期化状態です。 ● **SELECTING**—クライアントがDHCPサーバを検索するため、DHCP-DISCOVERメッセージを送信し、DHCPサーバからの応答を待っています。 ● **REQUESTING**—クライアントがIPアドレスを要求するDHCP-REQUESTメッセージを送信し、DHCPサーバからの応答を待っています。 ● **BOUND**—クライアントがDHCPサーバからDHCP-ACKメッセージを受信し、正常にIPアドレスを受信しました。 ● **RENEWING**—T1タイマがタイムアウトしました。 ● **REBOUNDING**— T2タイマがタイムアウトしました。
Allocated IP	DHCPサーバによって割り当てられたIPアドレスです。
Allocated lease	割り当てられたリース時間です。
T1	DHCPクライアントのIPアドレスの1/2リース時間です。単位は秒です。
T2	DHCPクライアントのIPアドレスの7/8リース時間です。単位は秒です。
Lease from....to....	リース開始時間と終了時間です。
DHCP server	IPアドレスを割り当てたDHCPサーバのIPアドレスです。
Transaction ID	トランザクションIDです。IPアドレスの割り当てを特定するために、クライアントがランダムに選択する番号です。
Default router	クライアントに割り当てられるゲートウェイアドレスです。
Classless static routes	クライアントに割り当てられるクラスレススタティックルートです。
Static routes	クライアントに割り当てられるクラスフルスタティックルートです。
DNS servers	クライアントに割り当てられるDHCPサーバのアドレスです。
Domain name	クライアントに割り当てられるドメイン名サフィックスです。

フィールド	説明
Boot servers	DHCPクライアント用に指定されるPXEサーバアドレスです（最大16アドレス）。オプション43によって取得されます。
ACS parameter	ACSのパラメータです。
URL	ACSのURLです。
Username	ACSにログインするユーザ名です。
Password	ACSにログインするパスワードです。パスワードが設定されている場合、******と表示されます。パスワードが設定されていない場合、表示されません。
Client ID type	DHCPクライアントIDタイプです。 • クライアントIDとしてASCIIが使用されている場合、タイプの値は00です。 • クライアントIDとして指定したインタフェースのMACアドレスが使用されている場合、タイプの値は01です。 • クライアントIDとしてhexが使用されている場合、タイプの値は文字列の最初の2文字です。
Client ID value	DHCPクライアントIDの値です。
Client ID (with type) hex	タイプフィールドによるクライアントIDです。16進数の文字列です。
T1 will timeout in 1 day 11 hours 58 minutes 52 seconds.	T1タイマ（1/2リース時間）がタイムアウトする時間です。

関連コマンド

- **dhcp client identifier**
- **ip address dhcp-alloc**

9.1.4 ip address dhcp-alloc

Syntax

ip address dhcp-alloc

undo ip address dhcp-alloc

デフォルト

設定なし

View

Interface view

定義済みユーザロール

network-admin

説明

ip address dhcp-alloc コマンドは DHCP を使用して IP アドレスを取得するインタフェースを設定します。

undo ip address dhcp-alloc コマンドはインタフェースで DHCP の使用を停止します。

undo ip address dhcp-alloc コマンドを実行したとき、インタフェースは DHCP を通して取得した IP アドレスをリリースするため、DHCP-RELEASE メッセージを送信します。インタフェースがダウンしている場合、メッセージを送信することができません。

例

DHCP を使用して IP アドレスを取得する VLAN インタフェース 10 を設定します。

<Switch> system-view

[Switch] interface vlan-interface 10

[Switch-Vlan-interface10] ip address dhcp-alloc

目次

このセクションのページは **4-x-x** です。

10 章 DHCP スヌーピング.....10-1
10.1 DHCP snooping 設定コマンド.....10-1
10.1.1 dhcp snooping binding record.....10-1
10.1.2 dhcp snooping enable.....10-2
10.1.3 dhcp snooping information circuit-id.....10-2
10.1.4 dhcp snooping information enable.....10-5
10.1.5 dhcp snooping information remote-id.....10-6
10.1.6 dhcp snooping information strategy.....10-7
10.1.7 dhcp snooping trust.....10-8
10.1.8 display dhcp snooping binding.....10-9
10.1.9 display dhcp snooping information.....10-10
10.1.10 display dhcp snooping packet statistics.....10-12
10.1.11 display dhcp snooping trust.....10-13
10.1.12 reset dhcp snooping binding.....10-14
10.1.13 reset dhcp snooping packet statistics.....10-15

10章 DHCP スヌーピング

10.1 DHCP snooping設定コマンド

DHCP snooping は DHCP クライアントと DHCP サーバの間、あるいは DHCP クライアントとリレーエージェントの間にある場合動作します。

DHCP サーバと DHCP リレーエージェントの間にある場合、DHCP Snooping は動作しません。

10.1.1 dhcp snooping binding record

Syntax

dhcp snooping binding record

undo dhcp snooping binding record

デフォルト

無効

View

Layer 2 Ethernet interface

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

dhcp snooping binding record コマンドは DHCP snooping エントリのクライアント情報の記録を有効にします。

undo dhcp snooping binding record コマンドは DHCP snooping エントリのクライアント情報の記録を無効にします。

このコマンドはクライアントに直接接続しているポートで DHCP snooping が DHCP snooping エントリのクライアント情報の記録することを有効にします。

例

GigabitEthernet 1/0/1 で DHCP snooping エントリのクライアント情報の記録を有効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] dhcp snooping binding record

10.1.2 dhcp snooping enable

Syntax

dhcp snooping enable

undo dhcp snooping enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

dhcp snooping enable コマンドは DHCP snooping を有効にします。

undo dhcp snooping enable コマンドは DHCP snooping を無効にします。

DHCP snooping 機能はトラステッドポートの設定と一緒に使用します。トラステッドポートを設定する前に、DHCP snooping のすべてのポートは非トラステッドポートで、装置は DHCP サーバから送信されたすべての応答を廃棄します。

DHCP snooping が無効であるとき、装置は DHCP サーバからの応答をすべて転送します。

例

DHCP snooping を有効にします。

<Switch> system-view

[Switch] dhcp snooping enable

10.1.3 dhcp snooping information circuit-id

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*]

デフォルト

パディングモードは normal で、パディング形式は hex です。

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

vlan *vlan-id*: circuit ID サブオプションの VLAN ID を指定します。指定しない場合、デフォルト VLAN から受信したパケットの circuit ID サブオプションをパティングします。

string *circuit-id*: circuit ID サブオプションのパディング内容を指定します。設定範囲は 3～63 です。大文字、小文字を区別します。

normal: パディング形式を normal モードに指定します。このパディングの内容は VLAN ID とポート番号から構成されます。

verbose: パディング形式を verbose モードに指定します。パディング内容はノード識別子、Ethernet タイプ、インタフェース情報、VLAN ID が含まれます。デフォルトノードの識別子はアクセスノードの MAC アドレスです。デフォルトのインタフェース情報は Ethernet タイプ（eth で固定です）、シャーシ番号、スロット番号、サブスロット番号、インタフェース番号から構成されます。

node-identifier { **mac** | **sysname** | **user-defined** *node-identifier* }: アクセスノードの識別子を指定します。

- **mac**: ノード識別子としてアクセスノードの MAC アドレスを使用します。デフォルトのノード識別子です。
- **sysname**: ノード識別子として装置名を使用します。装置名は system view の **sysname** コマンドを使用して設定することができます。装置名のパディング形式は指定したパディング形式に関わらず、常に ASCII です。

🕮 **メモ**:

ノード識別子として **sysname** を指定した場合、装置名を設定するときに半角スペースを含むことができません。そうでなければ、DHCP snooping はオプション 82 の追加あるいは置き換えに失敗します。

- **user-defined** *node-identifier*: ユーザ定義のノード識別子を使用します。設定範囲は 1～50 です。大文字、小文字を区別します。指定された文字列のパディング形式は指定したパディング形式に関われず、常に ASCII になります。

format: circuit ID サブオプションのパディング形式を指定します。

ascii: パディング形式を ASCII に指定します。

hex: パディング形式を hex に指定します。

説明

dhcp snooping information circuit-id コマンドは circuit ID サブオプションのパディング内容とパディング形式を設定します。

undo dhcp snooping information circuit-id コマンドはデフォルトに戻します。

コマンドを複数回設定した場合、最後に行った設定が適用されます。

ユーザ定義、normal モード、verbose モードのパディング形式はコマンドの設定によって変わります。表 10-1 に異なるモードのパディング形式を示します。

表 10-1 異なるモードのパディング形式

キーワード（モード）	パディング形式が指定されていない場合	パディング形式が ASCII	パディング形式が hex
string *circuit-id*	パディング形式を指定できません。常にASCIIになります。	ー	ー
normal	hexです。	ASCIIです。	hexです。
verbose	VLAN IDはhexです。 ノード識別子、Ethernetタイプ、シャーシ番号、スロット番号、サブスロット番号、インタフェース番号はASCIIです。	ASCIIです。	ノード識別子、EthernetタイプはASCIIです。 シャーシ番号､スロット番号、サブスロット番号、インタフェース番号、VLAN IDはhexです。

例

circuit ID サブオプションのパディングモードが verbose、ノード識別子が装置名、パディング形式が ASCII として設定します。

<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

関連コマンド

- **dhcp snooping information enable**

- **dhcp snooping information strategy**
- **display dhcp snooping information**

10.1.4 dhcp snooping information enable

Syntax

dhcp snooping information enable

undo dhcp snooping information enable

デフォルト

無効

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

dhcp snooping information enable コマンドは DHCP snooping でオプション 82 のサポートを有効にします。

undo dhcp snooping information enable コマンドは DHCP snooping でオプション 82 のサポートを無効にします。

このコマンドによって DHCP snooping が DHCP サーバに要求を転送する前に、オプション 82 が含まれない DHCP 要求にオプション 82 を追加します。オプション 82 の内容は **dhcp snooping information circuit-id** コマンド、**dhcp snooping information remote-id** コマンドによって決まります。受信した DHCP 要求にオプション 82 が含まれる場合、DHCP snooping は **dhcp snooping information strategy** コマンドで設定された方法にしたがってパケットを処理します。

例

DHCP snooping でオプション 82 のサポートを有効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] dhcp snooping information enable

関連コマンド

- **dhcp snooping information circuit-id**
- **dhcp snooping information remote-id**

- **dhcp snooping information strategy**

10.1.5 dhcp snooping information remote-id

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*]

デフォルト

パディングモードは normal で、パディング形式は hex です。

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

vlan *vlan-id*: remote ID サブオプションの VLAN ID を指定します。指定しない場合、デフォルト VLAN から受信したパケットの remote ID サブオプションをパティングします。

string *remote-id*: remote ID サブオプションのパディング内容を指定します。設定範囲は 1～63 です。大文字、小文字を区別します。

sysname: remote ID サブオプションの内容として装置名を指定します。装置名は system view で **sysname** コマンドを使用して設定することができます。

normal: パディングモードを normal に指定します。このパディングの内容は受信インタフェースの MAC アドレスです。

format: remote ID サブオプションのパディング形式を指定します。デフォルトは hex です。

ascii: パディング形式を ASCII に指定します。

hex: パディング形式を hex に指定します。

説明

dhcp snooping information remote-id コマンドは remote ID サブオプションのパディングモードとパディング形式を設定します。

undo dhcp snooping information remote-id コマンドはデフォルトに戻します。

DHCP snooping は remote ID サブオプションの指定した文字列（**string**）あるいは装置名（**sysname**）に ASCII を使用します。normal モードのパディングモードはコマンドの設定によって変わります。

コマンドを複数回設定した場合、最後に行った設定が適用されます。

例

remote ID サブオプションのパディング内容を device001 に指定します。

<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

関連コマンド

- **dhcp snooping information enable**
- **dhcp snooping information strategy**
- **display dhcp snooping information**

10.1.6 dhcp snooping information strategy

Syntax

dhcp snooping information strategy { **drop** | **keep** | **replace** }

undo dhcp snooping information strategy

デフォルト

replace

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

drop: オプション 82 メッセージが含まれる DHCP メッセージを廃棄します。

keep: オプション 82 を含むメッセージをそのまま転送するよう指定します。

replace: もとのオプション 82 のメッセージを設定されたオプション 82 のメッセージに置き換えします。

説明

dhcp snooping information strategy コマンドはオプション 82 が含まれる要求メッセージの処理方法を設定します。

undo dhcp snooping information strategy コマンドはデフォルトに戻します。

このコマンドは DHCP 要求にオプション 82 が含まれるときのみ適用します。DHCP 要求にオプション 82 が含まれない場合、DHCP サーバに転送する前に、DHCP snooping は DHCP 要求にオプション 82 を追加します。

replace パラメータを指定した場合、オプション 82 のパディングモード、パディング形式を設定します。**keep** パラメータあるいは **drop** パラメータを指定した場合、オプション 82 のパディングモード、パディング形式を設定する必要がありません。

例

オプション 82 が含まれる要求メッセージの処理方法を keep に設定します。

<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

関連コマンド

- **dhcp snooping information circuit-id**
- **dhcp snooping information remote-id**

10.1.7 dhcp snooping trust

Syntax

dhcp snooping trust

undo dhcp snooping trust

デフォルト

DHCP snooping を有効にしたのち、すべてのポートが非トラステッドポートです。

View

Layer 2 Ethernet interface

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

dhcp snooping trust コマンドはトラステッドポートとしてポートを設定します。

undo dhcp snooping trust コマンドはポートをデフォルト状態に戻します。

DHCP クライアントが正常な IP アドレスを取得できるように、DHCP サーバに面しているポートをトラステッドポートに指定し、他のポートを非トラステッドポートに指定します。

例

トラステッドポートとして GigabitEthernet 1/0/1 を設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] dhcp snooping trust

関連コマンド

display dhcp snooping trust

10.1.8 display dhcp snooping binding

Syntax

display dhcp snooping binding [**ip** *ip-address* [**vlan** *vlan-id*]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ip *ip-address*: 指定された IP アドレスの DHCP snooping エントリを表示します。指定しない場合、すべての IP アドレスの DHCP snooping エントリを表示します。

vlan *vlan-id*: IP アドレスが存在する VLAN ID を指定します。指定しない場合、すべての VLAN の DHCP snooping エントリを表示します。

説明

display dhcp snooping binding コマンドは DHCP snooping エントリを表示します。

例

すべての DHCP snooping エントリを表示します。

<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
```

表 10-2 コマンド出力

フィールド	説明
DHCP snooping entries found	DHCP snoopingエントリの数です。
IP address	DHCPクライアントに割り当てられたIPアドレスです。
MAC address	DHCPクライアントのMACアドレスです。
Lease	残りリース期間です。単位は秒です。
VLAN	DHCP snoopingとQinQの両方が有効、あるいはDHCPパケットに2つのVLANタグが含まれる場合、このフィールドは外部VLANタグを示します。そうでない場合、DHCPクライアントが存在するポートに接続しているVLANを示します。
SVLAN	DHCP snoopingとQinQの両方が有効、あるいはDHCPパケットに2つのVLANタグが含まれる場合、このフィールドは内部VLANタグを示します。そうでない場合、**N/A**と表示されます。
Interface	DHCPクライアントに接続されたポートです。

関連コマンド

- **dhcp snooping enable**
- **reset dhcp snooping binding**

10.1.9 display dhcp snooping information

Syntax

display dhcp snooping information { **all** | **interface** *interface-type interface-number* }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all: すべてのレイヤ 2 Ethernet インタフェースのオプション 82 の設定を表示します。

interface *interface-type interface-number*: インタフェースのタイプと番号を指定します。

説明

display dhcp snooping information コマンドは DHCP snooping 装置のオプション 82 の設定を表示します。

例

すべてのインタフェースのオプション 82 の設定を表示します。

<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
   Vendor-specific:
     Padding format: BAS
     Node identifier: MAC
   VLAN 10:
     Circuit ID: abcd
     Remote ID: company
     Vendor-specific:
       Padding format: BAS
       Node identifier: User defined(abcd)
```

表 10-3 コマンド出力

フィールド	説明
Interface	インタフェース名です。
Status	オプション82の状態です。**Enable**あるいは**Disable**です。
Strategy	DHCP要求の処理方法です。 **Option 82**、**Drop**、**Keep**、**Replace**が含まれます。
Circuit ID	circuit IDサブオプションの内容です。

フィールド	説明
Padding format	オプション82のパディング形式です。 ● circuit IDサブオプションでは、パディング形式は**Normal**、**User Defined**、**Verbose (sysname)**、**Verbose (MAC)**、**Verbose (user defined)**があります。 ● remote IDサブオプションでは、パディング形式は**Normal**、**Sysname**、**User Defined**があります。 ● Vendor-Specificサブオプションの場合、パディング形式は**BAS**です。
Node identifier	アクセスノード識別子です。 ● circuit IDサブオプションの場合、このフィールドにはユーザ定義のノード識別子文字列が表示されます。 ● remote IDサブオプションの場合、このフィールドにはユーザ定義の文字列が表示されます。 ● Vendor-Specificサブオプションでは、ノード識別子は**MAC**、**Sysname**、または**User Defined(string)**である可能性があり、括弧内の文字列はユーザ定義ノード識別子を示します。
User defined	ユーザ定義サブオプションの内容です。
Format	オプション82サブオプションのコードタイプです。 ● circuit IDサブオプションでは、コードタイプはASCII、Default、Hexがあります。 ● remote IDサブオプションでは、コードタイプはASCII、Hexがあります。
Remote ID	remote IDサブオプションの内容です。
Vendor-specific	Vendor-Specificサブオプションの内容です。このフィールドは、Vendor-Specificサブオプションが設定されている場合にのみ表示されます。
VLAN	指定したVLANで受信したDHCPパケットのcircuit IDサブオプション、remote IDサブオプション、Vendor-Specificのサブオプションのパディングです。

10.1.10 display dhcp snooping packet statistics

Syntax

display dhcp snooping packet statistics [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

slot *slot-number*: IRF スタックメンバ装置を指定します。*slot-number* は IRF スタックユニットのメンバ装置の ID を示します。指定しない場合、マスタ装置の DHCP パケットの統計情報を表示します。

説明

display dhcp snooping packet statistics コマンドは DHCP snooping の DHCP パケットの統計情報を表示します。

例

DHCP snooping の DHCP パケットの統計情報を表示します。

<Switch> display dhcp snooping packet statistics

```
DHCP packets received              : 100
DHCP packets sent                  : 200
Invalid DHCP packets dropped         : 0
```

関連コマンド

reset dhcp snooping packet statistics

10.1.11 display dhcp snooping trust

Syntax

display dhcp snooping trust

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display dhcp snooping trust コマンドはトラステッドポートの情報を表示します。

例

トラステッドポートの情報を表示します。

<Switch> display dhcp snooping trust

```
DHCP snooping is enabled.
 Interface                                Trusted  VLAN
 ============================               =======  ================
 GigabitEthernet1/0/1                      Trusted

 VSI(Trust tunnel)                         Trusted
 ============================               ============

 Interface                 SrvID           Trusted
 ==================================          ============
```

関連コマンド

dhcp snooping trust

10.1.12 reset dhcp snooping binding

Syntax

reset dhcp snooping binding { **all** | **ip** *ip-address* [**vlan** *vlan-id*] }

View

User view

定義済みユーザロール

network-admin

パラメータ

all: すべての DHCP snooping エントリを削除します。

ip *ip-address*: 指定された IP アドレスの DHCP snooping エントリを削除します。

vlan *vlan-id*: 指定された VLAN の DHCP snooping エントリを削除します。指定しない場合、デフォルト VLAN の DHCP snooping エントリを削除します。

説明

reset dhcp snooping binding コマンドは DHCP snooping エントリを削除します。

例

すべての DHCP snooping エントリを削除します。

<Switch> reset dhcp snooping binding all

関連コマンド

display dhcp snooping binding

10.1.13 reset dhcp snooping packet statistics

Syntax

reset dhcp snooping packet statistics [**slot** *slot-number*]

View

User view

定義済みユーザロール

network-admin

パラメータ

slot *slot-number*: IRF スタックメンバ装置を指定します。*slot-number* は IRF スタックユニットのメンバ装置の ID を示します。指定しない場合、実行される IRF スタックメンバ装置の DHCP パケットの統計情報を削除します。

説明

reset dhcp snooping packet statistics コマンドは DHCP snooping の DHCP パケットの統計情報を削除します。

例

DHCP snooping の DHCP パケットの統計情報を表示します。

<Switch> reset dhcp snooping packet statistics

関連コマンド

display dhcp snooping packet statistics

目次

このセクションのページは **4-x-x** です。

11 章 BOOTP クライアント.....11-1
11.1 BOOTP クライアント設定コマンド.....11-1
11.1.1 display bootp client 11-1
11.1.2 ip address bootp-alloc 11-2

11章 BOOTP クライアント

11.1 BOOTPクライアント設定コマンド

11.1.1 display bootp client

Syntax

display bootp client [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: インタフェースのタイプと番号を指定します。指定しない場合、すべてのインタフェースの BOOTP クライアント情報を表示します。

説明

display bootp client コマンドは BOOTP クライアントの情報を表示します。

例

VLAN インタフェース 10 の BOOTP クライアントの情報を表示します。

<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
```

表 11-1 コマンド出力

フィールド	説明
BOOTP client information	BOOTPクライアントとして動作するインタフェースの情報です。
Allocated IP	BOOTPサーバによって割り当てられたBOOTPクライアントのIPアドレスです。

フィールド	説明
Transaction ID	BOOTPメッセージのXIDフィールドの値です。BOOTPクライアントがBOOTPサーバにBOOTP要求を送信するときにランダムに選択される番号です。この値はBOOTPサーバからの応答メッセージを一致させるために使用します。 BOOTP応答とBOOTP要求のXIDフィールドの値が異なる場合、BOOTPクライアントはBOOTP応答を廃棄します。
Mac Address	BOOTPクライアントのMACアドレスです。

関連コマンド

ip address bootp-alloc

11.1.2 ip address bootp-alloc

Syntax

ip address bootp-alloc

undo ip address bootp-alloc

デフォルト

IP アドレスを取得するためインタフェースは BOOTP を使用しません。

View

Interface view

定義済みユーザロール

network-admin

説明

ip address bootp-alloc コマンドは IP アドレスを取得するために BOOTP を使用するインタフェースを設定します。

undo ip address bootp-alloc コマンドはインタフェースで BOOTP を使用することを中止します。

例

IP アドレスを取得するために BOOTP を使用する VLAN インタフェース 10 を設定します。

<Switch> system-view

[Switch] interface vlan-interface 10

[Switch-Vlan-interface10] ip address bootp-alloc

関連コマンド

display bootp client

目次

このセクションのページは **4-x-x** です。

12 章 DNS 12-1
12.1 DNS 設定コマンド.....12-1
12.1.1 display dns domain 12-1
12.1.2 display dns host.....12-2
12.1.3 display dns server.....12-3
12.1.4 display ipv6 dns server.....12-5
12.1.5 dns domain 12-6
12.1.6 dns dscp 12-7
12.1.7 dns proxy enable 12-7
12.1.8 dns server 12-8
12.1.9 ip host.....12-9
12.1.10 ipv6 dns dscp 12-10
12.1.11 ipv6 dns server 12-11
12.1.12 ipv6 host 12-12
12.1.13 reset dns host.....12-13

12章 DNS

12.1 DNS設定コマンド

12.1.1 display dns domain

Syntax

display dns domain [**dynamic**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

dynamic: DHCP または他のプロトコルによってダイナミックに取得したドメイン名のサフィックスを表示します。指定しない場合、スタティックに設定したドメイン名のサフィックスおよび、ダイナミックに取得したドメイン名のサフィックスを表示します。

説明

display dns domain コマンドはドメイン名のサフィックスを表示します。

例

パブリックネットワークのドメイン名のサフィックスを表示します。

<Switch> display dns domain

```
Type:
  D: Dynamic    S: Static

No.    Type   Domain suffix
1      S      com
2      D      net
```

表 12-1 コマンド出力

フィールド	説明
No.	シーケンス番号です。

フィールド	説明
Type	ドメイン名のサフィックスのタイプです。 ● **S**—スタティックに設定されたドメイン名のサフィックスです。 ● **D**—DHCPまたは他のプロトコルによってダイナミックに取得したドメイン名のサフィックスです。
Domain suffix	ドメイン名のサフィックスです。

関連コマンド

dns domain

12.1.2 display dns host

Syntax

display dns host [**ip**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ip: タイプ A のクエリを指定します。タイプ A のクエリは IPv4 アドレスにドメイン名サフィックスをマッピングします。

説明

display dns host コマンドはドメイン名－IP アドレスのマッピングを表示します。

パラメータを指定しない場合、すべてのクエリタイプのドメイン名－IP アドレスのマッピングを表示します。

例

すべてのクエリタイプのドメイン名－IP アドレスのマッピングを表示します。

<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
```

表 12-2 コマンド出力

フィールド	説明
No.	シーケンス番号です。
Host name	ドメイン名です。
Type	ドメイン名－IPアドレスマッピングのタイプです。 • **S**—**ip host**コマンドあるいは**ipv6 host**コマンドで設定されたスタティックマッピングです。 • **D**—ダイナミックドメイン名解決によってダイナミックに取得したマッピングです。
TTL	マッピングがキャッシュに記録できる時間です。単位は秒です。 スタティックマッピングの場合、ハイフン（-）が表示されます。
Query type	クエリタイプです。タイプA、タイプAAAAがあります。
IP addresses	応答したIPアドレスです。 • タイプAクエリでは、応答したIPアドレスはIPv4アドレスです。 • タイプAAAAクエリでは、応答したIPアドレスはIPv6アドレスです。

関連コマンド

- **ip host**
- **reset dns host**

12.1.3 display dns server

Syntax

display dns server [**dynamic**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

dynamic: DHCP あるいは他のプロトコルによってダイナミックに取得した IPv4 DNS サーバの情報です。指定しない場合、スタティックに設定された IPv4 DNS サーバとダイナミックに取得した IPv4 DNS サーバを表示します。

説明

display dns server コマンドは IPv4 DNS サーバの情報を表示します。

例

パブリックネットワークの IPv4 DNS サーバの情報を表示します。

<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
```

表 12-3 コマンド出力

フィールド	説明
No.	シーケンス番号です。
Type	DNSサーバタイプです。 ● **S**—スタティックに設定されたDNSサーバの情報です。 ● **D**—DHCPあるいは他のプロトコルによってダイナミックに取得したDNSサーバの情報です。
IP address	DNSサーバのIPv4アドレスです。

関連コマンド

dns server

12.1.4 display ipv6 dns server

Syntax

display ipv6 dns server [**dynamic**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

dynamic: DHCP あるいは他のプロトコルによってダイナミックに取得した IPv6 DNS サーバの情報です。指定しない場合、スタティックに設定された IPv6 DNS サーバとダイナミックに取得した IPv6 DNS サーバを表示します。

説明

display ipv6 dns server コマンドは、IPv6 DNS サーバ情報を表示します。

例

パブリックネットワークの IPv6 DNS サーバ情報を表示します。

<Switch> display ipv6 dns server

```
Type:
  D: Dynamic    S: Static

No. Type  IPv6 address                            Outgoing Interface
1   S     2::2
```

表 12-4 コマンド出力

フィールド	説明
No.	シーケンス番号です。
Type	DNSサーバタイプです。 ● **S**—スタティックに設定されたDNSサーバの情報です。 ● **D**—DHCPあるいは他のプロトコルによってダイナミックに取得したDNSサーバの情報です。
IPv6 address	DNSサーバのIPv6アドレスです。
Outgoing Interface	出力インタフェースです。

関連コマンド

ipv6 dns server

12.1.5 dns domain

Syntax

dns domain *domain-name*

undo dns domain *domain-name*

デフォルト

ドメイン名サフィックスは設定されていません。既定のドメイン名のみが解決できます。

View

System view

定義済みユーザロール

network-admin

パラメータ

domain-name: ドメイン名サフィックスを指定します。ドメイン名サフィックスは、ドットにより区切られた文字列により構成されます。ドメイン名サフィックスは、大文字、小文字を区別しない文字、数字、ハイフン（-）、アンダーバー（_）、ドット（.）を使用することができます。たとえば、aabbcc.com です。合計の文字数は 253 文字までです。それぞれの区切られた文字列は 63 文字までです。

説明

dns domain コマンドはドメイン名サフィックスを設定します。

undo dns domain コマンドは指定されたドメイン名サフィックスを削除します。

システムはホスト解決を行うため、ホストから受信したドメイン名の順番でサフィックスを自動で追加します。

パブリックネットワークで最大 16 のドメイン名サフィックスを指定することができます。

例

パブリックネットワークのドメイン名サフィックスを設定します。

<Switch> system-view

[Switch] dns domain com

関連コマンド

display dns domain

12.1.6 dns dscp

Syntax

dns dscp *dscp-value*

undo dns dscp

デフォルト

0

View

System view

定義済みユーザロール

network-admin

パラメータ

dscp-value: DSCP を指定します。設定範囲は 0～63 です。

説明

dns dscp コマンドは DNS クライアントあるいは DNS Proxy によって送信された DNS パケットの DSCP を設定します。

undo dns dscp コマンドはデフォルトに戻します。

DHCP パケットの DSCP の値はパケットのプライオリティを指定します。パケットを送信するプライオリティに影響します。DSCP の値が大きくなると、プライオリティが高くなります。

例

送信 DNS パケットの DSCP を 30 に設定します。

<Switch> system-view

[Switch] dns dscp 30

12.1.7 dns proxy enable

Syntax

dns proxy enable

undo dns proxy enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

dns proxy enable コマンドは DNS Proxy を有効にします。

undo dns proxy enable コマンドは DNS Proxy を無効にします。

この設定は IPv4DNS と IPv6DNS の両方に適用されます。

例

DNS Proxy を有効にします。

<Switch> system-view

[Switch] dns proxy enable

12.1.8 dns server

Syntax

dns server *ip-address*

undo dns server [*ip-address*]

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

ip-address: DNS サーバの IPv4 アドレスを指定します。

説明

dns server コマンドは DNS サーバの IPv4 アドレスを指定します。

undo dns server コマンドは DNS サーバの IPv4 アドレスを削除します。

装置は IPv4 アドレスが指定された順番で、DNS サーバに DNS クエリ要求を送信します。

パブリックネットワークで最大 6 つの DNS サーバの IPv4 アドレスを指定することができます。

IPv4 アドレスを指定しない場合、**undo dns server** コマンドはパブリックネットワークのすべての DNS サーバの IPv4 アドレスを削除します。

例

DNS サーバの IPv4 アドレス 172.16.1.1 を指定します。

<Switch> system-view

[Switch] dns server 172.16.1.1

関連コマンド

display dns server

12.1.9 ip host

Syntax

ip host *host-name ip-address*

undo ip host *host-name ip-address*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

host-name: ホスト名を指定します。設定範囲は 1～253 です。大文字、小文字を区別しません。英字、数字、ハイフン（-）、アンダーライン（_）、ドット（.）を含めることができます。

ip-address: ホストの IPv4 アドレスを指定します。

説明

ip host コマンドはホスト名－IPv4 アドレスマッピングを作成します。

undo ip host コマンドはマッピングを削除します。

最大 1024 のホスト名－IPv4 アドレスマッピングを作成することができます。

パブリックネットワークで各ホスト名は 1 つの IPv4 アドレスのみマッピングすることができます。コマンドを複数回設定した場合、最後に行った設定が適用されます。

ホスト名を使用して **ping** コマンドのパラメータ **ip**、**-a**、**-c**、**-f**、**-h**、**-i**、**-m**、**-n**、**-p**、**-q**、**-r**、**-s**、**-t**、**-tos**、**–v** を実行することができます。**ping** コマンドのパラメータの詳細は、コマンドマニュアルのセクション 11 *システム管理*”*システムの保守とデバッグ*”を参照してください。

例

パブリックネットワークの IPv4 アドレス 10.110.0.1 をホスト名 aaa にマッピングします。

<Switch> system-view

[Switch] ip host aaa 10.110.0.1

関連コマンド

display dns host

12.1.10 ipv6 dns dscp

Syntax

ipv6 dns dscp *dscp-value*

undo ipv6 dns dscp

View

System view

定義済みユーザロール

network-admin

パラメータ

dscp-value: DSCP 値を指定します。設定範囲は 0～63 です。

説明

i**pv6 dns dscp** コマンドは IPv6 DNS クライアントまたは IPv6 DNS プロキシによって送信された IPv6 DNS パケットの DSCP 値を設定にします。

undo ipv6 dns dscp コマンドはデフォルトに戻します。

DSCP パケットの値は、パケットの優先順位レベルを指定し、パケットの送信優先順位に影響します。大きい DSCP 値は高い優先順位を表します。

例

送信 IPv6 DNS パケットの DSCP 値を 30 に設定します。

<Switch> system-view

[Switch] ipv6 dns dscp 30

関連コマンド

display ipv6 dns server

12.1.11 ipv6 dns server

Syntax

ipv6 dns server *ipv6-address* [*interface-type interface-number*]

undo ipv6 dns server [*ipv6-address* [*interface-type interface-number*]]

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

ipv6-address: DNS サーバの IPv6 アドレスを指定します。

interface-type interface-number: 出力インタフェースをタイプと番号で指定します。インタフェースを指定しない場合、装置は一致するルートの出力インタフェースから DNS パケットを転送します。DNS サーバの IPv6 アドレスがリンクローカルアドレスの場合は、この引数を指定します。DNS サーバの IPv6 アドレスがグローバルユニキャストアドレスである場合は、この引数を指定しないでください。

説明

ipv6 dns server コマンドは DNS サーバの IPv6 アドレスを指定します。

undo ipv6 dns server コマンドは DNS サーバの IPv6 アドレスを削除します。

ダイナミック DNS の場合、装置は IPv6 アドレスが指定されている順序で DNS サーバに DNS クエリ要求を送信します。

システムは、パブリックネットワークまたは各 VPN インスタンスに対して最大 6 つの DNS サーバ IPv6 アドレスを許可します。パブリックネットワークと VPN インスタンスの両方に DNS サーバの IPv6 アドレスを指定できます。

IPv6 アドレスを指定しない場合、**undo ipv6 dns server** コマンドは、パブリックネットワークまたは指定された VPN インスタンスのすべての DNS サーバ IPv6 アドレスを削除します。

例

#パブリックネットワークに DNS サーバの IPv6 アドレス 2002::1 を指定します。

<Switch> system-view

[Switch] ipv6 dns server 2002::1

関連コマンド

display ipv6 dns server

12.1.12 ipv6 host

Syntax

ipv6 host *host-name ipv6-address*

undo ipv6 host *host-name ipv6-address*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

host-name: ホスト名を指定します。設定範囲は 1～253 です。大文字、小文字を区別しません。英字、数字、ハイフン（-）、アンダーライン（_）、ドット（.）を含めることができます。

ipv6-address: ホストの IPv6 アドレスを指定します。

説明

ipv6 host コマンドは、ホスト名と IPv6 アドレスのマッピングを作成します。

undo ipv6 host コマンドは、ホスト名と IPv6 アドレスのマッピングを削除します。

以下の指定ができます。

- パブリックネットワークでのホスト名と IPv6 アドレスのマッピングと最大 1024 の VPN
- パブリックネットワークあるいはそれぞれの VPN での最大 1024 のホスト名と IPv6 アドレスのマッピング

パブリックネットワークや VPN において、各ホスト名は 1 つの IPv6 アドレスのみマッピングすることができます。コマンドを複数回設定した場合、最後に行った設定が適用されます。

ホスト名を使用して **ping ipv6** コマンドのパラメータ **-a**、**-c**、**-i**、**-m**、**-q**、**-s**、**-t**、**-tc**、**–v** または **-vpn-instance** を実行することができます。**ping** コマンドのパラメータの詳細は、コマンドマニュアルのセクション 11 *システム管理*”*システムの保守とデバッグ*”を参照してください。

例

Map IPv6 address 2001::1 to host name **aaa** for the public network.

<Switch> system-view

[Switch] ipv6 host aaa 2001::1

関連コマンド

ip host

12.1.13 reset dns host

Syntax

reset dns host [**ip** | **ipv6**]

View

User view

定義済みユーザロール

network-admin

パラメータ

ip: タイプ A のクエリを指定します。タイプ A のクエリは IPv4 アドレスにドメイン名サフィックスをマッピングします。

ipv6: タイプ AAAA のクエリを指定します。タイプ AAAA のクエリは IPv6 アドレスにドメイン名サフィックスをマッピングします。

説明

reset dns host コマンドはダイナミック DNS キャッシュの情報を削除します。

パラメータを指定しない場合、すべてのクエリタイプのダイナミック DNS キャッシュ情報を削除します。

例

パブリックネットワークのすべてのクエリタイプのダイナミック DNS キャッシュ情報を削除します。

<Switch> reset dns host

関連コマンド

display dns host

目次

このセクションのページは **4-x-x** です。

13 章 IP フォワーディングの基本 13-1
13.1 IP フォワーディングの基本設定コマンド.....13-1
13.1.1 display fib.....13-1

13章 IP フォワーディングの基本

13.1 IPフォワーディングの基本設定コマンド

13.1.1 display fib

Syntax

display fib [*ip-address* [*mask* | *mask-length*]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ip-address: 指定した宛先 IP アドレスに一致する FIB エントリを表示します。

mask: IP アドレスのマスクを指定します。

mask-length: IP アドレスのマスク長を指定します。マスクが連続する数です。設定範囲は 0～32 です。

説明

display fib コマンドは FIB エントリを表示します。

マスクあるいはマスク長を指定しないで IP アドレスを指定した場合、ロンゲストマッチに従う FIB エントリを表示します。つまり、もっとも長いマスク長に一致する FIB エントリを表示します

マスクあるいはマスク長を指定し、IP アドレスを指定した場合、正確に一致する FIB エントリを表示します。

例

パブリックネットワークのすべての FIB エントリを表示します。

<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  USGF     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
```

宛先 IP アドレス 10.2.1.1 に一致する FIB エントリを表示します。

<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
```

表 13-1 コマンド出力

フィールド	説明
Destination count	宛先アドレスの総数です。
FIB entry count	FIBエントリの総数です。
Destination/Mask	宛先アドレス/マスク長です。
Nexthop	ネクストホップアドレスです。
Flag	ルートフラグです。 ● **U**—使用可能なルートです。 ● **G**—ゲートウェイルートです。 ● **H**—ホストルートです。 ● **B**—ブラックホールルートです。 ● **D**—ダイナミックルートです。 ● **S**—スタティックルートです。 ● **R**—中継ルートです。 ● **F**—fastルート変更です。
OutInterface/Token	出力インタフェース/LSPインデックス番号です。
Label	内部ラベルです。

目次

このセクションのページは **4-x-x** です。

14 章 IP パフォーマンスの最適化 14-1
14.1 IP パフォーマンスの最適化設定コマンド 14-1
14.1.1 display icmp statistics 14-1
14.1.2 display ip statistics 14-2
14.1.3 display rawip 14-4
14.1.4 display rawip verbose 14-5
14.1.5 display tcp 14-9
14.1.6 display tcp statistics 14-10
14.1.7 display tcp verbose 14-12
14.1.8 display udp 14-18
14.1.9 display udp statistics 14-19
14.1.10 display udp verbose 14-20
14.1.11 ip forward-broadcast 14-23
14.1.12 ip icmp error-interval 14-24
14.1.13 ip mtu 14-25
14.1.14 ip redirects enable 14-27
14.1.15 ip ttl-expires enable 14-27
14.1.16 ip unreachables enable 14-28
14.1.17 reset ip statistics 14-30
14.1.18 reset tcp statistics 14-30
14.1.19 reset udp statistics 14-31
14.1.20 tcp path-mtu-discovery 14-31
14.1.21 tcp timer fin-timeout 14-32
14.1.22 tcp timer syn-timeout 14-33
14.1.23 tcp window 14-34

14章 IP パフォーマンスの最適化

14.1 IPパフォーマンスの最適化設定コマンド

14.1.1 display icmp statistics

Syntax

display icmp statistics [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

slot *slot-number*: IRF スタックメンバ装置の ICMP の統計情報を表示します。*slot-number* は IRF スタックメンバ装置の ID を指定します。指定しない場合、すべてのメンバ装置の ICMP の統計情報を表示します。

説明

display icmp statistics コマンドは ICMP パケットの送受信に関する統計情報を表示します。

例

ICMP の統計情報を表示します。

<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
```

14.1.2 display ip statistics

Syntax

display ip statistics [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

slot *slot-number*: IRF スタックメンバ装置の IP パケットの統計情報を表示します。*slot-number* は IRF スタックメンバ装置の ID を指定します。指定しない場合、すべてのメンバ装置の IP パケットの統計情報を表示します。

説明

display ip statistics コマンドは IP パケットの統計情報を表示します。

IP 統計情報はパケットの送受信、再構築に関する情報が含まれます。

例

IP パケットの統計情報を表示します。

<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
```

表 14-1 コマンド出力

フィールド	説明
Input	受信したパケットの統計情報です。 • **sum**–受信したパケットの総数です。 • **local**–装置へ送信されたパケットの総数です。 • **bad protocol**–不明なプロトコルのパケットの総数です。 • **bad format**–不正なフォーマットのパケットの総数です。 • **bad checksum**–不正なチェックサムのパケットの総数です。 • **bad options**–不正なオプションのパケットの総数です。
Output	送信したパケットの統計情報です。 • **forwarding**–転送されたパケットの総数です。 • **local**–ローカルに送信されたパケットの総数です。 • **dropped**–廃棄されたパケットの総数です。 • **no route**–ルートが無効なパケットの総数です。 • **compress fails**–圧縮に失敗したパケットの総数です。
Fragment	フラグメントパケットの統計情報です。 • **input**–受信したフラグメントパケットの総数です。 • **output**–送信したフラグメントパケットの総数です。 • **dropped**–廃棄されたフラグメントパケットの総数です。 • **fragmented**–正常にフラグメントされたパケットの総数です。 • **couldn't fragment**–フラグメントに失敗したパケットの総数です。
Reassembling	リアセンブルパケットの統計情報です。 • **sum**–リアセンブルしたパケットの総数です。 • **timeouts**–一定時間内にリアセンブルできなかったパケットの総数です。

関連コマンド

- **display ip interface**
- **reset ip statistics**

14.1.3 display rawip

Syntax

display rawip [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

slot *slot-number*: 指定した IRF スタックメンバ装置の RawIP 接続の概要情報を表示します。*slot-number* は IRF スタックメンバ装置の ID を指定します。指定しない場合、すべてのメンバ装置の RawIP 接続の概要情報を表示します。

説明

display rawip コマンドは RawIP 接続の概要情報を表示します。

RawIP 接続の概要情報はローカルアドレス、ピアのアドレス、プロトコル、PCB が含まれます。

例

RawIP 接続の概要情報を表示します。

<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
```

表 14-2 コマンド出力

フィールド	説明
Local Addr	ローカルIPアドレスです。
Foreign Addr	ピアのIPアドレスです。
Protocol	プロトコル番号です。
PCB	プロトコルコントロールブロックです。

14.1.4 display rawip verbose

Syntax

display rawip verbose [**slot** *slot-number* [**pcb** *pcb-index*]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

pcb *pcb-index*: 指定した PCB の RawIP 接続の詳細情報を表示します。*pcb-index* は PCB のインデックスを指定します。設定範囲は 16 進数で 1～ffffffffffffffff です。

slot *slot-number*: 指定した IRF スタックメンバ装置の RawIP 接続の詳細情報を表示します。*slot-number* は IRF スタックメンバ装置の ID を指定します。指定しない場合、すべてのメンバ装置の RawIP 接続の詳細情報を表示します。

説明

display rawip verbose コマンドは RawIP 接続の詳細情報を表示します。

RawIP 接続の詳細情報はソケット作成のタスク名、状態、オプション、タイプ、プロトコル番号、RawIP 接続の送信元 IP アドレス、RawIP 接続の宛先 IP アドレスが含まれます。

例

RawIP 接続の詳細情報を表示します。

<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
```

表 14-3 コマンド出力

フィールド	説明
Total RawIP socket number	RawIPソケットの総数です。
Creator	ソケットを作成したタスク名です。括弧の数はタスク名の処理番号です。
State	ソケットの状態です。
Options	ソケットのオプションです。
Error	エラーコードです。

Receiving buffer (cc/hiwat/lowat/drop/state)	以下の順番で受信バッファ情報を表示します。
	• **cc**–使用されているバッファ空間です。
	• **hiwat**–最大バッファ空間です。
	• **lowat**–最小バッファ空間です。
	• **drop**–パケット廃棄数です。
	• **state**–バッファ状態です。
	  • **CANTSENDMORE**–ピアにデータを送信できません。
	  • **CANTRCVMORE**–ピアからデータを受信できません。
	  • **RCVATMARK**–タグを受信しています。
	  • **N/A**–上記以外の状態です。

Sending buffer (cc/hiwat/lowat/state)	以下の順番で送信バッファ情報を表示します。
	• **cc**–使用されているバッファ空間です。
	• **hiwat**–最大バッファ空間です。
	• **lowat**–最小バッファ空間です。
	• **state**–バッファ状態です。
	  • **CANTSENDMORE**–ピアにデータを送信できません。
	  • **CANTRCVMORE**–ピアからデータを受信できません。
	  • **RCVATMARK**–タグを受信しています。
	  • **N/A**–上記以外の状態です。

フィールド	説明
Type	ソケットタイプです。 ● **1**–SOCK_STREAMです。このソケットはストリームの信頼できる転送を提供するためにTCPを使用します。 ● **2**–SOCK_DGRAMです。このソケットはデータグラムの転送を提供するためにUDPを使用します。 ● **3**–SOCK_RAWです。このソケットはアプリケーションが次の上位レイヤプロトコルヘッダを変更することを許可します。 ● **N/A**–上記以外のタイプです。
Protocol	ソケットを使用したプロトコル数です。
Connection info	送信元IPアドレスと宛先IPアドレスです。

フィールド	説明
Inpcb flags	インタネットPCBのフラグです。 • **INP_RECVOPTS**–IPオプションを受信します。 • **INP_RECVRETOPTS**–応答したIPオプションを受信します。 • **INP_RECVDSTADDR**–宛先IPアドレスを受信します。 • **INP_HDRINCL**–全体のIPヘッダを提供します。 • **INP_REUSEADDR**–IPアドレスを再利用します。 • **INP_REUSEPORT**–ポート番号を再利用します。 • **INP_ANONPORT**–ポート番号が指定されていません。 • **INP_RECVIF**–パケットの入力インタフェースを記録します。 • **INP_RECVTTL**–パケットのTTLを受信します。このフラグはUDPとRawIPのみサポートします。 • **INP_DONTFRAG**–DF(Don't Fragment)フラグを設定します。 • **INP_ROUTER_ALERT**–ルータ警告オプションのパケットを受信します。このフラグはRawIPのみサポートします。 • **INP_PROTOCOL_PACKET**–プロトコルパケットを識別します。 • **INP_RCVVLANID**–パケットのVLAN IDを受信します。このフラグはUDPとRawIPのみサポートします。 • **INP_RCVMACADDR**–フレームのMACアドレスを受信します。 • **INP_RECVTOS**–パケットのTOSを受信します。このフラグはUDPとRawIPのみサポートします。 • **INP_USEICMPSRC**–送信ICMPパケットの送信元IPアドレスとして指定したIPアドレスを使用します。 • **INP_SYNCPCB**–インタネットPCBが同期されるまで待ちます。 • **N/A**–上記以外のフラグです。
Inpcb extflag	インタネットPCBの拡張フラグです。 • **INP_EXTRCVPVCIDX**–受信したパケットのPVCインデックスの記録です。 • **INP_RCVPWID**–受信したパケットのPW IDの記録です。 • **INP_EXTRCVICMPERR**–ICMPエラーパケットを受信します。 • **INP_EXTFILTER**–受信したパケットの内容をフィルタします。 • **N/A**–上記以外のフラグです。

フィールド	説明
Inpcb vflag	インタネットPCBのIPバージョンフラグです。 • **INP_IPV4**–IPv4プロトコルです。 • **INP_TIMEWAIT**–TIMEWAIT状態です。 • **INP_ONESBCAST**–ブロードキャストパケットを送信します。 • **INP_DROPPED**–プロトコルがフラグを廃棄しました。 • **INP_SOCKREF**–Strongソケットを参照します。 • **INP_DONTBLOCK**–インタネットPCBの同期をブロックしません。 • **N/A**–上記以外のフラグです。
TTL	インタネットPCBのTTLです。
Send VRF	パケットが送信されたVRFです。 このフィールドは現在のソフトウェアバージョンでサポートしていません。
Receive VRF	パケットが受信されたVRFです。 このフィールドは現在のソフトウェアバージョンでサポートしていません。

14.1.5 display tcp

Syntax

display tcp [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

slot *slot-number*: 指定した IRF スタックメンバ装置の TCP 接続の概要情報を表示します。*slot-number* は IRF スタックメンバ装置の ID を指定します。指定しない場合、すべてのメンバ装置の TCP 接続の概要情報を表示します。

説明

display tcp コマンドは TCP 接続の概要情報を表示します。

TCP 接続の概要情報はローカル IP アドレス、ローカルポート番号、ピアの IP アドレス、ピアのポート番号、TCP 接続情報が含まれます。

例

TCP 接続の概要情報を表示します。

<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
```

表 14-4 コマンド出力

フィールド	説明
*	TCP接続が認証を使用することを示します。
Local Addr:port	ローカルIPアドレスとポート番号です。
Foreign Addr:port	ピアのIPアドレスとポート番号です。
State	TCP接続状態です。
PCB	PCBインデックスです。

14.1.6 display tcp statistics

Syntax

display tcp statistics [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

slot *slot-number*: 指定した IRF スタックメンバ装置の TCP トラフィックの統計情報を表示します。*slot-number* は IRF スタックメンバ装置の ID を指定します。指定しない場合、すべてのメンバ装置の TCP トラフィックの統計情報を表示します。

説明

display tcp statistics コマンドは TCP トラフィックの統計情報を表示します。

TCP トラフィックの統計情報は受信 TCP パケット、送信 TCP パケット、Syncache/syncookie が含まれます。

例

TCP トラフィックの統計情報を表示します。

<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
```

関連コマンド

reset tcp statistics

14.1.7 display tcp verbose

Syntax

display tcp verbose [**slot** *slot-number* [**pcb** *pcb-index*]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

pcb *pcb-index*: 指定した PCB の TCP 接続の詳細情報を表示します。*pcb-index* は PCB のインデックスを指定します。設定範囲は 16 進数で 1～ffffffffffffffff です。

slot *slot-number*: 指定した IRF スタックメンバ装置の TCP 接続の詳細情報を表示します。*slot-number* は IRF スタックメンバ装置の ID を指定します。指定しない場合、すべてのメンバ装置の TCP 接続の詳細情報を表示します。

説明

display tcp verbose コマンドは TCP 接続の詳細情報を表示します。

TCP 接続の詳細情報はソケット作成のタスク名、状態、オプション、タイプ、プロトコル番号、送信元 IP アドレス、送信元ポート番号、宛先 IP アドレス、宛先ポート番号、接続状態が含まれます。

例

TCP 接続の詳細情報を表示します。

<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
```

表 14-5 コマンド出力

フィールド	説明
TCP inpcb number	TCP IP PCBの数です。
tcpcb number	TCP PCBの数です。 TCP接続の状態がTIME_WAITである場合、表示されません。
Creator	ソケットを作成したタスク名です。括弧の数はタスク名の処理番号です。
State	ソケットの状態です。
Options	ソケットのオプションです。
Error	エラーコードです。

Receiving buffer
(cc/hiwat/lowat/state)
	以下の順番で受信バッファ情報を表示します。
	• **cc**–使用されているバッファ空間です。
	• **hiwat**–最大バッファ空間です。
	• **lowat**–最小バッファ空間です。
	• **state**–バッファ状態です。
	  • **CANTSENDMORE**–ピアにデータを送信できません。
	  • **CANTRCVMORE**–ピアからデータを受信できません。
	  • **RCVATMARK**–タグを受信しています。
	  • **N/A**–上記以外の状態です。

Sending buffer
(cc/hiwat/lowat/state)
	以下の順番で送信バッファ情報を表示します。
	• **cc**–使用されているバッファ空間です。
	• **hiwat**–最大バッファ空間です。
	• **lowat**–最小バッファ空間です。
	• **state**–バッファ状態です。
	  • **CANTSENDMORE**–ピアにデータを送信できません。
	  • **CANTRCVMORE**–ピアからデータを受信できません。
	  • **RCVATMARK**–タグを受信しています。
	  • **N/A**–上記以外の状態です。

フィールド	説明
Type	ソケットタイプです。 ● **1**–SOCK_STREAMです。このソケットはストリームの信頼できる転送を提供するためにTCPを使用します。 ● **2**–SOCK_DGRAMです。このソケットはデータグラムの転送を提供するためにUDPを使用します。 ● **3**–SOCK_RAWです。このソケットはアプリケーションが次の上位レイヤプロトコルヘッダを変更することを許可します。 ● **N/A**–上記以外のタイプです。
Protocol	ソケットを使用したプロトコル数です。
Connection info	送信元IPアドレス、送信元ポート番号、宛先IPアドレス、宛先ポート番号です。

フィールド	説明
Inpcb flags	インタネットPCBのフラグです。 • **INP_RECVOPTS**–IPオプションを受信します。 • **INP_RECVRETOPTS**–応答したIPオプションを受信します。 • **INP_RECVDSTADDR**–宛先IPアドレスを受信します。 • **INP_HDRINCL**–IPヘッダ全体を提供します。 • **INP_REUSEADDR**–IPアドレスを再利用します。 • **INP_REUSEPORT**–ポート番号を再利用します。 • **INP_ANONPORT**–ポート番号が指定されていません。 • **INP_RECVIF**–パケットの入力インタフェースを記録します。 • **INP_RECVTTL**–パケットのTTLを受信します。このフラグはUDPとRawIPのみサポートします。 • **INP_DONTFRAG**–DF(Don't Fragment)フラグを設定します。 • **INP_ROUTER_ALERT**–ルータで警告オプションのパケットを受信します。このフラグはRawIPのみサポートします。 • **INP_PROTOCOL_PACKET**–プロトコルパケットを識別します。 • **INP_RCVVLANID**–パケットのVLAN IDを受信します。このフラグはUDPとRawIPのみサポートします。 • **INP_RCVMACADDR**–フレームのMACアドレスを受信します。 • **INP_RECVTOS**–パケットのTOSを受信します。このフラグはUDPとRawIPのみサポートします。 • **INP_SYNCPCB**–インタネットPCBが同期されるまで待ちます。 • **N/A**–上記以外のフラグです。
Inpcb extflag	インタネットPCBの拡張フラグです。 • **INP_EXTRCVPVCIDX**–受信したパケットのPVCインデックスを記録します。 • **INP_RCVPWID**–受信したパケットのPW IDを記録します。 • **INP_EXTDONTDROP**–受信したパケットを廃棄しません。 • **N/A**–上記以外のフラグです。

フィールド	説明
Inpcb vflag	インタネットPCBのIPバージョンフラグです。 • **INP_IPV4**–IPv4プロトコルです。 • **INP_TIMEWAIT**–TIMEWAIT状態です。 • **INP_ONESBCAST**–ブロードキャストパケットを送信します。 • **INP_DROPPED**–プロトコルがフラグを廃棄しました。 • **INP_SOCKREF**–Strongソケットを参照します。 • **INP_DONTBLOCK**–インタネットPCBの同期をブロックしません。 • **N/A**–上記以外のフラグです。
TTL	インタネットPCBのTTLです。
TCP options	TCPオプションです。 • **TF_MD5SIG**–MD5署名を有効にします。 • **TF_NODELAY**–TCP内の送信データをバッファするNagleアルゴリズムを無効にします。 • **TF_NOOPT**–TCPオプションがありません。 • **TF_NOPUSH**–TCPバッファにバッファされるセグメントが満杯になるまでTCPデータの送信を強制的に遅延させます。 • **TF_BINDFOREIGNADDR**–ピアのIPアドレスを割り当てます。 • **TF_NSR**–TCP NSRを有効にします。 • **TF_REQ_SCALE**–TCPウィンドウのscaleオプションを有効にします。 • **TF_REQ_TSTMP**–タイムスタンプオプションを有効にします。 • **TF_SACK_PERMIT**–TCP selective acknowledgementオプションを有効にします。 • **TF_ENHANCED_AUTH**–拡張認証オプションを有効にします。
NSR state	TCP接続の状態です。括弧の数は接続の役割です。 • **M**–メイン接続です。 • **S**–Standby接続です。
Send VRF	パケットが送信されたVRFです。 このフィールドは現在のソフトウェアバージョンでサポートしていません。

フィールド	説明
Receive VRF	パケットが受信されたVRFです。 このフィールドは現在のソフトウェアバージョンでサポートしていません。

14.1.8 display udp

Syntax

display udp [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

slot *slot-number*: 指定したIRFスタックメンバ装置のUDP接続の概要情報を表示します。*slot-number* は IRF スタックメンバ装置の ID を指定します。指定しない場合、すべてのメンバ装置の UDP 接続の概要情報を表示します。

説明

display udp コマンドは UDP 接続の概要情報を表示します。

UDP 接続の概要情報はローカル IP アドレス、ローカルポート番号、ピアの IP アドレス、ピアのポート番号が含まれます。

例

UDP 接続の概要情報を表示します。

<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
```

表 14-6 コマンド出力

フィールド	説明
Local Addr:port	ローカルIPアドレスとポート番号です。
Foreign Addr:port	ピアのIPアドレスとポート番号です。

フィールド	説明
PCB	PCBインデックスです。

14.1.9 display udp statistics

Syntax

display udp statistics [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

slot *slot-number*: 指定したIRFスタックメンバ装置のUDPトラフィックの統計情報を表示します。*slot-number* は IRF スタックメンバ装置の ID を指定します。指定しない場合、すべてのメンバ装置の UDP トラフィックの統計情報を表示します。

説明

display udp statistics コマンドは UDP トラフィックの統計情報を表示します

UDP トラフィックの統計情報は受信 UDP パケット、送信 UDP パケットが含まれます。

例

UDP トラフィックの統計情報を表示します。

<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
```

関連コマンド

reset udp statistics

14.1.10 display udp verbose

Syntax

display udp verbose [**slot** *slot-number* [**pcb** *pcb-index*]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

pcb *pcb-index*: 指定した PCB の UDP 接続の詳細情報を表示します。*pcb-index* は PCB のインデックスを指定します。設定範囲は 16 進数で 1～ffffffffffffffff です。

slot *slot-number*: 指定した IRF スタックメンバ装置の UDP 接続の詳細情報を表示します。*slot-number* は IRF スタックメンバ装置の ID を指定します。指定しない場合、すべてのメンバ装置の UDP 接続の詳細情報を表示します。

説明

display udp verbose コマンドは UDP 接続の詳細情報を表示します。

UDP 接続の詳細情報は UDP 接続のソケット作成のタスク名、状態、オプション、タイプ、プロトコル番号、送信元 IP アドレス、送信元ポート番号、宛先 IP アドレス、宛先ポート番号が含まれます。

例

UDP 接続の詳細情報を表示します。

<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
```

表 14-7 コマンド出力

フィールド	説明
Total UDP socket number	UDPソケットの総数です。
Creator	ソケットを作成したタスク名です。括弧の数はタスク名の処理番号です。
State	ソケットの状態です。
Options	ソケットのオプションです。
Error	エラーコードです。
Receiving buffer(cc/hiwat/lowat/drop/state)	以下の順番で受信バッファ情報を表示します。 • **cc**–使用されているバッファ空間です。 • **hiwat**–最大バッファ空間です。 • **lowat**–最小バッファ空間です。 • **drop**–廃棄されたパケット数です。 • **state**–バッファ状態です。 　• **CANTSENDMORE**–ピアにデータを送信できません。 　• **CANTRCVMORE**–ピアからデータを受信できません。 　• **RCVATMARK**–タグを受信しています。 　• **N/A**–上記以外の状態です。
Sending buffer(cc/hiwat/lowat/state)	以下の順番で送信バッファ情報を表示します。 • **cc**–使用されているバッファ空間です。 • **hiwat**–最大バッファ空間です。 • **lowat**–最小バッファ空間です。 • **state**–バッファ状態です。 　• **CANTSENDMORE**–ピアにデータを送信できません。 　• **CANTRCVMORE**–ピアからデータを受信できません。 　• **RCVATMARK**–タグを受信しています。 　• **N/A**–上記以外の状態です。

フィールド	説明
Type	ソケットタイプです。 • **1**–SOCK_STREAMです。このソケットはストリームの信頼できる転送を提供するためにTCPを使用します。 • **2**–SOCK_DGRAMです。このソケットはデータグラムの転送を提供するためにUDPを使用します。 • **3**–SOCK_RAWです。このソケットはアプリケーションが次の上位レイヤプロトコルヘッダを変更することを許可します。 • **N/A**–上記以外のタイプです。
Protocol	ソケットを使用したプロトコル数です。
Inpcb flags	インタネットPCBのフラグです。 • **INP_RECVOPTS**–IPオプションを受信します。 • **INP_RECVRETOPTS**–応答したIPオプションを受信します。 • **INP_RECVDSTADDR**–宛先IPアドレスを受信します。 • **INP_HDRINCL**–全体のIPヘッダを提供します。 • **INP_REUSEADDR**–IPアドレスを再利用します。 • **INP_REUSEPORT**–ポート番号を再利用します。 • **INP_ANONPORT**–ポート番号が指定されていません。 • **INP_RECVIF**–パケットの入力インタフェースを記録します。 • **INP_RECVTTL**–パケットのTTLを受信します。このフラグはUDPとRawIPのみサポートします。 • **INP_DONTFRAG**–DF(Don't Fragment)フラグを設定します。 • **INP_ROUTER_ALERT**–ルータで警告オプションのパケットを受信します。このフラグはRawIPのみサポートします。 • **INP_PROTOCOL_PACKET**–プロトコルパケットを識別します。 • **INP_RCVVLANID**–パケットのVLAN IDを受信します。このフラグはUDPとRawIPのみサポートします。 • **INP_RCVMACADDR**–フレームのMACアドレスを受信します。 • **INP_RECVTOS**–パケットのTOSを受信します。このフラグはUDPとRawIPのみサポートします。 • **INP_SYNCPCB**–インタネットPCBが同期されるまで待ちます。 • **N/A**–上記以外のフラグです。

フィールド	説明
Inpcb extflag	インタネットPCBの拡張フラグです。 • **INP_EXTRCVPVCIDX**–受信したパケットのPVCインデックスを記録します。 • **INP_RCVPWID**–受信したパケットのPW IDを記録します。 • **N/A**–上記以外のフラグです。
Inpcb vflag	インタネットPCBのIPバージョンフラグです。 • **INP_IPV4**–IPv4プロトコルです。 • **INP_TIMEWAIT**–TIMEWAIT状態です。 • **INP_ONESBCAST**–ブロードキャストパケットを送信します。 • **INP_DROPPED**–プロトコルがフラグを廃棄しました。 • **INP_SOCKREF**–Strongソケットを参照します。 • **INP_DONTBLOCK**–インタネットPCBの同期をブロックしません。 • **N/A**–上記以外のフラグです。
TTL	インタネットPCBのTTLです。
Send VRF	パケットが送信されたVRFです。 このフィールドは現在のソフトウェアバージョンでサポートしていません。
Receive VRF	パケットが受信されたVRFです。 このフィールドは現在のソフトウェアバージョンでサポートしていません。

14.1.11 ip forward-broadcast

Syntax

ip forward-broadcast

undo ip forward-broadcast

デフォルト

無効

View

Interface view

定義済みユーザロール

network-admin

説明

ip forward-broadcast コマンドは直接接続されたネットワークにダイレクトブロードキャストパケットの送受信をインタフェースで有効にします。

undo ip forward-broadcast コマンドは直接接続されたネットワークにダイレクトブロードキャストパケットの送受信をインタフェースで無効にします。

ダイレクトブロードキャストパケットは指定したネットワークのすべてのホストに送信されるブロードキャストパケットのことです。ダイレクトブロードキャストパケットの宛先 IP アドレスのネットワーク ID は宛先ネットワークを識別し、ホスト ID は値がすべて 1 です。

インタフェースが、ダイレクトブロードキャストをネットワークに転送することを許可した場合、ハッカーがネットワークに攻撃をする可能性があります。しかし、特定のシナリオでは、インタフェースは UDP ヘルパー機能、Wake on LAN をサポートするため、ダイレクトブロードキャストパケットの送受信を行う必要があります。

このコマンドは UDP ヘルパー機能をサポートするため、直接接続されたネットワークにダイレクトブロードキャストパケットの送受信をインタフェースで有効にします。UDP ヘルパー機能はダイレクトブロードキャストパケットをユニキャストパケットに変換し、特定のサーバに転送します。

このコマンドは Wake on LAN をサポートするため、直接接続されたネットワーク向けに、別のサブネットから受信したダイレクトブロードキャストパケットの転送をインタフェースで有効にします。Wake on LAN は宛先ネットワークのホストを起動するためにダイレクトブロードキャストパケットを送信します。

例

直接接続されたネットワークにダイレクトブロードキャストパケットの送受信を VLAN インタフェース 2 で有効にします。

```
<Switch> system-view
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip forward-broadcast
```

14.1.12 ip icmp error-interval

Syntax

ip icmp error-interval *interval* [*bucketsize*]

undo ip icmp error-interval

デフォルト

最大バケットサイズは最大 10 トークンで、バケットに 100 ミリ秒の間隔でトークンが配置されます。

View

System view

定義済みユーザロール

network-admin

パラメータ

interval: バケットに到着するトークンの間隔を設定します。設定範囲は 0～2147483647 です。ICMP レートリミットを無効にする場合 0 に設定します。

bucketsize: 最大トークンバケットサイズを指定します。設定範囲は 1～200 です。

説明

ip icmp error-interval コマンドは ICMP エラーメッセージがトークンバケット（bucket）に到着する間隔と、トークンパケットサイズを設定します。つまり ICMP レートリミットを設定します。

undo ip icmp error-interval コマンドはデフォルトに戻します。

このコマンドは ICMP エラーメッセージが送信されるレートを制限します。このコマンドを使用することで、ネットワークの衝突が発生する可能性のある短い時間内に過度の ICMP エラーメッセージを送信することを防ぐことができます。トークンバケットアルゴリズムは 1 つの ICMP エラーメッセージを表す 1 つのトークンが用いられます。

バケットに入ることができるトークンが最大に到達するまでトークンは指定された間隔でバケットに配置されます。

ICMP エラーメッセージが送信されるとき、バケットからトークンがバケットから取り除かれます。バケットが空の時、新しいトークンがバケットに配置されるまで ICMP エラーメッセージは送信されません。

例

ICMP エラーメッセージの送信間隔を 200 ミリ秒、トークンのバケットサイズを 40 に設定します。

<Switch> system-view

[Switch] ip icmp error-interval 200 40

14.1.13 ip mtu

Syntax

ip mtu *mtu-size*

undo ip mtu

デフォルト

設定なし

View

Interface view

定義済みユーザロール

network-admin

パラメータ

mtu-size: MTU を指定します。設定範囲は 128～1500 バイトです。

説明

ip mtu コマンドはインタフェースを通過する IPv4 パケットの MTU を設定します。

undo ip mtu コマンドはデフォルトに戻します。

出力インタフェースの MTU を超過したとき、装置は以下のどちらか 1 つを処理します。

- パケットのフラグメントが禁止されている場合、装置はパケットを廃棄します。
- パケットのフラグメントが許可されている場合、装置はパケットを分割し、フラグメントしたパケットを転送します。

フラグメントと再構築は、システムリソースを消費します。フラグメントを防ぐため、ネットワーク環境にもとづいて、適切にインタフェースの MTU サイズを設定します。

例

VLAN インタフェース 100 の MTU を 1280 バイトに設定します。

<Switch> system-view

[Switch] interface vlan-interface 100

[Switch-Vlan-interface100] ip mtu 1280

⚠ 注意：

自装置が発信元となるパケットに対してフラグメントの動作をします。
自装置が中継するパケットに対しては、IPv4 パケットが出力インタフェースの MTU サイズを超えたとき、装置はパケットを廃棄します。

14.1.14 ip redirects enable

Syntax

ip redirects enable

undo ip redirects enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

ip redirects enable コマンドは ICMP リダイレクトメッセージの送信を有効にします。

undo ip redirects enable コマンドは ICMP リダイレクトメッセージの送信を無効にします。

ICMP リダイレクトパケット機能はホストの管理を簡略化し、最適なルートを見つけ出すために、ホストが正しいルーティングテーブルを徐々に確立することができます。

ホストはすべてのパケットをデフォルトゲートウェイに送信するため、デフォルトルートへのルートのみがあります。デフォルトゲートウェイは、以降のパケットを送信するために正しいネクストホップを再選択するよう、以下の条件で、送信元の装置に ICMP リダイレクトパケットを送信します。

- 受信インタフェースと送信インタフェースが同じです。
- 選択したルートが ICMP リダイレクトパケットで作成されていない、あるいは変更されていません。
- 選択されたルートが 0.0.0.0 へのルートではありません。
- 受信したパケットに送信元ルートオプションがありません。

例

ICMP リダイレクトメッセージの送信を有効にします。

<Switch> system-view

[Switch] ip redirects enable

14.1.15 ip ttl-expires enable

Syntax

ip ttl-expires enable

undo ip ttl-expires enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

ip ttl-expires enable コマンドは ICMP タイムアウトパケットの送信を有効にします。

undo ip ttl-expires enable コマンドは ICMP タイムアウトパケットの送信を無効にします。

装置は以下のルールによって ICMP タイムアウトパケットを送信します。

- パケットの宛先が装置自身ではなく、パケットの TTL フィールドが 1 であるとき、装置は以下の状態の場合、送信元に ICMP TTL Expired の ICMP エラーパケットを送信します。
  - パケットの宛先が装置自身ではありません。
  - パケットの TTL フィールドが 1 です。
- 宛先が装置自身である IP データグラムの最初のフラグメントパケットを、装置が受信したとき、タイマを始動します。データグラムのすべてのフラグメントパケットを受信する前にタイマが満了した場合、装置は ICMP Fragment Reassembly Timeout の ICMP エラーパケットを送信します。

ICMP タイムアウトパケットの送信を無効にした装置は ICMP TTL Expired の ICMP エラーパケットを送信しませんが、ICMP Fragment Reassembly Timeout のメッセージを送信します。

例

ICMP タイムアウトパケットの送信を有効にします。

<Switch> system-view

[Switch] ip ttl-expires enable

14.1.16 ip unreachables enable

Syntax

ip unreachables enable

undo ip unreachables enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

ip unreachables enable コマンドは ICMP 宛先到達不能メッセージの送信を有効にします。

undo ip unreachables enable コマンドは ICMP 宛先到達不能メッセージの送信を無効にします。

装置は以下のルールで宛先到達不能メッセージを送信します。

- 以下の状態の場合、装置は Network Unreachable の ICMP エラーパケットを送信元に送信します。
  - 受信したパケットがルートに一致しません。
  - ルーティングテーブルにデフォルトルートがありません。
- 以下の状態の場合、装置は Protocol Unreachable の ICMP エラーパケットを送信元に送信します。
  - 受信したパケットの宛先が装置です。
  - パケットのトランスポート層プロトコルが装置でサポートしていません。
- 以下の状態の場合、装置は ICMP Port Unreachable の ICMP エラーパケットを送信元に送信します。
  - 受信したパケットの宛先が装置です。
  - パケットのポート番号が実行中のプロセスとマッチしません。
- 以下の状態の場合、装置は Source Routing Failure の ICMP エラーパケットを送信元に送信します。
  - パケットを送信するために送信元が、Strict Source Routing を使用しています。
  - 中継装置で、送信元により指定されたネクストホップが直接接続されていないことを検出しました。
- 以下の状態の場合、装置は Fragmentation Needed and Don't Fragment-Set の ICMP エラーパケットを送信元に送信します。
  - 送信インタフェースの MTU がパケットより小さいです。
  - パケットに DF セット(フラグメント禁止)が付与されています。

例

ICMP 宛先到達不能メッセージの送信を有効にします。

<Switch> system-view

[Switch] ip unreachables enable

14.1.17 reset ip statistics

Syntax

reset ip statistics [**slot** *slot-number*]

View

User view

定義済みユーザロール

network-admin

パラメータ

slot *slot-number*: 指定した IRF スタックメンバ装置の IP トラフィックの統計情報を削除します。*slot-number* は IRF スタックメンバ装置の ID を指定します。指定しない場合、すべてのメンバ装置の IP トラフィックの統計情報を削除します。

説明

reset ip statistics コマンドは IP トラフィックの統計情報を削除します。

新しく一定期間内の IP トラフィックの統計情報を取得する場合、このコマンドを使用し、最初に既存の IP トラフィックの統計情報を削除します。

例

IP トラフィックの統計情報を削除します。

<Switch> reset ip statistics

関連コマンド

- **display ip interface**
- **display ip statistics**

14.1.18 reset tcp statistics

Syntax

reset tcp statistics

View

User view

定義済みユーザロール

network-admin

説明

reset tcp statistics コマンドは TCP トラフィックの統計情報を削除します。

例

TCP トラフィックの統計情報を削除します。

<Switch> reset tcp statistics

関連コマンド

display tcp statistics

14.1.19 reset udp statistics

Syntax

reset udp statistics

View

User view

定義済みユーザロール

network-admin

説明

reset udp statistics コマンドは UDP トラフィックの統計情報を削除します。

例

UDP トラフィックの統計情報を削除します。

<Switch> reset udp statistics

関連コマンド

display udp statistics

14.1.20 tcp path-mtu-discovery

Syntax

tcp path-mtu-discovery [**aging** *age-time* | **no-aging**]

undo tcp path-mtu-discovery

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

パラメータ

aging *age-time*: path MTU のエージング時間を設定します。設定時間は 10～30 分です。デフォルトは 10 分です。

no-aging: path MTU をエージアウトしません。

説明

tcp path-mtu-discovery コマンドは TCP path MTU discovery を有効にします。

undo tcp path-mtu-discovery コマンドは TCP path MTU discovery を無効にします。

TCP path MTU discovery を有効にしたのち、すべての新しい TCP 接続は、path MTU を検出します。装置は IP のフラグメントを発生させないように MSS の計算をするため、path MTU を使用します。

TCP path MTU discovery を無効にしたのち、システムはすべての path MTU タイマを停止します。その後に確立された TCP 接続は path MTU を検出しませんが、以前に確立された TCP 接続は path MTU を検出することができます。

例

TCP path MTU discovery を有効にし、path MTU のエージング時間を 20 分に設定します。

<Switch> system-view

[Switch] tcp path-mtu-discovery aging 20

14.1.21 tcp timer fin-timeout

Syntax

tcp timer fin-timeout *time-value*

undo tcp timer fin-timeout

デフォルト

675 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

time-value: TCP FIN wait タイマを指定します。設定範囲は 76～3600 秒です。

説明

tcp timer fin-timeout コマンドは TCP FIN wait タイマを設定します。

undo tcp timer fin-timeout コマンドはデフォルトに戻します。

状態が FIN_WAIT_2 に変更したとき、TCP は TCP FIN wait タイマを開始します。時間内に FIN パケットを受信しない場合、TCP 接続が終了します。

FIN パケットを受信した場合、TCP は TIME_WAIT に接続状態を変更します。non-FIN パケットを受信すると、TCP はタイマを再スタートし、TCP はタイマが満了したとき TCP 接続を切断します。

例

TCP FIN wait タイマを 800 秒に設定します。

<Switch> system-view

[Switch] tcp timer fin-timeout 800

14.1.22 tcp timer syn-timeout

Syntax

tcp timer syn-timeout *time-value*

undo tcp timer syn-timeout

デフォルト

75 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

time-value: TCP SYN wait タイマを指定します。設定範囲は 2～600 秒です。

説明

tcp timer syn-timeout コマンドは TCP SYN wait タイマを設定します。

undo tcp timer syn-timeout コマンドはデフォルトに戻します。

TCP は SYN パケットを送信した後、SYN wait タイマを開始します。SYN wait タイマの間隔以内にパケットを受信しない場合、TCP は接続の確立に失敗します。

例

TCP SYN wait タイマを 80 秒に設定します。

<Switch> system-view

[Switch] tcp timer syn-timeout 80

14.1.23 tcp window

Syntax

tcp window *window-size*

undo tcp window

デフォルト

63 KB

View

System view

定義済みユーザロール

network-admin

パラメータ

window-size: TCP 受信/送信バッファのサイズを指定します。設定範囲は 1～64KB です。

説明

tcp window コマンドは TCP 受信/送信バッファのサイズを設定します。

undo tcp window コマンドはデフォルトに戻します。

例

TCP 受信/送信バッファのサイズを 3KB に設定します。

<Switch> system-view

[Switch] tcp window 3

目次

このセクションのページは **4-x-x** です。

15 章 UDP ヘルパー 15-1
15.1 UDP ヘルパー設定コマンド 15-1
15.1.1 display udp-helper interface 15-1
15.1.2 reset udp-helper statistics 15-2
15.1.3 udp-helper enable 15-3
15.1.4 udp-helper port 15-3
15.1.5 udp-helper server 15-5

15章 UDP ヘルパー

15.1 UDPヘルパー設定コマンド

15.1.1 display udp-helper interface

Syntax

display udp-helper interface *interface-type interface-number*

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface-type interface-number: インタフェースのタイプと番号を指定します。

説明

display udp-helper interface コマンドは、インタフェースで UDP ヘルパーによってブロードキャストからユニキャストに変換された情報を表示します。

このコマンドは宛先サーバと UDP ヘルパーによって UDP ブロードキャストパケットから変換されたユニキャストパケットの総数の情報を示します。

例

VLAN インタフェース 100 で UDP ヘルパーによってブロードキャストからユニキャストへの変換について情報を表示します。

<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
```

表 15-1 コマンド出力

フィールド	説明
Interface	インタフェース名です。

フィールド	説明
Server VPN instance	宛先サーバが所属するVPNインスタンスです。 このフィールドは現在のソフトウェアバージョンでサポートしていません。
Server address	UDPパケットが転送される宛先サーバです。
Packets sent	UDPヘルパーによってブロードキャストからユニキャストに変換されたユニキャストパケット数です。

関連コマンド

- **reset udp-helper statistics**
- **udp-helper server**

15.1.2 reset udp-helper statistics

Syntax

reset udp-helper statistics

View

User view

定義済みユーザロール

network-admin

説明

reset udp-helper statistics コマンドは UDP ヘルパーによってブロードキャストからユニキャストに変換された UDP パケットの統計情報を削除します。

例

UDP ヘルパーによってブロードキャストからユニキャストに変換された UDP パケットの統計情報を削除します。

<Switch> reset udp-helper statistics

関連コマンド

display udp-helper interface

15.1.3 udp-helper enable

Syntax

udp-helper enable

undo udp-helper enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

udp-helper enable コマンドは UDP ヘルパーを有効にします。

undo udp-helper enable コマンドは UDP ヘルパーを無効にします。

インタフェースで UDP ヘルパーを適用する場合、以下のことを確認してください。

- UDP ヘルパーが有効です。
- udp-helper port コマンドで UDP ポート番号が設定されています。
- UDP ヘルパー用にインタフェースでパケット変換が設定されています。

例

UDP ヘルパーを有効にします。

<Switch> system-view

[Switch] udp-helper enable

関連コマンド

- **udp-helper port**
- **udp-helper server**

15.1.4 udp-helper port

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** }

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

port-number: UDP ポート番号を指定します。設定範囲は 1～65535 です。67、68 のポート番号を除きます。

dns: DNS パケットで使用される UDP ポート番号 53 を指定します。

netbios-ds: NetBIOS データグラム分散サービスによって使用される UDP ポート番号 138 を指定します。

netbios-ns: NetBIOS 名前サービスパケットによって使用される UDP ポート番号 137 を指定します。

tacacs: TACACS パケットによって使用される UDP ポート番号 49 を指定します。

tftp: TFTP パケットによって使用される UDP ポート番号 69 を指定します。

time: time プロトコルパケットによって使用される UDP ポート番号 37 を指定します。

説明

udp-helper port コマンドは UDP ヘルパーの UDP ポート番号を指定します。

undo udp-helper port コマンドは UDP ポート番号を削除します。

UDP ブロードキャストパケットあるいは UDP マルチキャストパケットを受信すると、UDP ヘルパーは、パケットの UDP 宛先ポート番号に一致させるため、指定された UDP ポートを使用します。

UDP ポート番号を指定するため、ポート番号あるいは対応するプロトコルを指定することができます。たとえば、**udp-helper port 53** コマンドと **udp-helper port dns** コマンドは同じ UDP ポート番号を指定します。

装置で UDP ポートを最大 256 まで指定することができます。

例

UDP ヘルパーの UDP ポート番号 100 を指定します。

<Switch> system-view

[Switch] udp-helper port 100

15.1.5 udp-helper server

Syntax

udp-helper server *ip-address* [**global**]

undo udp-helper server [*ip-address* [**global**]]

デフォルト

設定なし

View

Interface view

定義済みユーザロール

network-admin

パラメータ

ip-address: 宛先サーバの IP アドレスを指定します。ドットで区切り、10 進数で指定します。

global : 変換されたユニキャストパケットをパブリックネットワークのサーバに転送します。

説明

udp-helper server コマンドは、ブロードキャストからユニキャストに変換するために UDP ヘルパーの宛先サーバを設定します。

undo udp-helper server コマンドは、宛先サーバを削除します。

UDP ブロードキャストパケットを受信するインタフェースの宛先サーバを指定します。パケットの宛先 UDP ポート番号が UDP ヘルパーのポートに一致しない場合、UDP ヘルパーは指定したサーバにブロードキャストパケットを転送します。

インタフェースでブロードキャストパケットに変換するため、UDP ヘルパーは最大 20 のユニキャストとマルチキャストアドレスを指定することができます。

ip-address パラメータを指定しない場合、**undo udp-helper server** コマンドはインタフェースのすべての宛先サーバを削除します。

例

VLAN インタフェース 100 でブロードキャストをユニキャストに変換するために UDP ヘルパーの宛先サーバを 192.1.1.2 に設定します。

<Switch> system-view

[Switch] interface vlan-interface 100

[Switch-Vlan-interface100] udp-helper server 192.1.1.2

VLAN インタフェース 100 でブロードキャストをユニキャストに変換するために UDP ヘルパーのパブリックネットワークの宛先サーバを 192.1.1.2 に設定します。

<Switch> system-view

[Switch] interface vlan-interface 100

[Switch-Vlan-interface100] udp-helper server 192.1.1.2 global

関連コマンド

display udp-helper interface

目次

このセクションのページは **4-x-x** です。

16 章 IPv6 の基本.....16-1
16.1 IPv6 の基本設定コマンド.....16-1
16.1.1 display ipv6 fib.....16-1
16.1.2 display ipv6 interface.....16-2
16.1.3 display ipv6 neighbors.....16-8
16.1.4 display ipv6 neighbors count.....16-10
16.1.5 display ipv6 neighbors vpn-instance.....16-11
16.1.6 display ipv6 pathmtu.....16-13
16.1.7 display ipv6 rawip.....16-14
16.1.8 display ipv6 rawip verbose.....16-15
16.1.9 display ipv6 statistics.....16-19
16.1.10 display ipv6 tcp.....16-21
16.1.11 display ipv6 tcp verbose.....16-22
16.1.12 display ipv6 udp.....16-28
16.1.13 display ipv6 udp verbose.....16-29
16.1.14 ipv6 address.....16-33
16.1.15 ipv6 address anycast.....16-34
16.1.16 ipv6 address auto.....16-35
16.1.17 ipv6 address auto link-local.....16-36
16.1.18 ipv6 address eui-64.....16-38
16.1.19 ipv6 address link-local.....16-39
16.1.20 ipv6 hop-limit.....16-40
16.1.21 ipv6 hoplimit-expires enable.....16-41
16.1.22 ipv6 icmpv6 error-interval.....16-41
16.1.23 ipv6 icmpv6 multicast-echo-reply enable.....16-43
16.1.24 ipv6 mtu.....16-43
16.1.25 ipv6 nd autoconfig managed-address-flag.....16-44
16.1.26 ipv6 nd autoconfig other-flag.....16-45
16.1.27 ipv6 nd dad attempts.....16-46
16.1.28 ipv6 nd ns retrans-timer.....16-47
16.1.29 ipv6 nd nud reachable-time.....16-48
16.1.30 ipv6 nd ra halt.....16-49
16.1.31 ipv6 nd ra interval.....16-50
16.1.32 ipv6 nd ra prefix.....16-51
16.1.33 ipv6 nd ra router-lifetime.....16-52
16.1.34 ipv6 neighbor.....16-53

16.1.35 ipv6 neighbor stale-aging....16-55
16.1.36 ipv6 neighbors max-learning-num 16-56
16.1.37 ipv6 pathmtu....16-57
16.1.38 ipv6 pathmtu age 16-58
16.1.39 ipv6 unreachables enable....16-59
16.1.40 reset ipv6 neighbors....16-59
16.1.41 reset ipv6 pathmtu 16-61
16.1.42 reset ipv6 statistics....16-61

16章 IPv6 の基本

16.1 IPv6の基本設定コマンド

16.1.1 display ipv6 fib

Syntax

display ipv6 fib [*ipv6-address* [*prefix-length*]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ipv6-address: IPv6 アドレスを指定します。指定しない場合、すべての IPv6 FIB エントリを表示します。

prefix-length: IPv6 アドレスのプレフィックス長を指定します。設定範囲は 0～128 です。指定しない場合、ロンゲストマッチに従う IPv6 FIB エントリを表示します。つまり、もっとも長いマスク長に一致する IPv6 FIB エントリを表示します。

説明

display ipv6 fib コマンドは IPv6 FIB エントリを表示します。

例

パブリックネットワークのすべての IPv6 FIB エントリを表示します。

<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
```

表 16-1 コマンド出力

フィールド	説明
Destination count	宛先アドレスの総数です。
FIB entry count	IPv6 FIBエントリの総数です。
Destination	宛先アドレスです。
Prefix length	宛先アドレスのプレフィックス長です。
Nexthop	ネクストホップです。
Flags	ルートフラグです。 • **U**–使用可能なルートです。 • **G**–ゲートウェイルートです。 • **H**–ホストルートです。 • **B**–ブラックホールルートです。 • **D**–ダイナミックルートです。 • **S**–スタティックルートです。 • **R**–中継ルートです。 • **F**– fastルート変更です。
Time stamp	IPv6 FIBエントリが作成された時間です。
Label	内部MPLSラベルです。
Interface	出力インタフェースです。
Token	ラベルスイッチパスインデックス番号です。

16.1.2 display ipv6 interface

Syntax

display ipv6 interface [*interface-type* [*interface-number*]] [**brief**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface-type: インタフェースのタイプを指定します。

interface-number: インタフェースの番号を指定します。

brief: 概要情報を表示します。物理状態、リンクレイヤプロトコル、IPv6 アドレスを含む概要情報を表示します。指定しない場合、IPv6 の設定、動作情報、IPv6 パケットの統計情報を含む詳細情報を表示します。

説明

display ipv6 interface コマンドは IPv6 インタフェース情報を表示します。

インタフェースを指定しない場合、すべてのインタフェースの IPv6 情報を表示します。

interface-type のみを指定した場合、指定したタイプのインタフェースの IPv6 情報を表示します。

interface-type と *interface-number* の両方を指定した場合、指定したインタフェースの IPv6 情報を表示します。

例

VLAN インタフェース 2 の IPv6 情報を表示します。

<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
```

表 16-2 コマンド出力

フィールド	説明
Vlan-interface2 current state	インタフェースの物理状態です。 ● **Administratively DOWN**–**shutdown**コマンドでインタフェースがシャットダウンしています。インタフェースは運用上においてdownしています。 ● **DOWN**–インタフェースはupですが、インタフェースのすべてのポートがダウンしているため、物理状態がダウンしています。 ● **UP**–インタフェースの運用上と物理状態の両方がup状態です。
Line protocol current state	インタフェースのリンクレイヤ状態です。 ● **DOWN**–インタフェースのリンクレイヤ状態がダウンしています。 ● **UP**–インタフェースのリンクレイヤ状態がupです。

フィールド	説明
IPv6 is enabled	IPv6がインタフェースで有効です。この機能はインタフェースでIPv6アドレスが設定されたのち、自動で有効になります。
link-local address	インタフェースのリンクローカルアドレスです。
Global unicast address(es)	インタフェースのグローバルユニキャストアドレスです。 IPv6アドレスの状態です。 ● **TENTATIVE**–初期状態です。DADが実行されている、あるいはアドレスで実行されています。 ● **DUPLICATE**–アドレスがリンクで固有ではありません。 ● **PREFERRED**–アドレスが優先され、パケットの送信元アドレスあるいは宛先アドレスとして使用できます。この状態のアドレスがある場合、コマンドはアドレス状態を表示しません。 ● **DEPRECATED**–アドレスが優先された有効期限を超過していますが、有効な有効期限です。有効期限が有効ですが、新しい接続のための送信元アドレスとして使用することはできません。アドレスへのパケットは正常に処理されます。 グローバルユニキャストアドレスが手動で設定されない場合、アドレスが取得された方法を以下に示します。 ● **AUTOCFG**–ステートレスオートコンフィギュレーションです。 ● **DHCP**–DHCPv6サーバによって割り当てられました。 ● **EUI-64**–EUI-64 IPv6アドレスを手動で設定しました。 ● **RANDOM**–自動でランダムにアドレスが作成されました。 アドレスが手動でエニーキャストアドレスを設定した場合、**ANYCAST**がマーキングされます。
valid lifetime	プレフィックスを使用するオートコンフィギュレーショングローバルユニキャストアドレスがどれくらい有効であるかを指定します。
preferred lifetime	プレフィックスを使用するオートコンフィギュレーショングローバルユニキャストアドレスがどれくらい優先されるかを指定します。
Joined group address(es)	インタフェースが追加されたマルチキャストグループのアドレスです。
MTU	インタフェースのMTU（Maximum transmission unit）です

フィールド	説明
ND DAD is enabled, number of DAD attempts	DADが有効です。 ● DADが有効である場合、このフィールドはDADのNSメッセージを送信する試行回数を表示します。(**ipv6 nd dad attempts**コマンドで設定されます。) ● DADが無効である場合、このフィールドは**ND DAD is disabled.**と表示されます。DADを無効にするため、試行回数を0に設定します。
ND reachable time	隣接装置の到達可能時間です。
ND retransmit interval	NSメッセージを再転送する間隔です。
Hosts use stateless autoconfig for addresses	ホストがステートレスオートコンフィギュレーションによってIPv6アドレスを取得しました。
InReceives	エラーパケットを含むインタフェースで受信されたすべてのIPv6パケットです。
InTooShorts	受信した短すぎるIPv6パケットです。たとえば、40バイト未満のパケット長のパケットです。
InTruncatedPkts	パケットヘッダで指定されたペイロード長よりも短いパケット長を受信したIPv6パケットです。
InHopLimitExceeds	パケットヘッダで指定された、受信した制限を超えたホップ回数のIPv6パケットです。
InBadHeaders	受信した不正な基本ヘッダのIPv6パケットです。
InBadOptions	受信した不正な拡張ヘッダのIPv6パケットです。
ReasmReqds	受信したIPv6フラグメントです。
ReasmOKs	フラグメントの数ではなく、再構成されたパケット数です。
InFragDrops	特定のエラーのため、廃棄されたIPv6フラグメントです。
InFragTimeouts	規定された期間を超えてシステムバッファ内に留まって廃棄された受信IPv6フラグメントです。
OutFragFails	出力インタフェース上でフラグメントに失敗したパケットです。
InUnknownProtos	不明またはサポートされていないプロトコルタイプの受信IPv6パケットです。
InDelivers	受信したアプリケーションレイヤプロトコルで配信されたIPv6パケットです。(たとえばICMPv6、TCP、UDPです)
OutRequests	IPv6アプリケーションプロトコルによって送信されたローカルIPv6パケットです。
OutForwDatagrams	出力インタフェースによって転送されたパケットです。

フィールド	説明
InNoRoutes	該当するルートが発見されず廃棄された受信IPv6パケットです。
InTooBigErrors	PMTUの超過で廃棄された受信IPv6パケットです。
OutFragOKs	出力インタフェースでフラグメントされたパケットです。
OutFragCreates	出力インタフェースでフラグメントされたパケット数です。
InMcastPkts	インタフェースで受信したIPv6マルチキャストパケットです。
InMcastNotMembers	インタフェースが一致するマルチキャストグループに加入していないために廃棄された受信IPv6マルチキャストパケットです。
OutMcastPkts	インタフェースで送信されたIPv6マルチキャストパケットです。
InAddrErrors	無効な宛先アドレスのために廃棄されたIPv6パケットです。
InDiscards	パケットの内容のエラーではなくリソース問題のために廃棄された受信IPv6パケットです。
OutDiscards	パケットの内容のエラーではなくリソース問題のために廃棄された送信IPv6パケットです。

すべてのインタフェースの IPv6 の概要情報を表示します。

<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
```

表 16-3 コマンド出力

フィールド	説明
*down: administratively down	**shutdown**コマンドを使用してインタフェースが運用上シャットダウンしています。
(s): spoofing	インタフェースのスプーフィング属性です。 インタフェースのリンクプロトコルの状態はupですが、リンクはオンデマンドで一時的に確立されているか存在しません。
Interface	インタフェースの名前です。

フィールド	説明
Physical	インタフェースの物理状態です。 ● ***down**–**shutdown**コマンドでインタフェースがシャットダウンしています。 ● **down**–VLANのすべてのポートがダウンしているため、インタフェースがupですが物理状態はダウンしています。 ● **up**–インタフェースの運用上と物理状態がupです。
Protocol	インタフェースのリンクレイヤプロトコル状態です。 ● **down**–インタフェースのネットワークレイヤプロトコルの状態がダウンしています。 ● **up**–インタフェースのネットワークレイヤプロトコルの状態がupです。
IPv6 Address	インタフェースのIPv6アドレスです。 ● 少なくとも1つのグローバルユニキャストアドレスが設定されている場合、もっとも小さいアドレスが表示されます。 ● グローバルユニキャストアドレスが設定されていない場合、リンクローカルアドレスが表示されます。 ● アドレスが設定されていない場合、**Unassigned**と表示されます。

16.1.3 display ipv6 neighbors

Syntax

display ipv6 neighbors { { *ipv6-address* | **all** | **dynamic** | **static** } [**slot** *slot-number*] | **interface** *interface-type interface-number* | **vlan** *vlan-id* } [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ipv6-address: 情報が表示されているネイバの IPv6 アドレスを指定します。

all: パブリックネットワークとすべてのプライベートネットワークでダイナミックおよびスタティックに設定されたネイバを含むすべてのネイバの情報を表示します。

dynamic: ダイナミックに取得したすべてのネイバの情報を表示します。

static: スタティックに設定されたすべてのネイバの情報を表示します。

slot *slot-number*: メンバ ID で IRF スタックメンバ装置を指定します。指定しない場合、すべてのメンバ装置のネイバの情報を表示します。

interface *interface-type interface-number*:インタフェースのタイプと番号を指定します。

vlan *vlan-id*: ID で VLAN を指定します。VLAN ID の設定範囲は 1～4094 です。

verbose: ネイバの詳細情報を表示します。

説明

display ipv6 neighbors コマンドは IPv6 ネイバ情報を表示します。

例

すべての IPv6 ネイバ情報を表示します。

<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
```

すべての IPv6 ネイバの詳細情報を表示します。

<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
```

表 16-4 コマンド出力

フィールド	説明
IPv6 Address	ネイバのIPv6アドレスです。
Link Layer	ネイバのリンクレイヤアドレス（MACアドレス）です。
VID	ネイバに接続しているインタフェースが属しているVLANです。VLAN IDあるいはVSIインタフェースが不正である場合、**N/A**と表示します。

フィールド	説明
Interface/Link ID	ネイバに接続しているインタフェースです。リンクIDは最大8つの16進数の文字列です。
State	ネイバの状態です。 ● **INCMP**–アドレスは解決中です。ネイバのリンクレイヤアドレスは不明です。 ● **REACH**–ネイバが到達可能です。 ● **STALE**–ネイバの到達可能性が不明です。装置はネイバにデータを送信しない限り、これ以上到達可能性を検証しません。 ● **DELAY**–ネイバの到達可能性が不明です。装置は遅延後にNSメッセージを送信します。 ● **PROBE**–ネイバの到達可能性が不明です。装置はNSメッセージを送信して、ネイバの到達可能性を検証します。
Type	ネイバ情報タイプです。 ● **S**–スタティックに設定されました。 ● **D**–ダイナミックに取得されました。 ● **O**–OpenFlowモジュールから学習しました。 ● **R**–PoEあるいはPortalモジュールから学習しました。 ● **I**–無効です。
Age	ハイフン（-）はスタティックエントリです。 ダイナミックエントリでは、経過した到達可能時間が表示されます。単位は秒です。到達可能でない場合、（#）が表示されます。
Vpn-instance	VPNの名前です。VPNが設定されていない場合[No Vrf]と表示されます。
NickName	ネイバのニックネームです。最大4つの16進数の文字列です。

関連コマンド

- **ipv6 neighbor**
- **reset ipv6 neighbors**

16.1.4 display ipv6 neighbors count

Syntax

display ipv6 neighbors { { **all** | **dynamic** | **static** } [**slot** *slot-number*] | **interface** *interface-type interface-number* | **vlan** *vlan-id* } **count**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all: ダイナミックに作成およびスタティックに設定されたネイバエントリを含む、すべてのネイバエントリの総数を表示します。

dynamic: ダイナミックに作成されたネイバエントリの総数を表示します。

static: スタティックに設定されたネイバエントリの総数を表示します。

slot *slot-number*: メンバ ID で IRF スタックメンバ装置を指定します。指定しない場合、すべてのメンバ装置のネイバエントリの数を表示します。

interface *interface-type interface-number*:インタフェースのタイプと番号を指定します。

vlan *vlan-id*: ID で VLAN を指定します。VLAN ID の設定範囲は 1～4094 です。

説明

display ipv6 neighbors count コマンドはネイバエントリの数を表示します。

例

ダイナミックに作成されたネイバエントリの総数を表示します。

<Switch> display ipv6 neighbors dynamic count

```
Total number of dynamic entries: 2
```

16.1.5 display ipv6 neighbors vpn-instance

Syntax

display ipv6 neighbors vpn-instance *vpn-instance-name* [**count**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

vpn-instance-name: VPN インスタンスを名前で指定します。大文字小文字を区別し、設定範囲は 1～31 文字です。VPN は、事前に設定しておかなければなりません。

count: 指定された VPN でネイバエントリの総数を表示します。

説明

display ipv6 neighbors vpn-instance コマンドは、VPN のネイバ情報を表示します。

例

 # vpn1 のネイバ情報を表示します。

<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 -
```

表 16-5 コマンド出力

フィールド	説明
IPv6 Address	ネイバのIPv6アドレスです。
Link-layer	ネイバのリンクレイヤアドレス（MACアドレス）です。
VID	ネイバに接続しているインタフェースが属しているVLANです。
Interface	ネイバに接続しているインタフェースです。
State	ネイバの状態です。 ● **INCMP**–アドレスは解決中です。ネイバのリンクレイヤアドレスは不明です。 ● **REACH**–ネイバが到達可能です。 ● **STALE**–ネイバの到達可能性が不明です。装置はネイバにデータを送信しない限り、これ以上到達可能性を検証しません。 ● **DELAY**–ネイバの到達可能性が不明です。装置は遅延後に NS メッセージを送信します。 ● **PROBE**–ネイバの到達可能性が不明です。装置はNSメッセージを送信して、ネイバの到達可能性を検証します。

フィールド	説明
T	ネイバ情報タイプです。 ● **S**–スタティックに設定されました。 ● **D**–ダイナミックに取得されました。 ● **O**–OpenFlowモジュールから学習しました。OpenFlowは QX-S5100Gシリーズではサポートしていません。 ● **I**–無効です。
Age	ハイフン（-）はスタティックエントリです。 ダイナミックエントリでは、経過した到達可能時間が表示されます。単位は秒です。到達可能でない場合、（#）が表示されます。

16.1.6 display ipv6 pathmtu

Syntax

display ipv6 pathmtu { *ipv6-address* | { **all** | **dynamic** | **static** } [**count**] }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ipv6-address: 宛先 IPv6 アドレスの PMTU の情報を表示します。

all: パブリックネットワークのすべての PMTU の情報を表示します。

dynamic: すべてのダイナミック PMTU の情報を表示します。

static: すべてのスタティック PMTU の情報を表示します。

count: PMTU エントリの総数を表示します。

説明

display ipv6 pathmtu コマンドは IPv6 PMTU（Path MTU）情報を表示します。

例

すべての PMTU の情報を表示します。

<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
```

PMTU エントリの総数を表示します。

<Switch> display ipv6 pathmtu all count

```
Total number of entries: 3
```

表 16-6 コマンド出力

フィールド	説明
PathMTU	IPv6アドレスへのネットワークのパスMTUの値です。
Age	PMTUの存続時間です。スタティックPMTUの場合、ハイフン（-）と表示されます。
Type	PMTUのタイプです。 ● **Dynamic**–ダイナミックにネゴシエートされています。 ● **Static**–スタティックに設定されています。
Total number of entries	PMTUエントリの総数です。

関連コマンド

- **ipv6 pathmtu**
- **reset ipv6 pathmtu**

16.1.7 display ipv6 rawip

Syntax

display ipv6 rawip [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

slot *slot-number*: 指定した IRF スタックメンバ装置の IPv6 RawIP 接続の概要情報を表示します。*slot-number* は IRF スタックメンバ装置の ID を指定します。指定しない場合、すべてのメンバ装置の IPv6 RawIP 接続の概要情報を表示します。

説明

display ipv6 rawip コマンドは IPv6 RawIP 接続の概要情報を表示します。

例

IPv6 RawIP 接続の概要情報を表示します。

<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
```

表 16-7 コマンド出力

フィールド	説明
Local Addr	ローカルIPv6アドレスです。
Foreign Addr	ピアのIPv6アドレスです。
Protocol	ポート番号です。
PCB	プロトコルコントロールブロックのインデックスです。

16.1.8 display ipv6 rawip verbose

Syntax

display ipv6 rawip verbose [**slot** *slot-number* [**pcb** *pcb-index*]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

pcb *pcb-index*: 指定した PCB の IPv6 RawIP 接続の概要情報を表示します。*pcb-index* は PCB のインデックスを指定します。設定範囲は 1～16 です。

slot *slot-number*: 指定した IRF スタックメンバ装置の IPv6 RawIP 接続の詳細情報を表示します。*slot-number* は IRF スタックメンバ装置の ID を指定します。指定しない場合、すべてのメンバ装置の IPv6 RawIP 接続の詳細情報を表示します。

説明

display ipv6 rawip verbose コマンドは IPv6 RawIP 接続の詳細情報を表示します。

例

IPv6 RawIP 接続の詳細情報を表示します。

<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
```

表 16-8 コマンド出力

フィールド	説明
Total RawIP socket number	IPv6 RawIP ソケットの総数です。
Creator	ソケットを作成したタスク名です。括弧の数はタスク名の処理番号です。
State	ソケットの状態です。
Options	ソケットのオプションです。
Error	エラーコードです。

フィールド	説明

Receiving buffer (cc/hiwat/lowat/drop/state)	以下の順番で受信バッファ情報を表示します。
	• **cc**–使用されているバッファ空間です。
	• **hiwat**–最大バッファ空間です。
	• **lowat**–最小バッファ空間です。
	• **drop**–廃棄されたパケット数です。
	• **state**–バッファ状態です。
	  • **CANTSENDMORE**–ピアにデータを送信できません。
	  • **CANTRCVMORE**–ピアからデータを受信できません。
	  • **RCVATMARK**–タグを受信しています。
	  • **N/A**–上記以外の状態です。

Sending buffer(cc/hiwat/lowat/state)	以下の順番で送信バッファ情報を表示します。
	• **cc**–使用されているバッファ空間です。
	• **hiwat**–最大バッファ空間です。
	• **lowat**–最小バッファ空間です。
	• **state**–バッファ状態です。
	  • **CANTSENDMORE**–ピアにデータを送信できません。
	  • **CANTRCVMORE**–ピアからデータを受信できません。
	  • **RCVATMARK**–タグを受信しています。
	  • **N/A**–上記以外の状態です。

Type	ソケットタイプです。 • **1**–SOCK_STREAMです。このソケットはストリームの信頼できる転送を提供するためにTCPを使用します。 • **2**–SOCK_DGRAMです。このソケットはデータグラムの転送を提供するためにUDPを使用します。 • **3**–SOCK_RAWです。このソケットはアプリケーションが次の上位レイヤプロトコルヘッダを変更することを許可します。 • **N/A**–上記以外のタイプです。
Protocol	ソケットを使用しているプロトコル番号です。58はICMPを示します。
Connection info	送信元IPv6アドレスと宛先IPv6アドレスを含む接続情報です。

フィールド	説明
Inpcb flags	インタネットPCBのフラグです。 ● **INP_RECVOPTS**–IPv6オプションを受信します。 ● **INP_RECVRETOPTS**–応答したIPv6オプションを受信します。 ● **INP_RECVDSTADDR**–宛先IPv6アドレスを受信します。 ● **INP_HDRINCL**–全体のIPv6ヘッダを提供します。 ● **INP_REUSEADDR**–IPv6アドレスを再利用します。 ● **INP_REUSEPORT**–ポート番号を再利用します。 ● **INP_ANONPORT**–ポート番号が指定されていません。 ● **INP_PROTOCOL_PACKET**–プロトコルパケットを識別します。 ● **INP_RCVVLANID**–パケットのVLAN IDを受信します。このフラグはUDPとRaw IPのみサポートします。 ● **IN6P_IPV6_V6ONLY**–IPv6プロトコルスタックのみサポートします。 ● **IN6P_PKTINFO**–送信元IPv6アドレスとパケットの入力インタフェースを受信します。 ● **IN6P_HOPLIMIT**–ホップ制限を受信します。 ● **IN6P_HOPOPTS**–hop-by-hopオプション拡張ヘッダを受信します。 ● **IN6P_DSTOPTS**–宛先オプション拡張ヘッダを受信します。 ● **IN6P_RTHDR**–ルーティング拡張ヘッダを受信します。 ● **IN6P_RTHDRDSTOPTS**–ルーティング拡張ヘッダに優先する宛先オプションヘッダを受信します。 ● **IN6P_TCLASS**–パケットのトラフィッククラスを受信します。 ● **IN6P_AUTOFLOWLABEL**–自動でフローラベルを付けます。 ● **IN6P_RFC2292**–RFC2292で指定されたAPIを使用します。 ● **IN6P_MTU**–データパスに沿った各リンクのMTUの相違を検出します。TCPはこのフラグをサポートしません。 ● **INP_RCVMACADDR**–フレームのMACアドレスを受信します。 ● **INP_USEICMPSRC**–送信ICMPパケットの送信元IPv6アドレスとして指定されたIPv6アドレスを使用します。 ● **INP_SYNCPCB**–インタネットPCBが同期されるまで待ちます。 ● **N/A**–上記以外のフラグです。

フィールド	説明
Inpcb extflag	インタネットPCBの拡張フラグです。 ● **INP_EXTRCVPVCIDX**–受信したパケットのPVCインデックスの記録です。 ● **INP_RCVPWID**–受信したパケットのPW IDの記録です。 ● **INP_EXTRCVICMPERR**–ICMPエラーパケットを受信します。 ● **INP_EXTFILTER**–受信したパケットの内容をフィルタします。 ● **N/A**–上記以外のフラグです。
Inpcb vflag	インタネットPCBのIPバージョンフラグです。 ● **INP_IPV4**–IPv4プロトコルです。 ● **INP_IPV6**–IPv6プロトコルです。 ● **INP_IPV6PROTO**–IPv6プロトコルをもとにしたインタネットPCBを作成します。 ● **INP_TIMEWAIT**–TIMEWAIT状態です。 ● **INP_ONESBCAST**–ブロードキャストパケットを送信します。 ● **INP_DROPPED**–プロトコルがフラグを廃棄しました。 ● **INP_SOCKREF**–Strongソケットを参照します。 ● **INP_DONTBLOCK**–インタネットPCBの同期をブロックしません。 ● **N/A**–上記以外のフラグです。
Hop limit	インタネットPCBのホップ制限です。ホップの最小数は括弧に表示されます。
Send VRF	送信されたインスタンスです。
Receive VRF	受信されたインスタンスです。

16.1.9 display ipv6 statistics

Syntax

display ipv6 statistics [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

slot *slot-number*: 指定した IRF スタックメンバ装置の IPv6、ICMPv6 パケットの統計情報を表示します。*slot-number* は IRF スタックメンバ装置の ID を指定します。指定しない場合、すべてのメンバ装置の IPv6、ICMPv6 パケットの統計情報を表示します。

説明

display ipv6 statistics コマンドは IPv6、ICMPv6 パケットの統計情報を表示します。

例

IPv6、ICMPv6 パケットの統計情報を表示します。

<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
```

関連コマンド

reset ipv6 statistics

16.1.10 display ipv6 tcp

Syntax

display ipv6 tcp [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

slot *slot-number*: 指定した IRF スタックメンバ装置の IPv6 TCP 接続の概要情報を表示します。*slot-number* は IRF スタックメンバ装置の ID を指定します。指定しない場合、すべてのメンバ装置の IPv6 TCP 接続の概要情報を表示します。

説明

display ipv6 tcp コマンドは IPv6 TCP 接続の概要情報を表示します。

例

IPv6 TCP 接続の概要情報を表示します。

<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
```

表 16-9 コマンド出力

フィールド	説明
*	TCP接続が認証を使用することを示します。
LAddr->port	ローカルIPv6アドレスとポート番号です。
FAddr->port	ピアのIPv6アドレスとポート番号です。
State	IPv6 TCP接続状態です。
PCB	PCBインデックスです。

16.1.11 display ipv6 tcp verbose

Syntax

display ipv6 tcp verbose [**slot** *slot-number* [**pcb** *pcb-index*]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

pcb *pcb-index*: 指定した PCB の IPv6 TCP 接続の詳細情報を表示します。*pcb-index* は PCB のインデックスを指定します。設定範囲は 1～16 です。

slot *slot-number*: 指定した IRF スタックメンバ装置の IPv6 TCP 接続の詳細情報を表示します。*slot-number* は IRF スタックメンバ装置の ID を指定します。指定しない場合、すべてのメンバ装置の IPv6 TCP 接続の詳細情報を表示します。

説明

display ipv6 tcp verbose コマンドは IPv6 TCP 接続の詳細情報を表示します。

例

IPv6 TCP 接続の詳細情報を表示します。

<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
```

表 16-10 コマンド出力

フィールド	説明
TCP inpcb number	IPv6 TCPインタネットPCBの数です。
tcpcb number	IPv6 TCP PCBの数です。（TIME_WAIT状態のTCP PCBを除きます）
Creator	ソケットを作成したタスク名です。括弧の数はタスク名の処理番号です。
State	ソケットの状態です。
Options	ソケットのオプションです。
Error	エラーコードです。

フィールド	説明

Receiving buffer(cc/hiwat/lowat/state)	以下の順番で受信バッファ情報を表示します。
	• **cc**–使用されているバッファ空間です。
	• **hiwat**–最大バッファ空間です。
	• **lowat**–最小バッファ空間です。
	• **state**–バッファ状態です。
	  • **CANTSENDMORE**–ピアにデータを送信できません。
	  • **CANTRCVMORE**–ピアからデータを受信できません。
	  • **RCVATMARK**–タグを受信しています。
	  • **N/A**–上記以外の状態です。

Sending buffer(cc/hiwat/lowat/state)	以下の順番で送信バッファ情報を表示します。
	• **cc**–使用されているバッファ空間です。
	• **hiwat**–最大バッファ空間です。
	• **lowat**–最小バッファ空間です。
	• **state**–バッファ状態です。
	  • **CANTSENDMORE**–ピアにデータを送信できません。
	  • **CANTRCVMORE**–ピアからデータを受信できません。
	  • **RCVATMARK**–タグを受信しています。
	  • **N/A**–上記以外の状態です。

Type	ソケットタイプです。 • **1**–SOCK_STREAMです。このソケットはストリームの信頼できる転送を提供するためにTCPを使用します。 • **2**–SOCK_DGRAMです。このソケットはデータグラムの転送を提供するためにUDPを使用します。 • **3**–SOCK_RAWです。このソケットはアプリケーションが次の上位レイヤプロトコルヘッダを変更することを許可します。 • **N/A**–上記以外のタイプです。
Protocol	ソケットを使用したプロトコル数です。6はTCPを示します。
Connection info	送信元IPv6アドレス、送信元ポート番号、宛先IPv6アドレス、宛先ポート番号を含む接続情報です。

フィールド	説明
Inpcb flags	インタネットPCBのフラグです。 ● **INP_RECVOPTS**–IPv6オプションを受信します。 ● **INP_RECVRETOPTS**–応答したIPv6オプションを受信します。 ● **INP_RECVDSTADDR**–宛先IPv6アドレスを受信します。 ● **INP_HDRINCL**–全体のIPv6ヘッダを提供します。 ● **INP_REUSEADDR**–IPv6アドレスを再利用します。 ● **INP_REUSEPORT**–ポート番号を再利用します。 ● **INP_ANONPORT**–ポート番号が指定されていません。 ● **INP_PROTOCOL_PACKET**–プロトコルパケットを識別します。 ● **INP_RCVVLANID**–パケットのVLAN IDを受信します。このフラグはUDPとRaw IPのみサポートします。 ● **IN6P_IPV6_V6ONLY**–IPv6プロトコルスタックのみサポートします。 ● **IN6P_PKTINFO**–送信元IPv6アドレスとパケットの入力インタフェースを受信します。 ● **IN6P_HOPLIMIT**–ホップ制限を受信します。 ● **IN6P_HOPOPTS**–hop-by-hopオプション拡張ヘッダを受信します。 ● **IN6P_DSTOPTS**–宛先オプション拡張ヘッダを受信します。 ● **IN6P_RTHDR**–ルーティング拡張ヘッダを受信します。 ● **IN6P_RTHDRDSTOPTS**–ルーティング拡張ヘッダに優先する宛先オプションヘッダを受信します。 ● **IN6P_TCLASS**–パケットのトラフィッククラスを受信します。 ● **IN6P_AUTOFLOWLABEL**–自動でフローラベルを付けます。 ● **IN6P_RFC2292**–RFC2292で指定されたAPIを使用します。 ● **IN6P_MTU**–データパスに沿った各リンクのMTUの相違を検出します。TCPはこのフラグをサポートしません。 ● **INP_RCVMACADDR**–フレームのMACアドレスを受信します。 ● **INP_SYNCPCB**–インタネットPCBが同期されるまで待ちます。 ● **N/A**–上記以外のフラグです。

フィールド	説明
Inpcb extflag	インタネットPCBの拡張フラグです。 ● **INP_EXTRCVPVCIDX**–受信したパケットのPVCインデックスの記録です。 ● **INP_RCVPWID**–受信したパケットのPW IDの記録です。 ● **INP_EXTDONTDROP**–受信したパケットを廃棄しません。 ● **N/A**–上記以外のフラグです。
Inpcb vflag	インタネットPCBのIPバージョンフラグです。 ● **INP_IPV4**–IPv4プロトコルです。 ● **INP_IPV6**–IPv6プロトコルです。 ● **INP_IPV6PROTO**–IPv6プロトコルをもとにしたインタネットPCBを作成します。 ● **INP_TIMEWAIT**–TIMEWAIT状態です。 ● **INP_ONESBCAST**–ブロードキャストパケットを送信します。 ● **INP_DROPPED**–プロトコルがフラグを廃棄しました。 ● **INP_SOCKREF**– Strongソケットを参照します。 ● **INP_DONTBLOCK**–インタネットPCBの同期をブロックしません。 ● N/A–上記以外のフラグです。
Hop limit	インタネットPCBのホップ制限です。

フィールド	説明
Connection state	TCP接続状態です。 ● **CLOSED**–サーバがクライアントから切断要求の応答を受信します。 ● **LISTEN**–サーバが接続要求を待っています。 ● **SYN_SENT**–クライアントはサーバから接続要求の応答を待っています。 ● **SYN_RCVD**–サーバは接続要求を受信します。 ● **ESTABLISHED**–サーバとクライアントが接続を確立し、双方向にデータを送信することができます。 ● **CLOSE_WAIT**–サーバがクライアントから切断要求を受信します。 ● **FIN_WAIT_1**–クライアントは、サーバが切断要求に応答することを待っています。 ● **CLOSING**–サーバとクライアントが互いに切断要求を受信したとき、サーバとクライアントは、ピアからの切断応答を待っています。 ● **LAST_ACK**–サーバは、クライアントから切断要求の応答を待っています。 ● **FIN_WAIT_2**–クライアントはサーバから切断応答を受信します。 ● **TIME_WAIT**–クライアントはサーバから切断要求を受信します。

フィールド	説明
TCP options	TCPオプションです。 ● **TF_MD5SIG**–MD5署名を有効にします。 ● **TF_NODELAY**–TCP内の送信データをバッファするNagleアルゴリズムを無効にします。 ● **TF_NOOPT**– TCPオプションがありません。 ● **TF_NOPUSH**– TCPバッファにバッファされるセグメントが満杯になるまでTCPデータの送信を強制的に遅延させます。 ● **TF_BINDFOREIGNADDR**–ピアのIPアドレスを割り当てます。 ● **TF_NSR**–TCP NSRを有効にします。 ● **TF_REQ_SCALE**–TCPウィンドウのscaleオプションを有効にします。 ● **TF_REQ_TSTMP**–タイムスタンプオプションを有効にします。 ● **TF_SACK_PERMIT**–TCP selective acknowledgementオプションを有効にします。 ● **TF_ENHANCED_AUTH**–拡張認証オプションを有効にします。
NSR state	TCP接続の状態です。括弧の数は接続の役割です。 ● **M**–メイン接続です。 ● **S**–Standby接続です。
Send VRF	パケットが送信されたVRFです。
Receive VRF	VRFから受信されたパケットです。

16.1.12 display ipv6 udp

Syntax

display ipv6 udp [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

slot *slot-number*: 指定した IRF スタックメンバ装置の IPv6 UDP トラフィックの統計情報を表示します。*slot-number* は IRF スタックメンバ装置の ID を指定します。指定しない場合、すべてのメンバ装置の IPv6 UDP トラフィックの統計情報を表示します。

説明

display ipv6 udp コマンドは IPv6 UDP 接続の概要情報を表示します。

例

IPv6 UDP 接続の概要情報を表示します。

<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
```

表 16-11 コマンド出力

フィールド	説明
LAddr->port	ローカルIPv6アドレスとポート番号です。
FAddr->port	ピアのIPv6アドレスとポート番号です。
PCB	PCBインデックスです。

16.1.13 display ipv6 udp verbose

Syntax

display ipv6 udp verbose [**slot** *slot-number* [**pcb** *pcb-index*]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

pcb *pcb-index*: 指定した PCB の IPv6 UDP 接続の詳細情報を表示します。*pcb-index* は PCB のインデックスを指定します。設定範囲は 1～16 です。

slot *slot-number*: 指定した IRF スタックメンバ装置の IPv6 UDP 接続の詳細情報を表示します。*slot-number* は IRF スタックメンバ装置の ID を指定します。指定しない場合、すべてのメンバ装置の IPv6 UDP 接続の詳細情報を表示します。

説明

display ipv6 udp verbose コマンドは IPv6 UDP 接続の詳細情報を表示します。

例

IPv6 UDP 接続の詳細情報を表示します。

<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
```

表 16-12 コマンド出力

フィールド	説明
Total UDP socket number	IPv6 UDP ソケットの総数です。
Creator	ソケットを作成したタスク名です。括弧の数はタスク名の処理番号です。
State	ソケットの状態です。
Options	ソケットのオプションです。

フィールド	説明
Error	エラーコードです。

Receiving buffer(cc/hiwat/lowat/drop/state)	以下の順番で受信バッファ情報を表示します。
	• cc–使用されているバッファ空間です。
	• **hiwat**–最大バッファ空間です。
	• **lowat**–最小バッファ空間です。
	• **drop**–廃棄されたパケット数です。
	• **state**–バッファ状態です。
	  • **CANTSENDMORE**–ピアにデータを送信できません。
	  • **CANTRCVMORE**–ピアからデータを受信できません。
	  • **RCVATMARK**–タグを受信しています。
	  • **N/A**–上記以外の状態です。

Sending buffer(cc/hiwat/lowat/state)	以下の順番で送信バッファ情報を表示します。
	• **cc**–使用されているバッファ空間です。
	• **hiwat**–最大バッファ空間です。
	• **lowat**–最小バッファ空間です。
	• **state**–バッファ状態です。
	  • **CANTSENDMORE**–ピアにデータを送信できません。
	  • **CANTRCVMORE**–ピアからデータを受信できません。
	  • **RCVATMARK**–タグを受信しています。
	  • **N/A**–上記以外の状態です。

Type	ソケットタイプです。 • **1**–SOCK_STREAMです。このソケットはストリームの信頼できる転送を提供するためにTCPを使用します。 • **2**–SOCK_DGRAMです。このソケットはデータグラムの転送を提供するためにUDPを使用します。 • **3**–SOCK_RAWです。このソケットはアプリケーションが次の上位レイヤプロトコルヘッダを変更することを許可します。 • **N/A**–上記以外のタイプです。
Protocol	ソケットを使用したプロトコル数です。17はUDPを示します。
Connection info	送信元IPv6アドレス、送信元ポート番号、宛先IPv6アドレス、宛先ポート番号を含む接続情報です。

フィールド	説明
Inpcb flags	インタネットPCBのフラグです。 ● **INP_RECVOPTS**–IPv6オプションを受信します。 ● **INP_RECVRETOPTS**–応答したIPv6オプションを受信します。 ● **INP_RECVDSTADDR**–宛先IPv6アドレスを受信します。 ● **INP_HDRINCL**–全体のIPv6ヘッダを提供します。 ● **INP_REUSEADDR**–IPv6アドレスを再利用します。 ● **INP_REUSEPORT**–ポート番号を再利用します。 ● **INP_ANONPORT**–ポート番号が指定されていません。 ● **INP_PROTOCOL_PACKET**–プロトコルパケットを識別します。 ● **INP_RCVVLANID**–パケットのVLAN IDを受信します。このフラグはUDPとRaw IPのみサポートします。 ● **IN6P_IPV6_V6ONLY**–IPv6プロトコルスタックのみサポートします。 ● **IN6P_PKTINFO**–送信元IPv6アドレスとパケットの入力インタフェースを受信します。 ● **IN6P_HOPLIMIT**–ホップ制限を受信します。 ● **IN6P_HOPOPTS**–hop-by-hopオプション拡張ヘッダを受信します。 ● **IN6P_DSTOPTS**–宛先オプション拡張ヘッダを受信します。 ● **IN6P_RTHDR**–ルーティング拡張ヘッダを受信します。 ● **IN6P_RTHDRDSTOPTS**–ルーティング拡張ヘッダに優先する宛先オプションヘッダを受信します。 ● **IN6P_TCLASS**–パケットのトラフィッククラスを受信します。 ● **IN6P_AUTOFLOWLABEL**–自動でフローラベルを付けます。 ● **IN6P_RFC2292**–RFC2292で指定されたAPIを使用します。 ● **IN6P_MTU**–データパスに沿った各リンクのMTUの相違を検出します。TCPはこのフラグをサポートしません。 ● **INP_RCVMACADDR**–フレームのMACアドレスを受信します。 ● **INP_SYNCPCB**–インタネットPCBが同期されるまで待ちます。 ● **N/A**–上記以外のフラグです。

フィールド	説明
Inpcb extflag	インタネットPCBの拡張フラグです。 ● **INP_EXTRCVPVCIDX**–受信したパケットのPVCインデックスの記録です。 ● **INP_RCVPWID**–受信したパケットのPW IDの記録です。 ● **N/A**–上記以外のフラグです。
Inpcb vflag	インタネットPCBのIPバージョンフラグです。 ● **INP_IPV4**–IPv4プロトコルです。 ● **INP_IPV6**–IPv6プロトコルです。 ● **INP_IPV6PROTO**–IPv6プロトコルをもとにしたインタネットPCBを作成します。 ● **INP_TIMEWAIT**–TIMEWAIT状態です。 ● **INP_ONESBCAST**–ブロードキャストパケットを送信します。 ● **INP_DROPPED**–プロトコルがフラグを廃棄しました。 ● **INP_SOCKREF**–Strongソケットを参照します。 ● **INP_DONTBLOCK**–インタネットPCBの同期をブロックしません。 ● **N/A**–上記以外のフラグです。
Hop limit(minimum hop limit)	インタネットPCBのホップ制限です。
Send VRF	送信されたインスタンスです。
Receive VRF	受信されたインスタンスです。

16.1.14 ipv6 address

Syntax

ipv6 address { *ipv6-address prefix-length* | *ipv6-address*/*prefix-length* }

undo ipv6 address [*ipv6-address prefix-length* | *ipv6-address*/*prefix-length*]

デフォルト

設定なし

View

Interface view

定義済みユーザロール

network-admin

パラメータ

ipv6-address: IPv6 アドレスを指定します。

prefix-length: プレフィックス長を指定します。設定範囲は 1～128 です。

説明

ipv6 address コマンドはインタフェースに IPv6 グローバルユニキャストアドレスを設定します。

undo ipv6 address コマンドはインタフェースに IPv6 グローバルユニキャストアドレスを削除します。

パブリック IPv4 アドレスと同様に、ISP に IPv6 グローバルユニキャストアドレスが割り当てられます。グローバルルーティングエントリの数を削減するため、アドレスタイプはプレフィックスの集約を行うことができます。

パラメータを指定しない場合、**undo ipv6 address** コマンドはインタフェースのすべての IPv6 アドレスを削除します。

例

VLAN インタフェース 100 の IPv6 グローバルユニキャストアドレスを 2001::1、プレフィックス長を 64 に設定します。

方法 1：

<Switch> system-view

[Switch] interface vlan-interface 100

[Switch-Vlan-interface100] ipv6 address 2001::1/64

方法 2：

<Switch> system-view

[Switch] interface vlan-interface 100

[Switch-Vlan-interface100] ipv6 address 2001::1 64

16.1.15 ipv6 address anycast

Syntax

ipv6 address { *ipv6-address prefix-length* | *ipv6-address*/*prefix-length* } **anycast**

undo ipv6 address { *ipv6-address prefix-length* | *ipv6-address*/*prefix-length* } **anycast**

デフォルト

設定なし

View

Interface view

定義済みユーザロール

network-admin

パラメータ

ipv6-address: IPv6 エニーキャストアドレスを指定します。

prefix-length: プレフィックス長を指定します。設定範囲は 1～128 です。

説明

ipv6 address anycast コマンドはインタフェースの IPv6 エニーキャストアドレスを設定します。

undo ipv6 address anycast コマンドはインタフェースの IPv6 エニーキャストアドレスを削除します。

例

VLAN インタフェース 100 の IPv6 エニーキャストアドレスを 2001::1、プレフィックス長を 64 に設定します。

方法 1：

<Switch> system-view

[Switch] interface vlan-interface 100

[Switch-Vlan-interface100] ipv6 address 2001::1/64 anycast

方法 2：

<Switch> system-view

[Switch] interface vlan-interface 100

[Switch-Vlan-interface100] ipv6 address 2001::1 64 anycast

16.1.16 ipv6 address auto

Syntax

ipv6 address auto

undo ipv6 address auto

デフォルト

無効

View

Interface view

定義済みユーザロール

network-admin

説明

ipv6 address auto コマンドはインタフェースでステートレスアドレス自動設定機能を有効にします。この機能が有効の場合、インタフェースは、グローバルにユニキャストアドレスを自動で作成します。

undo ipv6 address auto コマンドはインタフェースでステートレスアドレス自動設定機能を無効にします。

ステートレス自動設定機能によって、グローバルユニキャストアドレスが生成された後、リンクローカルアドレスは、自動で生成されます。

このグローバルユニキャストアドレスと自動で作成されたリンクローカルアドレスは以下のいずれかのコマンドで削除することができます。

- **undo ipv6 address auto**
- **undo ipv6 address**

例

VLAN インタフェース 100 でステートレスアドレス自動設定機能を有効にします。

<Switch> system-view

[Switch] interface vlan-interface 100

[Switch-Vlan-interface100] ipv6 address auto

16.1.17 ipv6 address auto link-local

Syntax

ipv6 address auto link-local

undo ipv6 address auto link-local

デフォルト

インタフェースにリンクローカルアドレスは設定されていません。インタフェースにグルーバル IPv6 ユニキャストアドレスを設定したのち、リンクローカルアドレスが自動的に作成されます。

View

Interface view

定義済みユーザロール

network-admin

説明

ipv6 address auto link-local コマンドはインタフェースのリンクローカルアドレスを自動的に作成します。

undo ipv6 address auto link-local コマンドはインタフェースの自動的に生成されたリンクローカルアドレスを削除します。

リンクローカルアドレスはネイバ検出とローカルリンクのステートレス自動設定に使用されます。送信元アドレスあるいは宛先アドレスとしてリンクローカルアドレスを使用したパケットは他のリンクに転送することができません。

インタフェースに IPv6 グローバルユニキャストアドレスが設定されると、リンクローカルアドレスが自動的に作成されます。自動的に作成されたリンクローカルアドレスは、**ipv6 address auto link-local** コマンドを使用して作成されたものと同じです。

インタフェースで **undo ipv6 address auto link-local** コマンドを使用することでのみ、**ipv6 address auto link-local** コマンドで作成されたリンクローカルアドレスを削除できます。IPv6 グローバルユニキャストアドレスが設定されたインタフェースで **undo ipv6 address auto link-local** コマンドを使用しても、インタフェースはリンクローカルアドレスを保持します。

ipv6 address link-local コマンドでインタフェースの IPv6 リンクローカルアドレスを手動で割り当てることができます。手動割り当ては、自動作成より優先されます。

- 最初に自動作成を採用して次に手動割り当てを行った場合、手動で割り当てたリンクローカルアドレスが自動作成アドレスを上書きします。
- 最初に手動割り当てを行って次に自動作成を取り入れた場合、以下のことが発生します。
  - □ 自動作成されたリンクローカルアドレスは有効になりません。
  - □ インタフェースのリンクローカルアドレスは手動割り当てのものがそのまま使われます。

手動で割り当てられたアドレスを削除すると、自動作成のリンクローカルアドレスが有効になります。

例

VLAN インタフェース 100 が自動的にリンクローカルアドレスを作成するよう設定します。

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ipv6 address auto link-local
```

関連コマンド

ipv6 address link-local

16.1.18 ipv6 address eui-64

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**

デフォルト

設定なし

View

Interface view

定義済みユーザロール

network-admin

パラメータ

ipv6-address/*prefix-length*: IPv6 アドレスと IPv6 プレフィックス長を指定します。*ipv6-address* と *prefix-length* は EUI-64 IPv6 アドレスのプレフィックスを一緒に指定します。*prefix-length* の設定範囲は 1～64 です。

説明

ipv6 address eui-64 コマンドはインタフェースの EUI IPv6 アドレスを設定します。

undo ipv6 address eui-64 コマンドはインタフェースの EUI IPv6 アドレスを削除します。

EUI IPv6 アドレスは指定されたプレフィックスと自動で作成されたインタフェース ID をもとに作成されます。EUI IPv6 アドレスを表示する場合、**display ipv6 interface** コマンドを使用します。

EUI IPv6 アドレスのプレフィックス長は 64 より大きな値にすることができません。

例

VLAN インタフェース 100 の EUI IPv6 アドレスを設定します。アドレスのプレフィックスは 2001::1/64 で、インタフェース ID は装置の MAC アドレスをもとに作成されます。

方法 1：

<Switch> system-view

[Switch] interface vlan-interface 100

[Switch-Vlan-interface100] ipv6 address 2001::1/64 eui-64

方法 2：

<Switch> system-view

[Switch] interface vlan-interface 100

[Switch-Vlan-interface100] ipv6 address 2001::1 64 eui-64

関連コマンド

display ipv6 interface

16.1.19 ipv6 address link-local

Syntax

ipv6 address *ipv6-address* **link-local**

undo ipv6 address *ipv6-address* **link-local**

デフォルト

設定なし

View

Interface view

定義済みユーザロール

network-admin

パラメータ

ipv6-address: IPv6 リンクローカルアドレスを指定します。アドレスの最初の 10 ビットは、1111111010（バイナリ表示）である必要があります。つまり、アドレス内の 16 進数の最初のグループの範囲は FE80 から FEBF になります。

説明

ipv6 address link-local コマンドはインタフェースにリンクローカルアドレスを設定します。

undo ipv6 address link-local コマンドはインタフェースにリンクローカルアドレスを削除します。

手動割り当ては、自動作成より優先されます。

最初に自動作成を採用して次に手動割り当てを行った場合、手動で割り当てたリンクローカルアドレスが自動作成アドレスを上書きします。

最初に手動割り当てを行い、次に自動作成を行った場合、以下のことが発生します。

- 自動作成されたリンクローカルアドレスは有効になりません。
- インタフェースのリンクローカルアドレスは手動割り当てのものがそのまま使われます。

手動で割り当てられたアドレスを削除すると、自動作成のリンクローカルアドレスが有効になります。IPvv6 リンクローカルアドレスの自動作成の詳細は、**ipv6 address auto link-local** コマンドを参照してください。

例

VLAN インタフェース 100 でリンクローカルアドレスを設定します。

<Switch> system-view

[Switch] interface vlan-interface 100

[Switch-Vlan-interface100] ipv6 address fe80::1 link-local

関連コマンド

ipv6 address auto link-local

16.1.20 ipv6 hop-limit

Syntax

ipv6 hop-limit *value*

undo ipv6 hop-limit

デフォルト

64

View

System view

定義済みユーザロール

network-admin

パラメータ

value: ホップ数を指定します。設定範囲は 1～255 です。

説明

ipv6 hop-limit コマンドは IPv6 ヘッダの Hop Limit フィールドを設定します。

undo ipv6 hop-limit コマンドはデフォルトに戻します。

Hop Limit は装置によって作成された IPv6 パケットが転送できる数を決定します。

装置が RA メッセージの Hop Limit フィールドを通知します。すべての RA メッセージの受信側は Hop Limit フィールドの値に **ipv6 hop-limit** コマンドで設定された値を使用します。

例

最大ホップ数を 100 に設定します。

<Switch> system-view

[Switch] ipv6 hop-limit 100

16.1.21 ipv6 hoplimit-expires enable

Syntax

ipv6 hoplimit-expires enable

undo ipv6 hoplimit-expires enable

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

ipv6 hoplimit-expires enable コマンドは ICMPv6 の時間超過パケットの送信を有効にします。

undo ipv6 hoplimit-expires enable コマンドは ICMPv6 時間超過パケットの送信を無効にします。

ICMPv6 時間超過メッセージは、ホップ制限が超過あるいはフラグメント再構築のタイムアウトにより、装置が IPv6 パケットを廃棄した後、IPv6 パケットの送信元に送信されます。

多くの ICMPv6 エラーメッセージにより装置の性能に影響することを防ぐために、この機能を無効にしてください。この機能を無効にしても装置は再構築時間超過メッセージを送信します。

例

ICMPv6 時間超過パケットの送信を無効にします。

<Switch> system-view

[Switch] undo ipv6 hoplimit-expires enable

16.1.22 ipv6 icmpv6 error-interval

Syntax

ipv6 icmpv6 error-interval *interval* [*bucketsize*]

undo ipv6 icmpv6 error-interval

デフォルト

トークンのバケットサイズは 10 です。

ICMPv6 エラーメッセージがバケットに到着する時間間隔は 100 ミリ秒です。

View

System view

定義済みユーザロール

network-admin

パラメータ

interval: バケットに到着する時間間隔を設定します。設定範囲は 0～2147483647 ミリ秒です。ICMPv6 レートリミットを無効にする場合、0 に設定します。

bucketsize: バケットで許容されるトークンの最大数を指定します。設定範囲は 1～200 です。

説明

ipv6 icmpv6 error-interval コマンドはトークンのバケットサイズ、および ICMPv6 エラーメッセージがバケットに到着する時間間隔を設定します。

undo ipv6 icmpv6 error-interval コマンドはデフォルトに戻します。

ネットワークの混雑状態を引き起こす可能性のある短い期間内に、過度の ICMPv6 エラーメッセージを送信することを避けるため、ICMPv6 エラーメッセージの送信レートを制限することができます。トークンバケット（bucket）アルゴリズムは、1 つの ICMPv6 エラーメッセージを示す 1 つのトークンが用いられます。

バケットに入ることができるトークンの最大数に達するまで、トークンは指定された間隔でバケットに配置されます。

ICMPv6 エラーメッセージが送信されるときに、トークンはバケットから取り除かれます。バケットが空のときに、新しいトークンがバケットに配置されるまで、ICMPv6 エラーメッセージは送信されません。

例

ICMPv6 エラーメッセージの時間間隔を 200 ミリ秒、トークンのバケットサイズを 40 に設定します。

<Switch> system-view

[Switch] ipv6 icmpv6 error-interval 200 40

16.1.23 ipv6 icmpv6 multicast-echo-reply enable

Syntax

ipv6 icmpv6 multicast-echo-reply enable

undo ipv6 icmpv6 multicast-echo-reply enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

ipv6 icmpv6 multicast-echo-reply enable コマンドはマルチキャストエコー要求への応答を有効にします。

undo ipv6 icmpv6 multicast-echo-reply enable コマンドはデフォルトに戻します。

ホストがマルチキャストエコー要求への応答を行うように設定されている場合、攻撃者は、このメカニズムを使用してホストに攻撃を行います。たとえば、攻撃者が送信元としてホスト A にマルチキャストアドレスのエコー要求を送信すると、マルチキャストグループのすべてのホストはホスト A にエコー応答を送信します。

攻撃を防ぐため、必要でない限り、マルチキャストエコー要求への応答を有効にしないでください。

例

マルチキャストエコー要求への応答を有効にします。

<Switch> system-view

[Switch] ipv6 icmpv6 multicast-echo-reply enable

16.1.24 ipv6 mtu

Syntax

ipv6 mtu *size*

undo ipv6 mtu

デフォルト

設定なし

View

Interface view

定義済みユーザロール

network-admin

パラメータ

size: インタフェースの MTUサイズを指定します。設定範囲は 1280～1500バイトです。

説明

ipv6 mtu コマンドはインタフェースから送信する IPv6 パケットの MTU を設定します。

undo ipv6 mtu コマンドはデフォルトの MTU に戻します。

IPv6 ルータはパケットのフラグメントをサポートしません。IPv6 ルータが IPv6 パケットを受信した後、パケットサイズが転送インタフェースの MTU よりも大きい場合、ルータはパケットを廃棄します。その一方、ルータは送信元ホストに ICMPv6 パケットが大きすぎるというメッセージによって MTU を送信します。送信元ホストは MTU に従いパケットをフラグメントし、パケットを再送します。パケット廃棄により余計なフローのオーバヘッドを削減するため、ネットワークでインタフェースの MTU を適切に設定します。

例

VLAN インタフェース 100 から送信する IPv6 パケットの MUT を 1280 バイトに設定します。

<Switch> system-view

[Switch] interface vlan-interface 100

[Switch-Vlan-interface100] ipv6 mtu 1280

16.1.25 ipv6 nd autoconfig managed-address-flag

Syntax

ipv6 nd autoconfig managed-address-flag

undo ipv6 nd autoconfig managed-address-flag

デフォルト

RA メッセージの M フラグは 0 です。RA メッセージを受信するホストは、IPv6 アドレスを取得するため、ステートレス自動設定を使用します。

View

Interface view

定義済みユーザロール

network-admin

説明

ipv6 nd autoconfig managed-address-flag コマンドは RA メッセージの管理アドレス設定フラグ（M）を 1 に設定します。

undo ipv6 nd autoconfig managed-address-flag コマンドはデフォルトに戻します。

RA メッセージの M フラグは、受信ホストが IPv6 アドレスを取得するため、ステートフル自動設定を使用するかどうかを決定します。

- もし RA メッセージの M フラグを 1 に設定した場合、IPv6 アドレスを取得するため、受信ホストはステートフル自動設定（たとえば、DHCPv6 サーバ）を使用します。
- もし RA メッセージの M フラグを 0 に設定した場合、IPv6 アドレスを取得するため、受信ホストはステートレス自動設定を使用します。ステートレス自動設定はリンクレイヤアドレスと RA メッセージのプレフィックス情報に従い IPv6 アドレスを作成します。

例

RA メッセージの管理アドレス設定フラグ（M）を 1 に設定します。

<Switch> system-view

[Switch] interface vlan-interface 100

[Switch-Vlan-interface100] ipv6 nd autoconfig managed-address-flag

16.1.26 ipv6 nd autoconfig other-flag

Syntax

ipv6 nd autoconfig other-flag

undo ipv6 nd autoconfig other-flag

デフォルト

RA メッセージの O フラグは 0 です。RA メッセージを受信するホストは、IPv6 アドレス以外の設定情報を取得するため、ステートレス自動設定を使用します。

View

Interface view

定義済みユーザロール

network-admin

説明

ipv6 nd autoconfig other-flag コマンドは RA メッセージの他のステートフル設定フラグ（O）を 1 に設定します。

undo ipv6 nd autoconfig other-flag コマンドはデフォルトに戻します。

RA メッセージの O フラグは、受信ホストが IPv6 アドレス以外の設定情報を取得するため、ステートフル自動設定を使用するかどうかを決定します。

- もし RA メッセージの O フラグを 1 に設定した場合、IPv6 アドレス以外の設定情報を取得するため、受信ホストはステートフル自動設定（たとえば、DHCPv6 サーバ）を使用します。
- もし RA メッセージの O フラグを 0 に設定した場合、IPv6 アドレス以外の設定情報を取得するため、受信ホストはステートレス自動設定を使用します。

例

RA メッセージの O フラグを 0 に設定します。

<Switch> system-view

[Switch] interface vlan-interface 100

[Switch-Vlan-interface100] undo ipv6 nd autoconfig other-flag

16.1.27 ipv6 nd dad attempts

Syntax

ipv6 nd dad attempts *interval*

undo ipv6 nd dad attempts

デフォルト

1

View

Interface view

定義済みユーザロール

network-admin

パラメータ

interval: DAD の NS メッセージを送信する試行回数を指定します設定範囲は 0～600 です。0 に設定すると DAD は無効になります。

説明

ipv6 nd dad attempts コマンドは DAD の NS メッセージを送信する試行回数を設定します。

undo ipv6 nd dad attempts コマンドはデフォルトに戻します。

IPv6 アドレスを取得したのち、インタフェースは DAD の NS メッセージを送信します。

インタフェースが **ipv6 nd ns retrans-timer** コマンドで指定された時間以内に応答を受信しない場合、インタフェースは NS メッセージを再送します。

インタフェースが試行回数（**ipv6 nd dad attempts** コマンドで設定します）を超過しても応答を受信しない場合、取得したアドレスが使用できないと認識します。

例

DAD の NS メッセージを送信する試行回数を 20 に設定します。

<Switch> system-view

[Switch] interface vlan-interface 100

[Switch-Vlan-interface100] ipv6 nd dad attempts 20

関連コマンド

- **display ipv6 interface**
- **ipv6 nd ns retrans-timer**

16.1.28 ipv6 nd ns retrans-timer

Syntax

ipv6 nd ns retrans-timer *value*

undo ipv6 nd ns retrans-timer

デフォルト

ローカルインタフェースは 1000 ミリ秒の間隔で NS メッセージを送信します。送信する RA メッセージの Retrans Timer フィールドを 0 に設定します。NS メッセージの再送間隔は受信装置によって決まります。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

value: NS メッセージを再送する間隔を指定します。設定範囲は 1000～4294967295 ミリ秒です。

説明

ipv6 nd ns retrans-timer コマンドは NS メッセージの再送間隔を設定します。

undo ipv6 nd ns retrans-timer コマンドはデフォルトに戻します。

装置が指定した時間間隔以内にピアから応答を受信しない場合、装置は NS メッセージを再送します。装置は指定した間隔で NS メッセージを再送し、送信する RA メッセージのフィールドの値に指定した時間間隔を設定します。

例

VLAN インタフェース 100 で NS メッセージを再送する時間間隔を 10000 ミリ秒に指定します。

<Switch> system-view

[Switch] interface vlan-interface 100

[Switch-Vlan-interface100] ipv6 nd ns retrans-timer 10000

関連コマンド

display ipv6 interface

16.1.29 ipv6 nd nud reachable-time

Syntax

ipv6 nd nud reachable-time *time*

undo ipv6 nd nud reachable-time

デフォルト

インタフェースのネイバ到達可能時間は 30000 ミリ秒です。RA メッセージの Reachable Time フィールドの値は 0 です。到達可能時間は受信装置によって決まります。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

time: インタフェースのネイバ到達可能時間を指定します。設定範囲は 1～3600000 ミリ秒です。

説明

ipv6 nd nud reachable-time コマンドはインタフェースのネイバ到達可能時間を設定します。

undo ipv6 nd nud reachable-time コマンドはデフォルトに戻します。

ネイバの到達可能性の検出を行い到達可能であった場合、装置は指定した到達可能時間内にネイバに到達できると認識します。指定した到達可能時間が終了した後、ネイバにパケットを送信する必要がある場合、装置はネイバが到達可能かどうか再確認を行います。装置はローカルインタフェースのネイバ到達可能時間を設定し、送信する RA メッセージの Reachable Time フィールドに指定した値を設定します。

例

VLAN インタフェース 100 のネイバ到達可能時間を 10000 ミリ秒に設定します。

<Switch> system-view

[Switch] interface vlan-interface 100

[Switch-Vlan-interface100] ipv6 nd nud reachable-time 10000

関連コマンド

display ipv6 interface

16.1.30 ipv6 nd ra halt

Syntax

ipv6 nd ra halt

undo ipv6 nd ra halt

デフォルト

有効

View

Interface view

定義済みユーザロール

network-admin

説明

ipv6 nd ra halt コマンドは RA メッセージ送信の抑制を有効にします。

undo ipv6 nd ra halt コマンドは RA メッセージ送信の抑制を無効にします。

例

VLAN インタフェース 100 の RA メッセージの抑制を無効にします。

<Switch> system-view

[Switch] interface vlan-interface 100

[Switch-Vlan-interface100] undo ipv6 nd ra halt

16.1.31 ipv6 nd ra interval

Syntax

ipv6 nd ra interval *max-interval min-interval*

undo ipv6 nd ra interval

デフォルト

RA メッセージの送信間隔の最大値は 600 秒です。RA メッセージの送信間隔の最小値は 200 秒です。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

max-interval: RA メッセージの送信間隔の最大値を指定します。設定範囲は 4～1800 秒です。

min-interval: RA メッセージの送信間隔の最小値を指定します。設定範囲は 3～最大値の 3/4 秒です。

説明

ipv6 nd ra interval コマンドは RA メッセージの送信間隔の最大値と最小値を設定します。

undo ipv6 nd ra interval コマンドはデフォルトに戻します。

装置は RA メッセージを送信間隔の最大値と最小値の間のランダムな時間に送信します。

RA メッセージの送信間隔の最大値は RA メッセージのルータのライフタイムと同じかそれ以下にしてください。

例

RA メッセージの送信間隔の最大値を 1000 秒、最小値を 700 秒に設定します。

<Switch> system-view

[Switch] interface vlan-interface 100

[Switch-Vlan-interface100] ipv6 nd ra interval 1000 700

関連コマンド

ipv6 nd ra router-lifetime

16.1.32 ipv6 nd ra prefix

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* }

デフォルト

RA メッセージのプレフィックス情報は設定されていません。RA メッセージを送信するインタフェースの IPv6 アドレスはプレフィックス情報として使用します。

IPv6 アドレスがスタティックに設定されている場合、プレフィックスは固定の有効ライフタイム 2592000 秒（30 日）と優先ライフタイム 604800 秒（7 日）を使用します。

IPv6 アドレスがダイナミックに設定されている場合（たとえば、DHCP などを使用します）、プレフィックスは IPv6 アドレスの有効ライフタイムと優先ライフタイムを使用します。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

ipv6-prefix: IPv6 プレフィックスを指定します。

prefix-length: IPv6 アドレスのプレフィックス長を指定します。

valid-lifetime: プレフィックスの有効ライフタイムを指定します。設定範囲は 0～4294967295 秒です。

preferred-lifetime: ステートレス自動設定に使用するプレフィックスの優先ライフタイムを指定します。設定範囲は 0～4294967295 秒です。優先ライフタイムは有効ライフタイムよりも大きい時間にすることはできません。

no-autoconfig: ステートレス自動設定を使用しないようにプレフィックスを指定します。指定しない場合、プレフィックスはステートレス自動設定を使用します。

off-link: プレフィックス付きのアドレスがリンク上で直接到達できないように指定します。指定しない場合、プレフィックス付きアドレスはリンク上で直接到達可能になります。

説明

ipv6 nd ra prefix コマンドは RA メッセージのプレフィックス情報を設定します。

undo ipv6 nd ra prefix コマンドはデフォルトに戻します。

同一リンクのホストが RA メッセージを受信したのち、ステートレス自動設定のため、RA メッセージのプレフィックス情報を使用することができます。

例

VLAN インタフェース 100 の RA メッセージのプレフィックス情報を設定します。

方法 1：

<Switch> system-view

[Switch] interface vlan-interface 100

[Switch-Vlan-interface100] ipv6 nd ra prefix 2001:10::100/64 100 10

方法 2：

<Switch> system-view

[Switch] interface vlan-interface 100

[Switch-Vlan-interface100] ipv6 nd ra prefix 2001:10::100 64 100 10

16.1.33 ipv6 nd ra router-lifetime

Syntax

ipv6 nd ra router-lifetime *time*

undo ipv6 nd ra router-lifetime

デフォルト

1800 秒

View

Interface view

定義済みユーザロール

network-admin

パラメータ

time: ルータのライフタイムを指定します。設定範囲は 0～9000 秒です。0 に設定した場合、デフォルトルータとして動作しません。

説明

ipv6 nd ra router-lifetime コマンドは RA メッセージのルータのライフタイムを設定します。

undo ipv6 nd ra router-lifetime コマンドはデフォルトに戻します。

RA メッセージのルータのライフタイムは、RA メッセージを送信するルータがデフォルトルータとして動作する長さを指定します。RA メッセージを受信するホストは、ルータのライフタイムをチェックし、デフォルトルータとして使用するかどうかを決定します。ルータのライフタイムが 0 である場合、ルータはデフォルトルータとして使用することができません。

RA メッセージのルータのライフタイムは RA メッセージの送信間隔と同じあるいはそれ以上の値にする必要があります。

例

VLAN インタフェース 100 の RA メッセージのルータのライフタイムを 1000 秒に設定します。

<Switch> system-view

[Switch] interface vlan-interface 100

[Switch-Vlan-interface100] ipv6 nd ra router-lifetime 1000

関連コマンド

ipv6 nd ra interval

16.1.34 ipv6 neighbor

Syntax

ipv6 neighbor *ipv6-address mac-address* { *vlan-id port-type port-number* | **interface** *interface-type interface-number* }

undo ipv6 neighbor *ipv6-address interface-type interface-number*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

ipv6-address: スタティックネイバエントリの IPv6 アドレスを指定します。

mac-address: スタティックネイバエントリの MAC アドレス（48 ビット）を指定します。形式は H-H-H です。

vlan-id: スタティックネイバエントリの VLAN ID を指定します。設定範囲は 1～4094 です。

port-type port-number: スタティックネイバエントリのレイヤ 2 ポートのタイプと番号を指定します。

interface *interface-type interface-number*: スタティックネイバエントリのレイヤ 3 インタフェースのタイプと番号を指定します。

説明

ipv6 neighbor コマンドはスタティックネイバエントリを設定します。

undo ipv6 neighbor コマンドはスタティックネイバエントリを削除します。

隣接エントリはリンクローカルノードの情報を記録します。エントリは NS メッセージと NA メッセージを使用してダイナミック、あるいはスタティックに設定することができます。

装置はネイバの IPv6 アドレスとローカルレイヤ 3 インタフェース番号でスタティックネイバエントリを固有に識別します。以下のいずれかの方法を使用してスタティックネイバエントリを設定することができます。

- **方法 1**－ネイバ IPv6 アドレスとリンクレイヤアドレスをローカルノードのレイヤ 3 インタフェースに割り当てます。
- **方法 2**－ネイバ IPv6 アドレスとリンクレイヤアドレスをローカルノードが含まれる VLAN のレイヤ 2 ポートに割り当てます。

VLAN インタフェースのスタティックネイバエントリを設定するため、上記の設定方法のどちらかを使用することができます。

- 方法 1 を使用する場合、ネイバエントリは INCMP 状態です。装置がレイヤ 2 ポート情報に対応する情報を取得した後、ネイバエントリは REACH 状態になります。
- 方法 2 を使用する場合、対応する VLAN インタフェースがすでに存在し、*port-type port-number* によって指定されたレイヤ 2 ポートが、*vlan-id* で指定されている VLAN に属している必要があります。スタティックネイバエントリが設定されたのち、装置はスタティックネイバエントリを一意に識別するため、VLAN インタフェースを IPv6 アドレスに関連づけ、ネイバエントリが REACH 状態になります。

VLAN インタフェースのスタティックネイバエントリを削除する場合、対応する VLAN インタフェースのみを指定してください。

例

VLAN インタフェース 1 のスタティックネイバエントリを設定します。

<Switch> system-view

[Switch] ipv6 neighbor 2000::1 fe-e0-89 interface Vlan-interface 1

関連コマンド

- **display ipv6 neighbors**
- **reset ipv6 neighbors**

16.1.35 ipv6 neighbor stale-aging

Syntax

ipv6 neighbor stale-aging *aging-time*

undo ipv6 neighbor stale-aging

デフォルト

240 分

View

System view

定義済みユーザロール

network-admin

パラメータ

aging-time: STALE 状態の ND エントリのエージングタイマを指定します。設定範囲は 1 ～1440 分です。

説明

ipv6 neighbor stale-aging コマンドは STALE 状態の ND エントリのエージングタイマを設定します。

undo ipv6 neighbor stale-aging コマンドはデフォルトに戻します。

エージングタイマは STALE 状態のすべての ND エントリに適用します。エージングタイマが終了する前に、STALE 状態の ND エントリがリフレッシュされない場合、NG エントリは DELAY 状態に遷移します。5 秒以内にリフレッシュされない場合、PROBE 状態に遷移し、装置は 3 回、NS メッセージを送信します。もし応答がない場合、ND エントリを削除します。

例

STALE 状態の ND エントリのエージングタイマを 120 分に設定します。

<Switch> system-view

[Switch] ipv6 neighbor stale-aging 120

16.1.36 ipv6 neighbors max-learning-num

Syntax

ipv6 neighbors max-learning-num *max-number*

undo ipv6 neighbors max-learning-num

デフォルト

16384

View

Layer 2/Layer 3 interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

max-number: インタフェースが学習できるダイナミックネイバエントリの最大数を指定します。設定範囲は 1～16384 です。

説明

ipv6 neighbors max-learning-num コマンドはインタフェースが学習できるダイナミックネイバエントリの最大数を指定します。これはインタフェースが多くのネイバテーブルのリソースを占有することを防止します。

undo ipv6 neighbors max-learning-num コマンドはデフォルトに戻します。

装置は NS メッセージと NA メッセージによって隣接ノードのリンクレイヤアドレスをダイナミックに取得することができ、そのアドレスをネイバテーブルに追加します。

ダイナミックネイバエントリが最大数に到達したとき、インタフェースはネイバ情報の学習を停止します。

例

VLAN インタフェース 100 が学習できるダイナミックネイバエントリの最大数を 10 に設定します。

<Switch> system-view

[Switch] interface vlan-interface 100

[Switch-Vlan-interface100] ipv6 neighbors max-learning-num 10

16.1.37 ipv6 pathmtu

Syntax

ipv6 pathmtu *ipv6-address value*

undo ipv6 pathmtu *ipv6-address*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

ipv6-address: IPv6 アドレスを指定します。

value: 指定された IPv6 アドレスの PMTU を指定します。設定範囲は 1280～10240 バイトです。

説明

ipv6 pathmtu コマンドは IPv6 アドレスのスタティック PMTU（Path MTU）を設定します。

undo ipv6 pathmtu コマンドは IPv6 アドレスのスタティック PMTU（Path MTU）を削除します。

宛先 IPv6 アドレスのスタティック PMTU を設定することができます。インタフェースを通して送信元ホストにパケットを送信するとき、インタフェースの MTU と指定された宛先 IPv6 アドレスのスタティック PMTU を比較します。もしパケットサイズが 2 つの値よりも大きい場合、ホストは小さい値に従ってパケットをフラグメントします。

例

IPv6 アドレスのスタティック PMTU を設定します。

<Switch> system-view

[Switch] ipv6 pathmtu fe80::12 1300

関連コマンド

- **display ipv6 pathmtu**
- **reset ipv6 pathmtu**

16.1.38 ipv6 pathmtu age

Syntax

ipv6 pathmtu age *age-time*

undo ipv6 pathmtu age

デフォルト

10 分

View

System view

定義済みユーザロール

network-admin

パラメータ

age-time: PMTU のエージング時間を指定します。設定範囲は 10～100 分です。

説明

ipv6 pathmtu age コマンドはダイナミック PMTU のエージング時間を設定します。

undo ipv6 pathmtu age コマンドはデフォルトに戻します。

送信元ホストから宛先ホストの PMTU がダイナミックに決定したのち、送信元ホストは MTU をもとにして宛先ホストに後続のパケットを送信します。

エージング時間が終了した後、以下のことが発生します。

- ダイナミック PMTU が削除されます。
- 送信元ホストは PMTU メカニズムによってダイナミック PMTU を再度決定します。

スタティック PMTU のエージング時間は無効です。

例

ダイナミック PMTU のエージング時間を 40 分に設定します。

<Switch> system-view

[Switch] ipv6 pathmtu age 40

関連コマンド

display ipv6 pathmtu

16.1.39 ipv6 unreachables enable

Syntax

ipv6 unreachables enable

undo ipv6 unreachables enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

ipv6 unreachables enable コマンドは IPv6 宛先到達不能メッセージの送信を有効にします。

undo ipv6 unreachables enable コマンドは IPv6 宛先到達不能メッセージの送信を無効にします。

宛先到達不能のエラーであるため、受信した IPv6 パケットの転送に失敗した場合、装置は以下の処理を行います。

- パケットを廃棄します。
- 送信元に対応する ICMPv6 Destination Unreachable エラーメッセージを送信します。

装置が間違って ICMPv6 Destination Unreachable エラーメッセージを作成した場合、攻撃リスクを防ぐため、ICMPv6 Destination Unreachable エラーメッセージの送信を無効にします。

例

IPv6 宛先到達不能メッセージの送信を有効にします。

<Switch> system-view

[Switch] ipv6 unreachables enable

16.1.40 reset ipv6 neighbors

Syntax

reset ipv6 neighbors { **all** | **dynamic** | **interface** *interface-type interface-number* | **slot** *slot-number* | **static** }

View

User view

定義済みユーザロール

network-admin

パラメータ

all: すべてのインタフェースのスタティック、ダイナミックネイバ情報を削除します。

dynamic: すべてのインタフェースのダイナミックネイバ情報を削除します。

interface *interface-type interface-number*: 指定されたタイプと番号のインタフェースのダイナミックネイバ情報を削除します。

slot *slot-number*: 指定した IRF スタックメンバ装置のダイナミックネイバ情報を削除します。*slot-number* は IRF スタックメンバ装置の ID を指定します。指定しない場合、すべてのメンバ装置のダイナミックネイバ情報を削除します。

static: すべてのインタフェースのスタティックネイバ情報を削除します。

説明

reset ipv6 neighbors コマンドは IPv6 ネイバ情報を削除します。

例

すべてのインタフェースのネイバ情報を削除します。

<Switch> reset ipv6 neighbors all

```
This will delete all the entries. Continue? [Y/N]:Y
```

すべてのインタフェースのダイナミックネイバ情報を削除します。

<Switch> reset ipv6 neighbors dynamic

```
This will delete all the dynamic entries. Continue? [Y/N]:Y
```

GigabitEthernet 1/0/1 のすべてのネイバ情報を削除します。

<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
```

関連コマンド

- **display ipv6 neighbors**
- **ipv6 neighbor**

16.1.41 reset ipv6 pathmtu

Syntax

reset ipv6 pathmtu { **all** | **dynamic** | **static** }

View

User view

定義済みユーザロール

network-admin

パラメータ

all: すべての PMTU 情報を削除します。

dynamic: すべてのダイナミック PMTU 情報を削除します。

static: すべてのスタティック PMTU 情報を削除します。

説明

reset ipv6 pathmtu コマンドは PMTU 情報を削除します。

例

すべての PMTU 情報を削除します。

<Switch> reset ipv6 pathmtu all

関連コマンド

display ipv6 pathmtu

16.1.42 reset ipv6 statistics

Syntax

reset ipv6 statistics [**slot** *slot-number*]

View

User view

定義済みユーザロール

network-admin

パラメータ

slot *slot-number*: 指定した IRF スタックメンバ装置の IPv6 パケットと ICMPv6 パケットの統計情報を削除します。*slot-number* は IRF スタックメンバ装置の ID を指定します。

指定しない、すべてのメンバ装置の IPv6 パケットと ICMPv6 パケットの統計情報を削除します。

説明

reset ipv6 statistics コマンドは IPv6 パケットと ICMPv6 パケットの統計情報を削除します。

例

IPv6 パケットと ICMPv6 パケットの統計情報を削除します。

<Switch> reset ipv6 statistics

関連コマンド

display ipv6 statistics

目次

このセクションのページは **4-x-x** です。

17 章 DHCPv6 17-1
17.1 DHCPv6 設定コマンド.....17-1
17.1.1 display ipv6 dhcp duid.....17-1
17.1.2 ipv6 dhcp select.....17-1

17章 DHCPv6

17.1 DHCPv6設定コマンド

17.1.1 display ipv6 dhcp duid

Syntax

display ipv6 dhcp duid

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display ipv6 dhcp duidh コマンドは、ローカル装置の DUID を表示します。

DHCP 固有識別子(DUID)は、DHCPv6 装置(DHCPv6 クライアント、サーバ、またはリレーエージェント)を一意に識別します。 DHCPv6 装置は、送信パケットに DUID を追加します。

このコマンドは、DHCPv6 プロセスが装置で実行された後にのみ出力を表示します。

例

ローカル装置の DUID を表示します。

<Switch> display ipv6 dhcp duid

```
The DUID of this device: 0003000100e0fc005552.
```

17.1.2 ipv6 dhcp select

Syntax

ipv6 dhcp select { **relay** | **server** }

undo ipv6 dhcp select

デフォルト

インタフェースは、DHCPv6 サーバモードまたは DHCPv6 リレーエージェントモードでは動作しません。DHCPv6 クライアントからの DHCPv6 パケットを破棄します。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

relay: インタフェースで DHCP リレーエージェントを有効にします。

server: インタフェースで DHCP サーバを有効にします。

説明

dhcp select コマンドはインタフェースで DHCP サーバあるいは DHCP リレーエージェントを有効にします。

undo dhcp select コマンドはデフォルトに戻します。

インタフェース上で DHCPv6 サーバモードを DHCPv6 リレーエージェントモードに変更する前に、次のコマンドを使用して IPv6 アドレス/プレフィックスバインディングを削除します。

- **reset ipv6 dhcp server ip-in-use**
- **reset ipv6 dhcp server pd-in-use**

DHCPv6 リレーエージェントまたは DHCPv6 サーバとして構成されているインタフェースでは、DHCPv6 クライアントを構成しないでください。

例

VLAN インタフェース 10 で DHCPv6 サーバを有効にします。

<Switch> system-view

[Switch] interface vlan-interface 10

[Switch-Vlan-interface10] ipv6 dhcp select server

VLAN インタフェース 20 で DHCPv6 リレーエージェントを有効にします。

<Switch> system-view

[Switch] interface vlan-interface 20

[Switch-Vlan-interface20] ipv6 dhcp select relay

関連コマンド

display ipv6 dhcp relay server-address

display ipv6 dhcp server

目次

このセクションのページは **4-x-x** です。

18 章 DHCPv6 リレーエージェント 18-1
18.1 DHCPv6 リレーエージェント設定コマンド.....18-1
18.1.1 display ipv6 dhcp relay server-address.....18-1
18.1.2 display ipv6 dhcp relay statistics.....18-2
18.1.3 ipv6 dhcp relay server-address.....18-5
18.1.4 reset ipv6 dhcp relay statistics.....18-7

18章 DHCPv6 リレーエージェント

18.1 DHCPv6 リレーエージェント設定コマンド

18.1.1 display ipv6 dhcp relay server-address

Syntax

display ipv6 dhcp relay server-address [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: タイプと番号でインタフェースを指定します。インタフェースを指定しない場合、このコマンドは、DHCPv6 リレーエージェントで有効になっているすべてのインタフェース上の DHCPv6 サーバアドレスを表示します。

説明

display ipv6 dhcp relay server-address コマンドは、DHCPv6 リレーエージェントで指定された DHCPv6 サーバアドレスを表示します。

例

DHCPv6 リレーエージェントが有効になっているすべてのインタフェースで、DHCPv6 サーバアドレスを表示します。

<Switch> display ipv6 dhcp relay server-address

```
Interface: Vlan-interface2
 Server address    Outgoing Interface        Public/VRF name
 2::3                                      --/--
 3::4            Vlan-interface4             Y/--
 4::5                                      --/1

Interface: Vlan-interface3
 Server address    Outgoing Interface        Public/VRF name
 2::3                                      --/--
```

```
3::4            Vlan-interface4          Y/--
4::5                                     --/1
```

VLAN インタフェース 2 に DHCPv6 サーバアドレスを表示します。

<Switch> display ipv6 dhcp relay server-address interface vlan-interface 2

```
Interface: Vlan-interface2
 Server address    Outgoing Interface        Public/VRF name
 2::3                                       --/--
 3::4            Vlan-interface4            Y/--
 4::5                                       --/1
```

表 18-1 コマンド出力

フィールド	説明
Server address	DHCPリレーエージェントで指定されたDHCPv6サーバアドレスです。
Outgoing Interface	DHCPv6パケットのインタフェースを出力します。 出力インタフェースが指定されていない場合、装置はルーティングテーブルで出力インタフェースを検索します。
Public/VRF name	DHCPv6サーバの場所。**ipv6 dhcp relay *server-address***コマンドの設定によって決定されます。 **public**キーワードも**vpn-instance** *vpn-instance-name*オプションも指定されていない場合、このフィールドには**--/--**と表示されます。 **public**キーワードが指定されている場合、このフィールドには**Y/--**と表示されます。 **vpn-instance** *vpn-instance-name*オプションを指定すると、スラッシュ(/)の後にVPNインスタンス名が表示されます(**例:--/1**)。

関連コマンド

- **ipv6 dhcp relay server-address**
- **ipv6 dhcp select**

18.1.2 display ipv6 dhcp relay statistics

Syntax

display ipv6 dhcp relay statistics [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: タイプと番号でインタフェースを指定します。インタフェースを指定しない場合、このコマンドは、DHCPv6 リレーエージェントが有効なすべてのインタフェースで DHCPv6 パケット統計情報を表示します。

説明

display ipv6 dhcp relay statistics コマンドは、DHCPv6 リレーエージェントに DHCPv6 パケット統計情報を表示します。

例

DHCPv6 リレーエージェントが有効になっているすべてのインタフェースで、DHCPv6 パケット統計情報を表示します。

<Switch> display ipv6 dhcp relay statistics

```
Packets dropped             :  4
Packets received            :  14
    Solicit                 :  0
    Request                 :  0
    Confirm                 :  0
    Renew                   :  0
    Rebind                  :  0
    Release                 :  0
    Decline                 :  0
    Information-request     :  7
    Relay-forward           :  0
    Relay-reply             :  7
Packets sent                :  14
    Advertise               :  0
    Reconfigure             :  0
    Reply                   :  7
    Relay-forward           :  7
    Relay-reply             :  0
```

VLAN インタフェース 2 の DHCPv6 リレーエージェントに DHCPv6 パケット統計情報を表示します。

<Switch> display ipv6 dhcp relay statistics interface vlan-interface 2

```
Packets dropped             : 4
Packets received            : 16
    Solicit                 : 0
    Request                 : 0
    Confirm                 : 0
    Renew                   : 0
    Rebind                  : 0
    Release                 : 0
    Decline                 : 0
    Information-request     : 8
    Relay-forward           : 0
    Relay-reply             : 8
Packets sent                : 16
    Advertise               : 0
    Reconfigure             : 0
    Reply                   : 8
    Relay-forward           : 8
    Relay-reply             : 0
```

表 18-2 コマンド出力

フィールド	説明
Packets dropped	破棄されたパケットの数です。
Packets received	受信パケット数です。
Solicit	受信した要請パケットの数です。
Request	受信した要求パケットの数です。
Confirm	受信した確認パケットの数です。
Renew	受信した更新パケットの数です。
Rebind	受信した再バインドパケットの数です。
Release	受信したリリースパケットの数です。
Decline	受信した拒否パケットの数です。
Information-request	受信した情報要求パケットの数です。
Relay-forward	受信した中継転送パケットの数です。

フィールド	説明
Relay-reply	受信したリレー応答パケットの数です。
Packets sent	送信されたパケットの数です。
Advertise	送信されたアドバタイズメントパケットの数です。
Reconfigure	送信された再構成パケットの数です。
Reply	送信された応答パケットの数です。
Relay-forward	送信されたリレーフォワードパケットの数です。
Relay-reply	送信されたリレー応答パケットの数です。

関連コマンド

reset ipv6 dhcp relay statistics

18.1.3 ipv6 dhcp relay server-address

Syntax

ipv6 dhcp relay server-address *ipv6-address* [interface *interface-type interface-number*] [**public** | vpn-instance *vpn-instance-name*]

undo ipv6 dhcp relay server-address [*ipv6-address* [**interface** *interface-type interface-number*] [**public** | **vpn-instance** *vpn-instance-name*]]

デフォルト

指定なし

View

Interface view

定義済みユーザロール

network-admin

Parameters

ipv6-address: DHCPv6 サーバの IPv6 アドレスを指定します。

interface *interface-type interface-number*: リレーエージェントが DHCPv6 要求を DHCPv6 サーバに転送するときに使用する出力インタフェースを指定します。出力イン

タフェースを指定しない場合、リレーエージェントは出力インタフェースのルーティングテーブルを検索します。

public: DHCPv6 サーバがパブリックネットワーク上にあることを指定します。 このキーワードを指定しない場合、DHCPv6 サーバがパブリックネットワーク上にあるか VPN 内にあるかは、DHCPv6 クライアントの場所によって異なります。

vpn-instance vpn-instance-name: DHCPv6 サーバが属する MPLS L3VPN インスタンスの名前を指定します。 インスタンス名は、1~31 文字の大文字と小文字を区別する文字列です。 このオプションを指定しない場合、DHCPv6 サーバがパブリックネットワーク上にあるか VPN 内にあるかは、DHCPv6 クライアントの場所によって異なります。

説明

ipv6 dhcp relay server-address コマンドは、DHCPv6 リレーエージェントで DHCPv6 サーバを指定します。**undo ipv6 dhcp relay server-address** コマンドは、DHCPv6 サーバアドレスを削除します。

DHCPv6 クライアントから要求を受信すると、インタフェースは要求をリレー転送メッセージにカプセル化し、指定された DHCPv6 サーバに転送します。

インタフェースでは、最大 8 台の DHCPv6 サーバを指定できます。 DHCPv6 リレーエージェントは、指定されたすべての DHCPv6 サーバに DHCP 要求を転送します。

DHCPv6 サーバアドレスがリンクローカルアドレスまたはマルチキャストアドレスの場合は、出力インタフェースを指定する必要があります。 出力インタフェースを指定しない場合、DHCPv6 パケットが DHCPv6 サーバに到達できないことがあります。

MPLS L3VPN を指定すると、DHCPv6 リレーエージェントは DHCP 要求をこの VPN 内の DHCPv6 サーバに転送します。

IPv6 アドレスを指定しない場合、**undo ipv6 dhcp relay server-address** コマンドは、インタフェースで指定されたすべての DHCPv6 サーバアドレスを削除します。

同じインタフェースで DHCPv6 クライアントと DHCPv6 リレーエージェントを有効にしないでください。

例

VLAN インタフェース 2 で DHCPv6 リレーエージェントを有効にし、DHCPv6 サーバアドレス 2001:1 :: 3 を指定します。

```
<Switch> system-view
[Switch] interface vlan-interface 2
[Switch -Vlan-interface2] ipv6 dhcp select relay
[Switch -Vlan-interface2] ipv6 dhcp relay server-address 2001:1::3
```

関連コマンド

- **display ipv6 dhcp relay server-address**

- **ipv6 dhcp select**

18.1.4 reset ipv6 dhcp relay statistics

Syntax

reset ipv6 dhcp relay statistics [**interface** *interface-type interface-number*]

View

User view

定義済みユーザロール

network-admin

パラメータ

interface *interface-type interface-number*: タイプと番号でインタフェースを指定します。インタフェースを指定しない場合、このコマンドはすべてのリレーエージェント統計情報をクリアします。

説明

reset ipv6 dhcp relay statistics コマンドは、DHCPv6 リレーエージェント上のパケット統計情報をクリアします。

例

DHCPv6 リレーエージェントのクリアパケット統計情報。

<Switch> reset ipv6 dhcp relay statistics

関連コマンド

display ipv6 dhcp relay statistics

目次

このセクションのページは **4-x-x** です。

19 章 DHCPv6 クライアント 19-1
19.1 DHCPv6 クライアント設定コマンド.....19-1
19.1.1 display ipv6 dhcp client 19-1
19.1.2 display ipv6 dhcp client statistics.....19-4
19.1.3 ipv6 address dhcp-alloc.....19-6
19.1.4 reset ipv6 dhcp client statistics.....19-7

19章 DHCPv6 クライアント

19.1 DHCPv6 クライアント設定コマンド

19.1.1 display ipv6 dhcp client

Syntax

display ipv6 dhcp client [**interface** *interface-type interface-number*]

Views

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: タイプと番号でインタフェースを指定します。インタフェースを指定しない場合、このコマンドはすべての DHCPv6 クライアントに関する情報を表示します。

説明

display ipv6 dhcp client コマンドは、DHCPv6 クライアント情報を表示します。

例

VLAN インタフェース 2 で DHCPv6 クライアント情報を表示します。

<Switch> display ipv6 dhcp client interface vlan-interface 2

```
Vlan-interface2:
  Type: Stateful client requesting address and prefix
    State: OPEN
    Client DUID: 0003000100e002000000
    Preferred server:
      Reachable via address: FE80::2E0:1FF:FE00:18
      Server DUID: 0003000100e001000000
    IA_NA: IAID 0x00000642, T1 50 sec, T2 80 sec
      Address: 1:1::2/128
        Preferred lifetime 100 sec, valid lifetime 200 sec
        Will expire on Feb 4 2014 at 15:37:20(288 seconds left)
    IA_PD: IAID 0x00000642, T1 50 sec, T2 80 sec
```

```
  Prefix: 12:34::/48
    Preferred lifetime 100 sec, valid lifetime 200 sec
    Will expire on Mar 27 2014 at 08:13:24 (199 seconds left)
DNS server addresses:
  2:2::3
Domain name:
  aaa.com
SIP server addresses:
  2:2::4
SIP server domain names:
  bbb.com
Options:
  Code: 88
    Length: 3 bytes
    Hex: AABBCC
```

表 19-1 コマンド出力

フィールド	説明
Type	DHCPv6クライアントのタイプ: ● **Stateful client requesting address**—IPv6アドレスを要求するDHCPv6クライアントです。 ● **Stateful client requesting prefix**—IPv6プレフィックスを要求するDHCPv6クライアントです。 ● **Stateful client requesting address and prefix**—IPv6アドレスとプレフィックスを要求するDHCPv6クライアントです。 ● **Stateless client**—ステートレスDHCPv6を介してIPv6アドレスとプレフィックス以外の設定パラメータを要求するDHCPv6クライアントです。

フィールド	説明
State	DHCPv6クライアントの現在の状態: ● **IDLE**—クライアントはアイドル状態です。 ● **SOLICIT**—クライアントがDHCPv6サーバを検出しています。 ● **REQUEST**—クライアントがIPv6アドレスまたはプレフィックスを要求しています。 ● **OPEN**—クライアントがIPv6アドレスまたはプレフィックスを取得しました。 ● **RENEW**—クライアントはリースを延長しています(T1以降T2以前)。 ● **REBIND**—クライアントはリースを延長しています(T2の後、リースの期限が切れる前)。 ● **RELEASE**—クライアントがIPv6アドレスまたはプレフィックスを解放しています。 ● **DECLINE**—アドレスまたはプレフィックスの競合のため、クライアントがIPv6アドレスまたはプレフィックスを拒否しています。 ● **INFO-REQUESTING**—クライアントは、ステートレスDHCPv6を介して設定パラメータを要求しています。
Client DUID	DHCPv6クライアントのDUIDです。
Preferred server	DHCPv6クライアントによって選択されたDHCPv6サーバに関する情報です。
Reachable via address	DHCPv6クライアントの到達可能アドレス。DHCPv6サーバまたはDHCPv6リレーエージェントのリンクローカルアドレスです。
Server DUID	DHCPv6サーバのDUIDです。
IA_NA	IA_NA情報です。
IA_PD	IA_PD情報です。
IAID	IA識別子です。
T1	T1値 (秒) です。
T2	T2値 (秒単位) です。
Address	IPv6アドレスを取得しました。 このフィールドは、DHCPv6クライアントタイプが**Stateful client requesting address**の場合にのみ表示されます。

フィールド	説明
Prefix	IPv6プレフィックスを取得しました。 このフィールドは、DHCPv6クライアントタイプが**Stateful client requesting prefix**の場合にのみ表示されます。
Preferred lifetime	推奨寿命 (秒) です。
valid lifetime	有効な存続時間 (秒単位) です。
Will expire on Feb 4 2014 at 15:37:20 (288 seconds left)	リースの期限が切れる時刻とリースの残りの時間。 リースが2100年より後に満了する場合、このフィールドには**Will expire after 2100**と表示されます。
DNS server addresses	DNSサーバのIPv6アドレスです。
Domain name	ドメイン名のサフィックスです。
SIP server addresses	SIPサーバのIPv6アドレスです。
SIP server domain names	SIPサーバのドメイン名です。
Options	自己定義オプションです。
Code	自己定義オプションのコードです。
Length	自己定義オプションの長さ (バイト単位) です。
Hex	16進数で表される自己定義オプションの内容です。

関連コマンド

- **ipv6 address dhcp-alloc**

19.1.2 display ipv6 dhcp client statistics

Syntax

display ipv6 dhcp client statistics [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: タイプと番号でインタフェースを指定します。インタフェースを指定しない場合、このコマンドはすべての DHCPv6 クライアントの統計情報を表示します。

説明

display ipv6 dhcp client statistics コマンドは、DHCPv6 クライアントの統計情報を表示します。

例

VLAN インタフェース 2 で DHCPv6 クライアント統計情報を表示します。

<Switch> display ipv6 dhcp client statistics interface vlan-interface 2

```
Interface                 : Vlan-interface2
Packets received           : 1
        Reply             : 1
        Advertise         : 0
        Reconfigure       : 0
        Invalid           : 0
Packets sent               : 5
        Solicit           : 0
        Request           : 0
        Renew             : 0
        Rebind            : 0
        Information-request : 5
        Release           : 0
        Decline           : 0
```

表 19-2 コマンド出力

フィールド	説明
Interface	DHCPv6クライアントとして機能するインタフェースです。
Packets Received	受信パケット数です。
Reply	受信した応答パケットの数です。
Advertise	受信したアドバタイズパケットの数です。
Reconfigure	受信した再構成パケットの数です。
Invalid	無効なパケットの数です。
Packets sent	送信されたパケットの数です。

フィールド	説明
Solicit	送信された要請パケットの数です。
Request	送信された要求パケットの数です。
Renew	送信された更新パケットの数です。
Rebind	送信された再バインドパケットの数です。
Information-request	送信された情報要求パケットの数です。
Release	送信されたリリースパケットの数です。
Decline	送信された拒否パケットの数です。

関連コマンド

reset ipv6 dhcp client statistics

19.1.3 ipv6 address dhcp-alloc

Syntax

ipv6 address dhcp-alloc [**option-group** *option-group-number* | **rapid-commit**] *

undo ipv6 address dhcp-alloc

デフォルト

設定なし

View

VLAN interface view

定義済みユーザロール

network-admin

パラメータ

option-group *option-group-number*: DHCPv6 クライアントが設定パラメータを保存するためのダイナミック DHCPv6 オプショングループを作成できるようにし、オプショングループに ID を割り当てます。ID の値の範囲は 1~100 です。このオプションを指定しない場合、DHCPv6 クライアントはダイナミック DHCPv6 オプショングループを作成しません。

rapid-commit: ラピッドアドレスまたはプレフィックスの割り当てをサポートします。

例

IPv6 アドレスの取得に DHCPv6 を使用するように VLAN インタフェース 10 を設定します。DHCPv6 クライアントを設定化して、ラピッドアドレス割り当てをサポートし、取得した設定パラメータ用のダイナミック DHCPv6 オプショングループ 1 を作成します。

<Switch> system-view

[Switch] interface vlan-interface 10

[Switch-Vlan-interface10] ipv6 address dhcp-alloc rapid-commit option-group 1

関連コマンド

display ipv6 dhcp client

19.1.4 reset ipv6 dhcp client statistics

Syntax

reset ipv6 dhcp client statistics [interface *interface-type interface-number*]

View

User view

定義済みユーザロール

network-admin

パラメータ

interface *interface-type interface-number*: タイプと番号でインタフェースを指定します。インタフェースを指定しない場合、このコマンドはすべての DHCPv6 クライアント統計情報をクリアします。

説明

reset ipv6 dhcp client statistics コマンドは、DHCPv6 クライアント統計情報をクリアします。

例

DHCPv6 クライアント統計情報をすべてクリアします。

<Switch> reset ipv6 dhcp client statistics

関連コマンド

display ipv6 dhcp client statistics

目次

このセクションのページは **4-x-x** です。

20 章 HTTP リダイレクト 20-1
20.1 HTTP リダイレクト設定コマンド 20-1
20.1.1 http-redirect https-port 20-1
20.1.2 http-redirect ssl-server-policy 20-2

20章 HTTP リダイレクト

20.1 HTTPリダイレクト設定コマンド

20.1.1 http-redirect https-port

Syntax

http-redirect https-port *port-number*

undo http-redirect https-port

デフォルト

8443

View

System view

定義済みユーザロール

network-admin

パラメータ

port-number: HTTPS リダイレクトサービスが HTTPS リクエストの待ち受ける TCP ポート番号を指定します。ポート番号は 1～65535 の範囲で指定します。

説明

http-redirect https-port コマンドでは、HTTPS リダイレクトするポート番号を指定します。

undo http-redirect https-port コマンドで、6654 ポートにリダイレクトします。🕮 メモ:

undo http-redirect https-port コマンドを実行した場合、デフォルトには戻りません。デフォルトに戻す場合は、**http-redirect https-port 8443** コマンドを実行してください。

TCP ポートを指定する際にウェルノンポートは指定しないでください。**display tcp port** コマンドで使用中の TCP ポート番号を確認することが可能です。

最後に実行した設定が適用されます。

例

HTTPS リダイレクトポートとして 8888 を指定します。

<Switch> system-view

[Switch] http-redirect https-port 8888

20.1.2 http-redirect ssl-server-policy

Syntax

http-redirect ssl-server-policy *policy-name*

undo http-redirect ssl-server-policy

デフォルト

指定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

policy-name: サーバポリシの名前をを指定します。1～31 文字で指定します。

説明

http-redirect ssl-server-policy で、SSL サーバポリシを HTTPS リダイレクトサービス関連付けします。

undo http-redirect ssl-server-policy で、デフォルトに戻します。

関連付けした SSL サーバポリシが存在していない場合、HTTPS リダイレクトは利用できません。最初に SSL サーバポリシを HTTPS リダイレクトサービスと関連付けして、それから SSL サーバポリシを設定することができます。

HTTPS リダイレクトサービスと関連した SSL サーバポリシを変更する場合、新しいポリシが直ちに適用されます。

最後に実行した設定が適用されます。

例

SSL サーバポリシ「**policy1**」を HTTPS リダイレクトサービスと関連付けします。

<Switch> system-view

[Switch] http-redirect ssl-server-policy policy1

QX-S5100G シリーズ Ethernet スイッチ

コマンドマニュアル

5. ルーティングプロトコル

本マニュアルは以下に示す章で構成されています。

01-IP ルーティングの概要
02-スタティックルーティング
03-IPv6 スタティックルーティング
04-RIP
05-OSPF
06-ポリシーベースルーティング
07-RIPng
08-OSPFv3
09-IPv6 ポリシーベースルーティング
10-ルーティングポリシー

目次

このセクションのページは **5-x-x** です。

1 章 IP ルーティングの概要 1-1
1.1 IP ルーティングの概要設定コマンド 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 1-6
1.1.5 display ip routing-table ip-address 1-9
1.1.6 display ip routing-table prefix-list 1-12
1.1.7 display ip routing-table protocol 1-13
1.1.8 display ip routing-table statistics 1-15
1.1.9 display ipv6 rib graceful-restart 1-16
1.1.10 display ipv6 routing-table 1-17
1.1.11 display ipv6 routing-table acl 1-21
1.1.12 display ipv6 routing-table ipv6-address 1-23
1.1.13 display ipv6 routing-table prefix-list 1-26
1.1.14 display ipv6 routing-table protocol 1-28
1.1.15 display ipv6 routing-table statistics 1-29
1.1.16 display rib graceful-restart 1-31
1.1.17 fib lifetime 1-34
1.1.18 non-stop-routing 1-34
1.1.19 protocol lifetime 1-35
1.1.20 reset ip routing-table statistics protocol 1-36
1.1.21 reset ipv6 routing-table statistics protocol 1-37
1.1.22 rib 1-38
1.1.23 routing-table limit 1-38

1章 IP ルーティングの概要

1.1 IPルーティングの概要設定コマンド

1.1.1 address-family ipv4

Syntax

address-family ipv4

undo address-family ipv4

デフォルト

設定なし

View

RIB view

定義済みユーザロール

network-admin

説明

address-family ipv4 コマンドは RIB IPv4 アドレスファミリーを作成し、RIB IPv4 address family view に移行します。

undo address-family ipv4 コマンドは RIB IPv4 アドレスファミリーを削除し、RIB IPv4 address family view のすべての設定を削除します。

例

RIB IPv4 アドレスファミリーを作成し、RIB IPv4 address family view に移行します。

<Switch> system-view

[Switch] rib

[Switch-rib] address-family ipv4

[Switch-rib-ipv4]

1.1.2 address-family ipv6

Syntax

address-family ipv6

undo address-family ipv6

デフォルト

設定なし

View

RIB view

定義済みユーザロール

network-admin

説明

address-family ipv6 コマンドは RIB IPv6 アドレスファミリーを作成し、RIB IPv6 address family view に移行します。

undo address-family ipv6 コマンドは RIB IPv6 アドレスファミリーを削除し、RIB IPv6 address family view のすべての設定を削除します。

例

RIB IPv6 アドレスファミリーを作成し、RIB IPv6 address family view に移行します。

<Switch> system-view

[Switch] rib

[Switch-rib] address-family ipv6

[Switch-rib-ipv6]

1.1.3 display ip routing-table

Syntax

display ip routing-table [**vpn-instance** *vpn-instance-name*] [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

vpn-instance *vpn-instance-name*: 名前で VPN インスタンスを指定します。大文字小文字を区別し、設定範囲は 1～31 文字です。このオプションを指定しない場合、パブリックネットワークのルーティングテーブルの情報を表示します。

verbose: アクティブと非アクティブルートを含むルーティングテーブルの詳細情報を表示します。指定しない場合、アクティブルートの概要情報のみ表示します。

説明

display ip routing-table コマンドはルーティングテーブルの情報を表示します。

例

ルーティングテーブルのアクティブルートの概要情報を表示します。

<Switch> display ip routing-table

```
        Destinations : 13       Routes : 13

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    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
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
```

表 1-1 コマンド出力

フィールド	説明
Destinations	宛先アドレスの数です。
Routes	ルート数です。
Destination/Mask	宛先アドレス/マスク長です。
Proto	ルートを指定したプロトコルです。
Pre	ルートの優先順位です。
Cost	ルートのコストです。
NextHop	ルートのネクストホップアドレスです。

フィールド	説明
Interface	ルートに従って転送されるパケットの出力インタフェースです。
Summary Count	ルート数です。

ルーティングテーブルのすべてのルートの詳細情報を表示します。

<Switch> display ip routing-table verbose

```
        Destinations : 13       Routes : 13

Destination: 0.0.0.0/32
   Protocol: Direct         Process ID: 0
  SubProtID: 0x0                 Age: 08h34m37s
       Cost: 0             Preference: 0
        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

Destination: 1.1.1.0/24
   Protocol: Static         Process ID: 0
  SubProtID: 0x0                 Age: 04h20m37s
       Cost: 0             Preference: 60
        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-interface1
BkTunnel ID: Invalid        BkInterface: N/A

...
```

表 1-2 コマンド出力

フィールド	説明
Destinations	宛先アドレスの数です。
Routes	ルート数です。
Destination	宛先アドレス/マスク長です。
Protocol	ルートを指定したプロトコルです。
SubProtID	ルーティングのサブプロトコルのIDです。
Age	ルーティングテーブルのルートが存在する時間です。
Cost	ルートのコストです。
Preference	ルートの優先順位です。
Tag	ルートタグです。
State	ルート状態です。 • **Active**—アクティブなユニキャストルートです。 • **Adv**—配信できるルートです。 • **Inactive**—非アクティブルートです。 • **NoAdv**—ルータが配信できないルートです。 • **Vrrp**—VRRPによって作成されたルートです。 • **Nat**—NATによって作成されたルートです。 • **TunE**—トンネルです。
OrigTblID	もとのルーティングテーブルIDです。
OrigVrf	ルートが属するもとのVPNです。
TableID	ルーティングテーブルのIDです。
OrigAs	もとのAS番号です。
NibID	ネクストホップのIDです。
LastAs	最新のAS番号です。
AttrID	属性IDです。
Neighbor	ルーティングプロトコルによって決定された隣接アドレスです。

フィールド	説明
Flags	ルートのフラグです。
OrigNextHop	ルートのネクストホップアドレスです。
RealNextHop	ルートの実際のネクストホップです。
BkLabel	バックアップラベルです。
BkNexthop	バックアップネクストホップです。
Interface	ルートに従って転送されるパケットの出力インタフェースです。
BkTunnel ID	バックアップトンネルIDです。
BkInterface	バックアップ出力インタフェースです。
FtnIndex	FTNエントリのインデックスです。
Summary Count	ルート数です。

1.1.4 display ip routing-table acl

Syntax

display ip routing-table [**vpn-instance** *vpn-instance-name*] **acl** *acl-number* [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

vpn-instance *vpn-instance-name*: 名前で VPN インスタンスを指定します。大文字小文字を区別し、設定範囲は 1～31 文字です。このオプションを指定しない場合、パブリックネットワークのルーティングテーブルの情報を表示します。

acl-number: 標準 ACL を指定します。設定範囲は 2000～2999 です。

verbose: 標準 ACL によって許可されたすべてのルートの詳細情報を表示します。指定しない場合、標準 ACL によって許可されたアクティブルートの概要情報のみ表示します。

説明

display ip routing-table acl コマンドは指定された標準 ACL によって許可されたルートの情報を表示します。

指定された ACL が存在しない、あるいはルールが設定されていない場合、すべてのルートの情報を表示します。

例

標準 ACL 2000 を定義し、ルートのフィルタリングのルールを設定します。

<Switch> system-view

[Switch] acl number 2000

[Switch-acl-basic-2000] rule permit source 192.168.1.0 0.0.0.255

[Switch-acl-basic-2000] rule deny source any

標準 ACL 2000 によって許可されたアクティブルートの概要情報を表示します。

[Switch-acl-basic-2000] display ip routing-table acl 2000

```
Routes Matched by Access control list : 2000
Summary Count : 4

Destination/Mask    Proto  Pre  Cost        NextHop         Interface
192.168.1.0/24      Direct 0    0           192.168.1.111   Vlan1
192.168.1.0/32      Direct 0    0           192.168.1.111   Vlan1
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   Vlan1
```

コマンド出力は表 1-1 を参照してください。

標準 ACL 2000 によって許可されたすべてのルートの詳細情報を表示します。

<Switch> display ip routing-table acl 2000 verbose

```
Routes Matched by Access control list : 2000
Summary Count : 4

Destination: 192.168.1.0/24
   Protocol: Direct         Process ID: 0
  SubProtID: 0x1                 Age: 04h20m37s
      Cost: 0             Preference: 0
       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-interface1
BkTunnel ID: Invalid       BkInterface: N/A

Destination: 192.168.1.0/32
   Protocol: Direct         Process ID: 0
  SubProtID: 0x0                 Age: 04h20m37s
       Cost: 0             Preference: 0
        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-interface1
BkTunnel ID: Invalid       BkInterface: N/A

Destination: 192.168.1.111/32
   Protocol: Direct         Process ID: 0
  SubProtID: 0x1                 Age: 04h20m37s
       Cost: 0             Preference: 0
        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

Destination: 192.168.1.255/32
   Protocol: Direct         Process ID: 0
  SubProtID: 0x0                 Age: 04h20m37s
       Cost: 0             Preference: 0
        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-interface1
BkTunnel ID: Invalid        BkInterface: N/A
```

コマンド出力は表 1-2 を参照してください。

1.1.5 display ip routing-table ip-address

Syntax

display ip routing-table [**vpn-instance** *vpn-instance-name*] *ip-address* [*mask* | *mask-length*] [**longer-match**] [**verbose**]

display ip routing-table [**vpn-instance** *vpn-instance-name*] *ip-address1* **to** *ip-address2* [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

vpn-instance *vpn-instance-name*: 名前で VPN インスタンスを指定します。大文字小文字を区別し、設定範囲は 1～31 文字です。このオプションを指定しない場合、パブリックネットワークのルーティングテーブルの情報を表示します。

ip-address: 宛先 IP アドレスを指定します。ドットで区切り、10 進数で指定します。

mask: IP アドレスマスクを指定します。ドットで区切り、10 進数で指定します。

mask-length: マスク長を指定します。設定範囲は 0～32 です。

longer-match: マスク長が最長のルートエントリを表示します。

ip-address1 **to** *ip-address2*: 宛先 IP アドレス範囲を指定します。

verbose: アクティブと非アクティブルートを含むルーティングテーブルの詳細情報を表示します。指定しない場合、アクティブルートの概要情報のみ表示します。

説明

display ip routing-table *ip-address* コマンドは指定した宛先アドレスのルート情報を表示します。

display ip routing-table *ip-address1* **to** *ip-address2* コマンドは宛先アドレス範囲のルート情報を表示します。

異なるパラメータを使用してコマンドを実行すると、異なる出力が得られます。

- **display ip routing-table** *ip-address*
  - □ システムは、入力された宛先 IP アドレスと各アクティブルートエントリのサブネットマスクの AND 演算を行います。
  - □ 各アクティブルートエントリの宛先 IP アドレスと対応するサブネットマスクの AND 演算を行います。

1 つのエントリに対する 2 つの演算結果が同じである場合、エントリが表示されます。

- **display ip routing-table** *ip-address mask*
  - □ システムは、入力された宛先 IP アドレスと入力されたサブネットマスクの AND 演算を行います。
  - □ 各アクティブルートエントリの宛先 IP アドレスと入力されたサブネットマスクの AND 演算を行います。

1 つのエントリに対する 2 つの演算結果が同じで､サブネットマスクが入力されたサブネットマスク以下の場合、このエントリが表示されます。

- **display ip routing-table** *ip-address* **longer-match**
  - □ システムは、入力された宛先 IP アドレスと各アクティブルートエントリのサブネットマスクの AND 演算を行います。
  - □ システムは、各アクティブルートエントリの宛先 IP アドレスと対応するサブネットマスクの AND 演算を行います。

複数のエントリに対する 2 つの演算結果が同じ場合、最もマスク長の長いエントリが表示されます。

- **display ip routing-table** *ip-address mask* **longer-match**
  - □ システムは、入力された宛先 IP アドレスと入力されたサブネットマスクの AND 演算を行います。
  - □ 各アクティブルートエントリの 宛先 IP アドレスと入力されたサブネットマスクの AND 演算を行います。

入力されたサブネットマスク以下のマスクを持つ複数のエントリに対する 2 つの演算結果が同じ場合、マスク長が最長のエントリが表示されます。

- **display ip routing-table** *ip-address1* **to** *ip-address2*

指定した範囲 *ip-address1*/32～*ip-address2*/32 の宛先アドレスのアクティブルートエントリを表示します。

例

宛先 IP アドレス 11.1.1.1 のルートエントリの概要情報を表示します。

<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
```

宛先 IP アドレス 11.0.0.1 およびマスク長 20 のルートの概要情報を表示します。

```
<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
```

宛先アドレス 11.0.0.1 のマスク長が最長のルートの概要情報を表示します。

```
<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
```

宛先アドレス 11.0.0.1、マスク長 20、マスク長が最長のルートの概要情報を表示します。

```
<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
```

宛先アドレス範囲 1.1.1.0～5.5.5.0 の宛先アドレスのルートの概要情報を表示します。

```
<Switch> display ip routing-table 1.1.1.0 to 5.5.5.0

Summary Count : 6

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
3.3.3.0/24          Direct 0    0           3.3.3.1         Vlan2
3.3.3.1/32          Direct 0    0           127.0.0.1       InLoop0
4.4.4.0/24          Direct 0    0           4.4.4.1         Vlan1
4.4.4.1/32          Direct 0    0           127.0.0.1       InLoop0
```

コマンド出力は表 1-1 を参照してください。

1.1.6 display ip routing-table prefix-list

Syntax

display ip routing-table [**vpn-instance** *vpn-instance-name*] **prefix-list** *prefix-list-name* [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

vpn-instance *vpn-instance-name*: 名前で VPN インスタンスを指定します。大文字小文字を区別し、設定範囲は 1～31 文字です。このオプションを指定しない場合、パブリックネットワークのルーティングテーブルの情報を表示します。

prefix-list-name: IP プレフィックスリストを指定します。設定範囲は 1～63 です。大文字、小文字を区別します。

verbose: IP プレフィックスリストによって許可されたすべてのルートの詳細情報を表示します。指定しない場合、IP プレフィックスリストによって許可されたアクティブルートの概要情報を表示します。

説明

display ip routing-table prefix-list コマンドはプレフィックスリストによって許可されたルートの情報を表示します。

指定した IP プレフィックスリストが存在しない場合、すべてのルートの情報を表示します。

例

ルート 1.1.1.0/24 を許可するプレフィックスリスト test を作成します。

<Switch> system-view

[Switch] ip prefix-list test permit 1.1.1.0 24

IP プレフィックスリストによって許可されたアクティブルートの概要情報を表示します。

[Switch] display ip routing-table prefix-list test

```
Routes Matched by 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         Vlan2
```

コマンド出力は表 1-1 を参照してください。

IP プレフィックスリストによって許可されたすべてのルートの詳細情報を表示します。

[Switch] display ip routing-table prefix-list test verbose

```
Routes Matched by Prefix list : test
Summary Count : 1

Destination: 1.1.1.0/24
   Protocol: Direct         Process ID: 0
  SubProtID: 0x1                 Age: 04h20m37s
       Cost: 0             Preference: 0
        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-interface2
BkTunnel ID: Invalid        BkInterface: N/A
```

コマンド出力は表 1-2 を参照してください。

1.1.7 display ip routing-table protocol

Syntax

display ip routing-table [**vpn-instance** *vpn-instance-name*] **protocol** *protocol* [**inactive** | **verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

vpn-instance *vpn-instance-name*: 名前で VPN インスタンスを指定します。大文字小文字を区別し、設定範囲は 1～31 文字です。このオプションを指定しない場合、パブリックネットワークのルーティングテーブルの情報を表示します。

protocol: ルーティングプロトコルを指定します。direct、rip、static を指定できます。

inactive: 非アクティブルートの情報を表示します。指定しない場合、アクティブルートと非アクティブルートの情報を表示します。

verbose: ルーティングテーブルの詳細情報を表示します。指定しない場合、ルーティングの概要情報を表示します。

説明

display ip routing-table protocol コマンドはプロトコルによって指定されたルートの情報を表示します。

例

ダイレクトルートの概要情報を表示します。

<Switch> display ip routing-table protocol direct

```
Summary Count : 13

Direct Routing Table Status : <Active>
Summary Count : 13

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
192.168.80.0/24     Direct 0    0           192.168.80.10   Vlan1
192.168.80.0/32     Direct 0    0           192.168.80.10   Vlan1
192.168.80.10/32    Direct 0    0           127.0.0.1       InLoop0
192.168.80.255/32   Direct 0    0           192.168.80.10   Vlan1

Direct Routing Table Status : <Inactive>
Summary Count : 0
```

スタティックルートの概要情報を表示します。

<Switch> display ip routing-table protocol static

```
Summary Count : 2

Static Routing Table Status : <Active>
Summary Count : 0

Static Routing Table Status : <Inactive>
Summary Count : 2

Destination/Mask    Proto  Pre  Cost        NextHop         Interface
1.2.3.0/24          Static 60   0           1.2.4.5         Vlan10
3.0.0.0/8           Static 60   0           2.2.2.2         Vlan1
```

コマンド出力は表 1-1 を参照してください。

1.1.8 display ip routing-table statistics

Syntax

display ip routing-table [**vpn-instance** *vpn-instance-name*] **statistics**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

vpn-instance *vpn-instance-name*: 名前で VPN インスタンスを指定します。大文字小文字を区別し、設定範囲は 1～31 文字です。このオプションを指定しない場合、パブリックネットワークの IPv4 ルートの統計情報を表示します。

説明

display ip routing-table statistics コマンドは IPv4 ルートの統計情報を表示します。

例

パブリックネットワークの IPv4 ルートの統計情報を表示します。

<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
ISIS       0          0          0          0
BGP        0          0          0          0
Total      15         15         35         20
```

表 1-3 コマンド出力

フィールド	説明
Total prefixes	プレフィックス総数です。
Active prefixes	アクティブプレフィックス数です。
Proto	ルートを指定したプロトコルです。
route	プロトコルによって指定されたルート数です。
active	アクティブルート数です。
added	ルータが起動あるいはルーティングテーブルが最後に削除した後にルーティングテーブルに追加されたルート数です。
deleted	deletedと記載されたルート数です。一定期間後に削除されます。
Total	ルートの総数です。

1.1.9 display ipv6 rib graceful-restart

Syntax

display ipv6 rib graceful-restart

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display ipv6 rib graceful-restart コマンドは IPv6 RIB GR の状態情報を表示します。

例

IPv6 RIB GR の状態情報を表示します。

<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+      480      31   End      No/No
```

コマンド出力は表 1-7 を参照してください。

1.1.10 display ipv6 routing-table

Syntax

display ipv6 routing-table [**vpn-instance** *vpn-instance-name*] [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

vpn-instance *vpn-instance-name*: 名前で VPN インスタンスを指定します。大文字小文字を区別し、設定範囲は 1～31 文字です。このオプションを指定しない場合、パブリックネットワークの IPv4 ルートの統計情報を表示します。

verbose: アクティブと非アクティブルートを含むルーティングテーブルの詳細情報を表示します。指定しない場合、アクティブルートの概要情報のみ表示します。

説明

display ipv6 routing-table コマンドは IPv6 ルーティングテーブルの情報を表示します。

例

IPv6 ルーティングテーブルのアクティブルートの概要情報を表示します。

<Switch> display ipv6 routing-table

```
Destinations : 3 Routes : 3

Destination: ::1/128                                Protocol  : Direct
NextHop    : ::1                                   Preference: 0
Interface  : InLoop0                                Cost      : 0

Destination: FE80::/10                              Protocol  : Direct
NextHop    : ::                                    Preference: 0
Interface  : NULL0                                  Cost      : 0

Destination: FF00::/8                               Protocol  : Direct
NextHop    : ::                                    Preference: 0
Interface  : NULL0                                  Cost      : 0
```

表 1-4 コマンド出力

フィールド	説明
Destinations	宛先アドレスの数です。
Routes	ルート数です。
Destination	宛先ネットワークあるいはホストのIPv6アドレス、プレフィックスです。
NextHop	ルートのネクストホップアドレスです。
Preference	ルートの優先順位です。
Interface	ルートに従って転送されるパケットの出力インタフェースです。
Protocol	ルートを追加したプロトコルです。 ● **O_INTRA**—OSPFイントラエリアルートです。 ● **O_INTER**—OSPFインターエリアルートです。 ● **O_ASE1**—OSPF エクスターナルタイプ1ルートです。 ● **O_ASE2**—OSPFエクスターナルタイプ2ルートです。 ● **O_NSSA1**—OSPF NSSAエクスターナルタイプ1ルートです。 ● **O_NSSA2**—OSPF NSSAエクスターナルタイプ2ルートです。 ● **O_SUM**—OSPFサマリルートです。 ● **IS_L1**—IS-IS レベル1ルートです。 ● **IS_L2**—IS-IS レベル2ルートです。 ● **IS_SUM**—IS-ISサマリルートです。
Cost	ルートのコストです。

フィールド	説明
Summary Count	ルート数です。

ルーティングテーブルのすべてのルートの詳細情報を表示します。

<Switch> display ipv6 routing-table verbose

```
Destinations : 3 Routes : 3

Destination: ::1/128
   Protocol: Direct         Process ID: 0
  SubProtID: 0x0                 Age: 00h53m50s
       Cost: 0             Preference: 0
        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

Destination: FE80::/10
   Protocol: Direct         Process ID: 0
  SubProtID: 0x0                 Age: 00h53m50s
       Cost: 0             Preference: 0
        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: NULL0
BkTunnel ID: Invalid        BkInterface: N/A

Destination: FF00::/8
   Protocol: Direct         Process ID: 0
  SubProtID: 0x0                 Age: 00h53m50s
```

```
      Cost: 0            Preference: 0
       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
```

表 1-5 コマンド出力

フィールド	説明
Destination	宛先ネットワークあるいはホストのIPv6アドレス、プレフィックスです。
Protocol	ルートを追加したプロトコルです。
SubProtID	ルーティングのサブプロトコルのIDです。
Age	ルーティングテーブルのルートが存在する時間です。
Cost	ルートのコストです。
Preference	ルートの優先順位です。
IpPre	IPプレシーデンスです。
QosLocalID	ローカルQoS IDです。
Tag	ルートのタグです。
State	ルートの状態です。 ● **Active**—アクティブなユニキャストルートです。 ● **Adv**—配信できるルートです。 ● **Inactive**—非アクティブルートです。 ● **NoAdv**—ルータが配信できないルートです。 ● **Vrrp**— VRRPによって作成されたルートです。 ● **Nat**— NATによって作成されたルートです。 ● **TunE**—トンネルです。
OrigTblID	もとのルーティングテーブルIDです。
OrigVrf	ルートが属するもとのVPNです。

フィールド	説明
TableID	ルーティングテーブルのIDです。
OrigAs	もとのAS番号です。
NibID	ネクストホップのIDです。
LastAs	最新のAS番号です。
AttrID	属性IDです。
Neighbor	ルーティングプロトコルによって決定された隣接アドレスです。
Flags	ルートのフラグです。
OrigNextHop	ルートのネクストホップアドレスです。
RealNextHop	ルートの実際のネクストホップです。
BkLabel	バックアップラベルです。
BkNexthop	バックアップネクストホップです。
Interface	ルートに従って転送されるパケットの出力インタフェースです。
BkTunnel ID	バックアップトンネルIDです。
BkInterface	バックアップ出力インタフェースです。
Summary Count	ルート数です。

1.1.11 display ipv6 routing-table acl

Syntax

display ipv6 routing-table [**vpn-instance** *vpn-instance-name*] **acl** *acl6-number* [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

vpn-instance *vpn-instance-name*: 名前で VPN インスタンスを指定します。大文字小文字を区別し、設定範囲は 1～31 文字です。このオプションを指定しない場合、パブリックネットワークの IPv4 ルートの統計情報を表示します。

acl6-number: 標準 IPv6 ACL を指定します。設定範囲は 2000～2999 です。

verbose: 標準 IPv6 ACL によって許可されたすべてのルートの詳細情報を表示します。指定しない場合、標準 IPv6 ACL によって許可されたアクティブルートの概要情報のみ表示します。

説明

display ipv6 routing-table acl コマンドは指定された標準 IPv6 ACL によって許可されたルートの情報を表示します。

指定された IPv6 ACL が存在しない、あるいはルールが設定されていない場合、すべての IPv6 ルートの情報を表示します。

例

標準 IPv6 ACL 2000 によって許可されたアクティブルートの概要情報を表示します。

<Switch> display ipv6 routing-table acl 2000

```
Routes Matched by Access control list : 2000
Summary Count : 3

Destination : ::1/128                          Protocol  : Direct
NextHop     : ::1                             Preference: 0
Interface   : InLoop0                         Cost      : 0

Destination : 1:1::/64                         Protocol  : Static
NextHop     : ::                              Preference: 60
Interface   : NULL0                           Cost      : 0
```

コマンド出力は表 1-4 を参照してください。

標準 IPv6 ACL 2000 によって許可されたすべてのルートの詳細情報を表示します。

<Switch> display ipv6 routing-table acl 2000 verbose

```
Routes Matched by Access control list : 2000
Summary Count : 3

Destination: ::1/128
   Protocol: Direct         Process ID: 0
  SubProtID: 0x0                 Age: 08h57m19s
      Cost: 0             Preference: 0
```

```
      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

Destination: 1:1::/64
   Protocol: Static        Process ID: 0
  SubProtID: 0x2                Age: 08h57m19s
       Cost: 0            Preference: 60
      Tag: 0                State: Active Adv
  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: NULL0
BkTunnel ID: Invalid      BkInterface: N/A
```

コマンド出力は表 1-5 を参照してください。

1.1.12 display ipv6 routing-table ipv6-address

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**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

vpn-instance *vpn-instance-name*: 名前で VPN インスタンスを指定します。大文字小文字を区別し、設定範囲は 1～31 文字です。このオプションを指定しない場合、パブリックネットワークの IPv4 ルートの統計情報を表示します。

ipv6-address: 宛先 IPv6 アドレスを指定します。

prefix-length: プレフィックス長を指定します。設定範囲は 0～28 です。

longer-match: プレフィックス長が最長のルートエントリを表示します。

ipv6-address1 **to** *ipv6-address2*: 宛先 IPv6 アドレス範囲を指定します。

verbose: アクティブと非アクティブルートを含むルーティングテーブルの詳細情報を表示します。指定しない場合、アクティブルートの概要情報のみ表示します。

説明

display ipv6 routing-table *ipv6-address* コマンドは指定した宛先 IPv6 アドレスのルート情報を表示します。

display ipv6 routing-table *ipv6-address1* **to** *ipv6-address2* コマンドは宛先アドレス範囲のルート情報を表示します。

異なるパラメータを使用してコマンドを実行すると、異なる出力が得られます。

- **display ipv6 routing-table** *ipv6-address*
  - □ システムは、入力された宛先 IPv6 アドレスと各アクティブルートエントリのプレフィックスの AND 演算を行います。
  - □ 各アクティブルートエントリの宛先 IPv6 アドレスとエントリのプレフィックスの AND 演算を行います。

1 つのエントリに対する 2 つの演算結果が同じである場合、エントリが表示されます。

- **display ipv6 routing-table** *ipv6-address prefix-length*
  - □ システムは、入力された宛先 IPv6 アドレスと入力されたプレフィックス長の AND 演算を行います。
  - □ 各アクティブルートエントリの宛先 IPv6 アドレスと入力されたプレフィックス長の AND 演算を行います。

1 つのエントリに対する 2 つの演算結果が同じで､入力されたプレフィックス以下の場合、このエントリが表示されます。

- **display ipv6 routing-table** *ipv6-address* **longer-match**
  - □ システムは、入力された宛先 IPv6 アドレスと各アクティブルートエントリのプレフィックス長の AND 演算を行います。
  - □ システムは、各アクティブルートエントリの宛先 IPv6 アドレスとエントリのプレフィックス長の AND 演算を行います。

複数のエントリに対する 2 つの演算結果が同じ場合、最もプレフィックスの長いエントリが表示されます。

- **display ipv6 routing-table** *ipv6-address prefix-length* **longer-match**

- □ システムは、入力された宛先 IPv6 アドレスと入力されたプレフィックス長の AND 演算を行います。
- □ 各アクティブルートエントリの 宛先 IPv6 アドレスと入力されたプレフィックス長の AND 演算を行います。

入力されたプレフィックス長以下のプレフィックス長を持つ複数のエントリに対する 2 つの演算結果が同じ場合、プレフィックス長が最長のエントリが表示されます。

- **display ipv6 routing-table** *ipv6-address1* **to** *ipv6-address2*

指定した範囲 *ipv6-address1*/128～*ipv6-address2*/128 の宛先アドレスのルートエントリを表示します。

例

宛先 IPv6 アドレス 10::1 127 のルートエントリの概要情報を表示します。

<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
```

宛先 IPv6 アドレス 10::1 およびプレフィックス長 127 のプレフィックス長が最長のルートの概要情報を表示します。

<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
```

宛先アドレス範囲 100::～300::の宛先アドレスのルートの概要情報を表示します。

<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
```

コマンド出力は表 1-4 を参照してください。

1.1.13 display ipv6 routing-table prefix-list

Syntax

display ipv6 routing-table [**vpn-instance** *vpn-instance-name*] **prefix-list** *prefix-list-name* [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

vpn-instance *vpn-instance-name*: 名前で VPN インスタンスを指定します。大文字小文字を区別し、設定範囲は 1～31 文字です。このオプションを指定しない場合、パブリックネットワークの IPv4 ルートの統計情報を表示します。

prefix-list-name: IPv6 プレフィックスリストを指定します。設定範囲は 1～63 です。大文字、小文字を区別します。

verbose: IPv6 プレフィックスリストによって許可されたすべての IPv6 ルートの詳細情報を表示します。指定しない場合、IPv6 プレフィックスリストによって許可されたアクティブ IPv6 ルートの概要情報を表示します。

説明

display ipv6 routing-table prefix-list コマンドは IPv6 プレフィックスリストによって許可された IPv6 ルートの情報を表示します。

指定した IPv6 プレフィックスリストが存在しない場合、すべてのルートの情報を表示します。

例

プレフィックス::1/128 を許可する IPv6 プレフィックスリスト test を作成します。

<Switch> system-view

[Switch] ipv6 prefix-list test permit ::1 128

IPv6 プレフィックスリストによって許可されたアクティブ IPv6 ルートの概要情報を表示します。

[Switch] display ipv6 routing-table prefix-list test

```
Routes Matched by Prefix list : test
Summary Count : 1

Destination: ::1/128                              Protocol  : Direct
NextHop    : ::1                                 Preference: 0
Interface  : InLoop0                              Cost      : 0
```

コマンド出力は表 1-4 を参照してください。

IPv6 プレフィックスリストによって許可されたすべてのルートの詳細情報を表示します。

[Switch] display ipv6 routing-table prefix-list test verbose

```
Routes Matched by Prefix list : test
Summary Count : 1

Destination: ::1/128
   Protocol: Direct         Process ID: 0
  SubProtID: 0x0                 Age: 08h57m19s
       Cost: 0             Preference: 0
        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
```

コマンド出力は表 1-5 を参照してください。

1.1.14 display ipv6 routing-table protocol

Syntax

display ipv6 routing-table [**vpn-instance** *vpn-instance-name*] **protocol** *protocol* [**inactive** | **verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

vpn-instance *vpn-instance-name*: 名前で VPN インスタンスを指定します。大文字小文字を区別し、設定範囲は 1～31 文字です。このオプションを指定しない場合、パブリックネットワークの IPv4 ルートの統計情報を表示します。

protocol: ルーティングプロトコルを指定します。direct、ospfv3、ripng、static を指定できます。

inactive: 非アクティブルートの情報を表示します。指定しない場合、アクティブルートと非アクティブルートの情報を表示します。

verbose: ルーティングテーブルの詳細情報を表示します。指定しない場合、ルーティングの概要情報を表示します。

説明

display ipv6 routing-table protocol コマンドはプロトコルによって指定された IPv6 ルートの情報を表示します。

例

ダイレクトルートの概要情報を表示します。

<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  : NULL0                              Cost      : 0

Destination: FF00::/8                           Protocol  : Direct
NextHop    : ::                                 Preference: 0
Interface  : NULL0                              Cost      : 0

Direct Routing Table Status : <Inactive>
Summary Count : 0
```

スタティックルートの概要情報を表示します。

<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  : Vlan2                              Cost      : 0

Destination: 2::2/128                           Protocol  : Static
NextHop    : fe80::3                            Preference: 60
Interface  : Vlan2                              Cost      : 0

Destination: 3::3/128                           Protocol  : Static
NextHop    : 2::2                               Preference: 60
Interface  : Vlan2                              Cost      : 0

Static Routing table Status : <Inactive>
Summary Count : 0
```

コマンド出力は表 1-4 を参照してください。

1.1.15 display ipv6 routing-table statistics

Syntax

display ipv6 routing-table [**vpn-instance** *vpn-instance-name*] **statistics**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

vpn-instance *vpn-instance-name*: 名前で VPN インスタンスを指定します。大文字小文字を区別し、設定範囲は 1～31 文字です。このオプションを指定しない場合、パブリックネットワークの IPv4 ルートの統計情報を表示します。

説明

display ipv6 routing-table statistics コマンドは IPv6 ルートの統計情報を表示します。

例

パブリックネットワークの IPv6 ルートの統計情報を表示します。

<Switch> display ipv6 routing-table statistics

```
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
```

表 1-6 コマンド出力

フィールド	説明
Total prefixes	プレフィックスの総数です。
Active prefixes	アクティブプレフィックス数です。
Proto	ルートを指定したプロトコルです。
route	プロトコルによって指定されたルート数です。
active	アクティブルート数です。
added	ルータが起動あるいはルーティングテーブルが最後に削除した後にルーティングテーブルに追加されたルート数です。
deleted	deletedと記載されたルート数です。一定期間後に削除されます。

フィールド	説明
Total	ルートの総数です。

1.1.16 display rib graceful-restart

Syntax

display rib graceful-restart

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display rib graceful-restart コマンドは RIB GR の状態情報を表示します。

例

IPv6 RIB GR の状態情報を表示します。

<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        480      31   End      No/No
 6    LDP        480      35   End      No/No
 7    SLSP       480      29   End      No/No
```

表 1-7 コマンド出力

フィールド	説明
RIB GR state	RIB GRの状態です。 ● **Start**—GRが起動します。 ● **IGP end**—すべてのIGPプロトコルがGRを完了します。 ● **VPN-triggering end**—VPNルートによって開始した最適ルートの選定が完了します。 ● **VPN-calculation end**—最適VPNルートの選定が完了します。 ● **Routing protocol end**—すべてのルーティングプロトコルがGRを完了します。 ● **NSR-calculation unfinished**—NSRが最適ルートの選定を完了していません。 ● **Triggering start**—開始したすべてのルートの選定が行われます。 ● **Triggering end**—開始したすべてのルートの選定が完了します。 ● **Phase1-calculation end**—最適ルートの選定のフェーズ1が完了します。 ● **All end**—すべてのプロトコルがGRを完了します。 ● **Phase2-calculation end**—最適ルートの選定のフェーズ1が完了します。

フィールド	説明
RCOM GR state	RCOM GRの状態です。 ● **Start**—GRが開始します。 ● **VPN-calculation end**—最適VPNルートの選定が完了します。 ● **VPN-notification end**—VPNルートがルート管理モジュールに配送されています。 ● **Routing protocol end**—すべてのルーティングプロトコルがGRを完了します。 ● **NSR-calculation unfinished**—NSRが最適ルートの選定を完了していません。 ● **Phase1-calculation end**—最適ルートの選定のフェーズ1が完了します。 ● **Notification end**—すべてのルートがルート管理モジュールに配送されています。 ● **Phase2-calculation end**—最適ルートの選定のフェーズ2が完了します。 ● **Flush start**—ルートをFIBに配信し始めます。 ● **Flush end**—FIBへのルートの配信が完了します。
No.	プロトコル番号です。
Lifetime	GRの間でのRIPのルート/ラベルの生存時間です。単位は秒です。
FD	プロトコルとRIB間で処理を行います。
State	プロトコルのGRの状態です。 ● **Init**—初期状態です。 ● **Listen**—リスニング状態です。 ● **Idle**－アイドル状態です。 ● **Active**－アクティブ状態です。 ● **Start**—GRが開始します。 ● **End**—GRが完了します。
Start/End	メッセージ送信状態です。 ● **No**—メッセージが送信されていません。 ● **Yes**—メッセージが送信されています。

1.1.17 fib lifetime

Syntax

fib lifetime *seconds*

undo fib lifetime

デフォルト

600 秒

View

RIB IPv4 address family view、RIB IPv6 address family view

定義済みユーザロール

network-admin

パラメータ

seconds: FIB のルートの最大生存時間を設定します。設定範囲は、0～900 秒です。0 に設定された際は、プロトコルまたは FIB プロセスが転換した後、FIB エントリはすぐにエージアウトします。

説明

fib lifetime コマンドは、FIB の IPv4 または IPv6 ルートの最大生存時間を設定します。

undo fib lifetime コマンドは、設定をデフォルトに戻します。

プロトコルまたは RIB プロセスの転換が発生し GR が設定されていない際は、このコマンドで指定された時間が経過すると FIB エントリはエージアウトします。

例

FIB の IPv4 ルートの最大生存時間を 60 秒に設定します。

<Switch> system-view

[Switch] rib

[Switch-rib] address-family ipv4

[Switch-rib-ipv4] fib lifetime 60

1.1.18 non-stop-routing

Syntax

non-stop-routing

undo non-stop-routing

デフォルト

無効

View

RIB IPv4 address family view

RIB IPv6 address family view

定義済みユーザロール

network-admin

説明

non-stop-routing コマンドは RIB NSR を有効にします。

undo non-stop-routing コマンドは RIB NSR を無効にします。

例

#RIB IPv4 アドレスファミリーの NSR を有効にします。

<Switch> system-view

[Switch] rib

[Switch-rib] address-family ipv4

[Switch-rib-ipv4] non-stop-routing

1.1.19 protocol lifetime

Syntax

protocol protocol lifetime *seconds*

undo protocol protocol lifetime

デフォルト

480 秒

View

RIB IPv4 address family view, RIB IPv6 address family view

定義済みユーザロール

network-admin

パラメータ

seconds: RIB のルートと、ラベルの生存時間を指定します。設定範囲は 0～900 秒です。0 を指定した場合、プロトコルの切り替わりが発生した場合、RIB はすぐにエージアウトします。

説明

protocol lifetime コマンドは RIB の IPv4 ルートあるいは IPv6 ルートと、ラベルの最大生存時間を設定します。

undo protocol lifetime コマンドはデフォルトに戻します。

GR が有効である場合、プロトコルは設定された生存時間内に GR が完了し、RIB にすべてのルートエントリをインストールすることができます。

例

OSPF ルートとラベルの最大生存時間を 60 秒に設定します。

<Switch> system-view

[Switch] rib

[Switch-rib] address-family ipv4

[Switch-rib-ipv4] protocol ospf lifetime 60

1.1.20 reset ip routing-table statistics protocol

Syntax

reset ip routing-table statistics protocol [**vpn-instance** *vpn-instance-name*] { *protocol* | **all** }

View

User view

定義済みユーザロール

network-admin

パラメータ

vpn-instance *vpn-instance-name*: 名前で VPN インスタンスを指定します。大文字小文字を区別し、設定範囲は 1～31 文字です。このオプションを指定しない場合、パブリックネットワークの IPv4 ルートの統計情報を表示します。

protocol: ルーティングプロトコルのルートの統計情報を削除します。direct、ospf、rip、static を指定できます。

all: すべての IPv4 ルーティングプロトコルのルートの統計情報を削除します。

説明

reset ip routing-table statistics protocol コマンドは IPv4 ルートの統計情報を削除します。

例

パブリックネットワークのすべての IPv4 ルートの統計情報を削除します。

<Switch> reset ip routing-table statistics protocol all

1.1.21 reset ipv6 routing-table statistics protocol

Syntax

reset ipv6 routing-table statistics protocol [**vpn-instance** *vpn-instance-name*] { *protocol* | **all** }

View

User view

定義済みユーザロール

network-admin

パラメータ

vpn-instance *vpn-instance-name*: 名前で VPN インスタンスを指定します。大文字小文字を区別し、設定範囲は 1～31 文字です。このオプションを指定しない場合、パブリックネットワークの IPv4 ルートの統計情報を表示します。

protocol: IPv6 ルーティングプロトコルのルートの統計情報を削除します。direct、ospfv3、ripng、static を指定できます。

all: すべての IPv6 ルーティングプロトコルのルートの統計情報を削除します。

説明

reset ipv6 routing-table statistics protocol コマンドは IPv6 ルートの統計情報を削除します。

例

パブリックネットワークのすべての IPv6 ルートの統計情報を削除します。

<Switch> reset ipv6 routing-table statistics protocol all

1.1.22 rib

Syntax

rib

undo rib

View

System view

定義済みユーザロール

network-admin

説明

rib コマンドは、RIB view に移行します。

undo rib コマンドは、RIB view ですべての設定を削除します。

例

RIB view に移行します。

<Switch> system-view

[Switch] rib

[Switch-rib]

1.1.23 routing-table limit

Syntax

routing-table limit *number* **simply-alert**

undo routing-table limit

デフォルト

設定なし

View

RIB IPv4 address family view

RIB IPv6 address family view

定義済みユーザロール

network-admin

パラメータ

number: 装置がサポートするアクティブ IPv4/IPv6 ルートの最大数を指定します。設定範囲は 1～4294967295 です。

simply-alert: 装置がアクティブなルートを受け入れながら、アクティブな IPv4/IPv6 ルートの数が最大数を超えたときにログメッセージを作成できるようにします。

説明

routing-table limit コマンドは装置がサポートするアクティブな IPv4/IPv6 ルートの最大数を設定します。

undo routing-table limit コマンドはデフォルトに戻します。

RIB IPv4 アドレスファミリービューでの設定は、パブリックネットワークとすべての VPN インスタンスのアクティブ IPv4 ルートの数を制限します。

RIB IPv6 アドレスファミリービューでの設定は、パブリックネットワークとすべての VPN インスタンスのアクティブ IPv6 ルートの数を制限します。

例

RIB IPv4 アドレスファミリビューで、パブリックネットワークおよびすべての VPN インスタンスのアクティブな IPv4 ルートの最大数を 1000 に設定します。装置はまだ新しいアクティブルートを受け入れますが、アクティブルートの最大数を超えるとシステムログメッセージを作成します。

<Switch> system-view

[Switch] rib

[Switch-rib] address-family ipv4

[Switch-rib-ipv4] routing-table limit 1000 simply-alert

目次

このセクションのページは **5-x-x** です。

2章 スタティックルーティング 2-1
2.1 スタティックルーティング設定コマンド 2-1
2.1.1 delete static-routes all 2-1
2.1.2 ip route-static 2-2
2.1.3 ip route-static default-preference 2-4

2章 スタティックルーティング

2.1 スタティックルーティング設定コマンド

2.1.1 delete static-routes all

Syntax

delete [**vpn-instance** *vpn-instance-name*] **static-routes all**

View

System view

定義済みユーザロール

network-admin

パラメータ

vpn-instance *vpn-instance-name*: 名前で VPN インスタンスを指定します。大文字小文字を区別し、設定範囲は 1～31 文字です。このオプションを指定しない場合、パブリックネットワークのすべてのスタティックルートを削除します。

説明

delete static-routes all コマンドはすべてのスタティックルートを削除します。

コマンドを実行すると、設定されているすべてのスタティックルートを削除する前に確認画面が表示されます。

1 つのスタティックルートを削除する場合、**undo ip route-static** コマンドを使用します。デフォルトルートを含むすべてのスタティックルートを削除する場合、**delete static-routes all** コマンドを使用します。

例

すべてのスタティックルートを削除します。

<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
```

関連コマンド

ip route-static

2.1.2 ip route-static

Syntax

ip route-static *dest-address* { *mask-length* | *mask* } { *interface-type interface-number* [*next-hop-address*] [**permanent**] | **bfd** { **control-packet** | **echo-packet** } | **permanent**] | *next-hop-address* [**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-value*] [**tag** *tag-value*] [**description** *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-value*]

ip route-static vpn-instance *s-vpn-instance-name dest-address* { *mask-length* | *mask* } { *interface-type interface-number* [*next-hop-address*] [**permanent**] | **bfd** { **control-packet** | **echo-packet** } | **permanent**] | *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-value*] [**tag** *tag-value*] [**description** *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-value*]

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

vpn-instance *s-vpn-instance-name*: 名前で VPN インスタンスを指定します。大文字小文字を区別し、設定範囲は 1～31 文字です。VPN は、それぞれルーティングテーブルを持っており、設定されたスタティックルートは指定された VPN のルーティングテーブルで指定されます。

dest-address: スタティックルートの宛先アドレスを指定します。ドットで区切り、10 進数で指定します。

mask-length/*mask*: IP アドレスのマスク長あるいはマスクを指定します。設定範囲は 0～32 です。ドットで区切り、10 進数で指定します。

vpn-instance *d-vpn-instance-name*: 名前で宛先 VPN インスタンスを指定します。大文字小文字を区別し、設定範囲は 1～31 文字です。宛先 VPN が指定された場合、設定されたネクストホップアドレスにもとづき、パケットは宛先 VPN から出力インタフェースを探します。

next-hop-address: ネクストホップの IP アドレスを指定します。ドットで区切り、10 進数で指定します。

bfd: スタティックルートのネクストホップの到達可能性を検出する BFD を有効にします。ネクストホップが到達不可能である場合、システムはすぐにバックアップルートに切り替えます。

control-packet: BFD コントロールモードを指定します。

bfd-source *ip-address*: BFD パケットの送信元 IP アドレスを指定します。ループバックインタフェースのアドレスを指定することを推奨します。

permanent: 固定のスタティックルートを指定します。出力インタフェースがダウンしても、固定のスタティックルートはアクティブのままです。

echo-packet: BFD エコーモードを指定します。

public: 指定されたネクストホップアドレスがパブリックネットワークにあることを示します。

track *track-entry-number*: track エントリの番号とスタティックルートを関連づけます。設定範囲は 1～1024 です。Track の詳細は、オペレーションマニュアルのセクション 10 *高可用性*”*Track*”を参照してください。

interface-type interface-number: 出力インタフェースのタイプと番号を指定します。出力インタフェースが NBMA インタフェースあるいはブロードキャストインタフェースである場合、または P2P インタフェースでない場合、ネクストホップアドレスを指定する必要があります。ブロードキャストインタフェースは Ethernet インタフェース、VLAN インタフェースが含まれます。

preference *preference-value*: スタティックルートの優先順位を指定します。設定範囲は 1～255 です。デフォルトは 60 です。

tag *tag-value*: スタティックルートをマーキングするためタグを設定します。設定範囲は 1～4294967295 です。デフォルトは 0 です。ルートのタグはルーティングポリシーのルート制御に使用されます。ルーティングポリシーの詳細は、オペレーションマニュアルのセクション 5 *ルーティングプロトコル*”*ルーティングポリシー*”を参照してください。

description *description-text*: スタティックルートの説明を設定します。設定範囲は 1～60 文字です。半角スペースのような記号を含むことができますがクエスチョンマーク(?)は含むことができません。

説明

ip route-static コマンドはスタティックルートを設定します。

undo ip route-static コマンドはスタティックルートを削除します。

宛先アドレスとマスクの両方が 0.0.0.0（あるいは 0）である場合、設定されたルートはデフォルトルートです。デフォルトルートはルーティングテーブルに一致するエントリがないパケットを転送するのに使用されます。

異なるルートの優先順位を設定するため、異なるルーティングポリシーを実装してください。たとえば、同一宛先の複数のルートのロードバランスを有効にする場合、ルートに同一の優先順位を割り当ててください。一方をバックアップルートとする場合、ルートに異なる優先順位を割り当ててください。

スタティックルートの出力インタフェースあるいはネクストホップアドレスを指定するとき、以下のガイドラインに従ってください。

- 出力インタフェースが Null 0 インタフェースである場合、ネクストホップアドレスは必要ありません。
- 出力インタフェースが複数のネクストホップを持つブロードキャストインタフェースである場合、出力インタフェースとネクストホップアドレスを同時に指定してください。ブロードキャストインタフェースは Ethernet インタフェース、VLAN インタフェースが含まれます。

スタティックルートを設定するとき、以下のガイドラインに従ってください。

- ルートが頻繁に切り替わる状態で BFD を有効にした場合、ルートのフラッピングを悪化させます。使用する場合、注意してください。BFD の詳細は、オペレーションマニュアルのセクション 10 *高可用性*”*BFD*”を参照してください。
- スタティックルーティングトラック NQA と併用を行う場合には、検出されるネクストホップと NQA 操作と同じ VPN インスタンス ID を設定しなければなりません。
- スタティックルートがルート再帰を必要とするとき、関連づけた Track エントリはスタティックルートの代わりに再帰ルートのネクストホップをモニタしてください。
- **permanent** を **bfd** あるいは **track** と一緒に使用しないでください。

例

宛先アドレスが 1.1.1.1/24、ネクストホップが 2.2.2.2、タグが 45、説明が for internet のスタティックルートを設定します。

<Switch> system-view

[Switch] ip route-static 1.1.1.1 24 2.2.2.2 tag 45 description for internet

関連コマンド

display ip routing-table protocol

2.1.3 ip route-static default-preference

Syntax

ip route-static default-preference *default-preference-value*

undo ip route-static default-preference

デフォルト

60

View

System view

定義済みユーザロール

network-admin

パラメータ

default-preference-value: スタティックルートのデフォルトの優先順位を設定します。設定範囲は 1～255 です。

説明

ip route-static default-preference コマンドはスタティックルートのデフォルトの優先順位を設定します。

undo ip route-static default-preference コマンドはデフォルトに戻します。

スタティックルートの優先順位を指定しない場合、デフォルトの優先順位が適用されます。

デフォルトの優先順位が再設定された場合、新しく追加されたスタティックルートが適用されます。

例

スタティックルートのデフォルトの優先順位を 120 に設定します。

<Switch> system-view

[Switch] ip route-static default-preference 120

関連コマンド

display ip routing-table protocol

目次

このセクションのページは **5-x-x** です。

3 章 IPv6 スタティックルーティング 3-1
3.1 IPv6 スタティックルーティング設定コマンド 3-1
3.1.1 delete ipv6 static-routes all 3-1
3.1.2 ipv6 route-static 3-2
3.1.3 ipv6 route-static default-preference 3-4

3章 IPv6 スタティックルーティング

3.1 IPv6 スタティックルーティング設定コマンド

3.1.1 delete ipv6 static-routes all

Syntax

delete ipv6 [**vpn-instance** *vpn-instance-name*] **static-routes all**

View

System view

定義済みユーザロール

network-admin

パラメータ

vpn-instance *vpn-instance-name*: VPN インスタンスを名前で指定します。大文字小文字を区別し、設定範囲は 1～31 文字です。このオプションを指定しない場合、コマンドはパブリックネットワークのすべての IPv6 スタティックルートを削除します。

説明

delete ipv6 static-routes all コマンドはすべての IPv6 スタティックルートを削除します。

コマンドを実行すると、設定されているすべての IPv6 スタティックルートを削除する前に確認画面が表示されます。

例

すべての IPv6 スタティックルートを削除します。

<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
```

関連コマンド

ipv6 route-static

3.1.2 ipv6 route-static

Syntax

ipv6 route-static *ipv6-address prefix-length* { *interface-type interface-number* [*next-hop-address*] [**bfd** { **control-packet** | **echo-packet** } | **permanent**] | *next-hop-address* [**bfd control-packet bfd-source** *ipv6-address* | **permanent**] | **vpn-instance** *d-vpn-instance-name next-hop-address* [**bfd control-packet bfd-source** *ipv6-address* | **permanent**] } [**preference** *preference-value*] [**tag** *tag-value*] [**description** *description-text*]

undo ipv6 route-static *ipv6-address prefix-length* [*interface-type interface-number* [*next-hop-address*] | *next-hop-address* | **vpn-instance** *d-vpn-instance-name next-hop-address*] [**preference** *preference-value*]

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** *ipv6-address* | **permanent**] | **vpn-instance** *d-vpn-instance-name next-hop-address* [**bfd control-packet bfd-source** *ipv6-address* | **permanent**] } [**preference** *preference-value*] [**tag** *tag-value*] [**description** *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-value*]

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

ipv6-address prefix-length: IPv6 アドレス、プレフィックス長を指定します。

interface-type interface-number: 出力インタフェースのタイプと番号を指定します。出力インタフェースが NBMA インタフェースあるいはブロードキャストインタフェースである場合、またはポイントツーポイント（P2P）インタフェースでない場合、ネクストホップアドレスを指定する必要があります。ブロードキャストインタフェースは Ethernet インタフェース、VLAN インタフェースが含まれます。

next-hop-address: ネクストホップの IPv6 アドレスを指定します。

bfd: スタティックルートのネクストホップの到達可能性を検出する BFD を有効にします。

control-packet: BFD コントロールモードを指定します。

bfd-source *ipv6-address*: BFD パケットの送信元 IPv6 アドレスを指定します。ループバックインタフェースのアドレスを指定することを推奨します。

echo-packet: BFD エコーモードを指定します。

permanent: 固定の IPv6 スタティックルートを指定します。出力インタフェースがダウンしても、固定の IPv6 スタティックルートはアクティブのままです。

public: ネクストホップがパブリックネットワークにあることを示します。

vpn-instance *d-vpn-instance-name*: 宛先 VPN インスタンスを名前で指定します。大文字小文字を区別し、設定範囲は 1～31 文字です。宛先 VPN を指定しない場合、スタティックルートの指定されたネクストホップに基づいてパケットは出力インタフェースを探します。

preference *preference-value*: IPv6 スタティックルートの優先順位を指定します。設定範囲は 1～255 です。デフォルトは 60 です。

tag *tag-value*: スタティックルートをマーキングするためタグを設定します。設定範囲は 1～4294967295 です。デフォルトは 0 です。ルートのタグはルーティングポリシーのルート制御に使用されます。ルーティングポリシーの詳細は、オペレーションマニュアルのセクション 5 *ルーティングプロトコル*”*ルーティングポリシー*”を参照してください。

description *description-text*: IPv6 スタティックルートの説明を設定します。設定範囲は 1～60 文字です。半角スペースのような記号を含むことができますがクエスチョンマーク（?）は含むことができません。

vpn-instance *s-vpn-instance-name*: 送信元 VPN インスタンスを名前で指定します。大文字小文字を区別し、設定範囲は 1～31 文字です。各 VPN はルーティングテーブルをそれぞれ持っており、設定されたスタティックルートは指定の VPN のルーティングテーブルに設定されます。

説明

ipv6 route-static コマンドは IPv6 スタティックルートを設定します。

undo ipv6 route-static コマンドは IPv6 スタティックルートを削除します。

宛先アドレスが::/0（あるいはプレフィックス長が 0）である場合、設定されたルートは IPv6 デフォルトルートです。IPv6 デフォルトルートはルーティングテーブルに一致するエントリがないパケットを転送するのに使用されます。

IPv6 スタティックルートの出力インタフェースがブロードキャストインタフェースである場合、ネクストホップアドレスを指定してください。ブロードキャストインタフェースは Ethernet インタフェース、VLAN インタフェースが含まれます。

IPv6 スタティックルートを設定するとき、以下のガイドラインに従ってください。

- ルートが頻繁に切り替わる状態で BFD を有効にした場合、ルートのフラッピングを悪化させます。使用する場合、注意してください。BFD の詳細は、オペレーションマニュアルのセクション 10 *高可用性*”*BFD*”を参照してください。
- エコーパケットのネクストホップ IPv6アドレスはグローバルユニキャストアドレスにしてください。

- **permanent** と、**bfd** を同時に指定しないでください。

例

宛先アドレスが 1:1:2::/64、ネクストホップが 1:1:3::1 の IPv6 スタティックルートを設定します。

<Switch> system-view

[Switch] ipv6 route-static 1:1:2:: 64 1:1:3::1

関連コマンド

display ipv6 routing-table protocol

3.1.3 ipv6 route-static default-preference

Syntax

ipv6 route-static default-preference *default-preference-value*

undo ipv6 route-static default-preference

デフォルト

60

View

System view

定義済みユーザロール

network-admin

パラメータ

default-preference-value: IPv6 スタティックルートのデフォルトの優先順位を設定します。設定範囲は 1～255 です。

説明

ipv6 route-static default-preference コマンドは IPv6 スタティックルートのデフォルトの優先順位を設定します。

undo ipv6 route-static default-preference コマンドはデフォルトに戻します。

IPv6 スタティックルートの優先順位を指定しない場合、デフォルトの優先順位が適用されます。

デフォルトの優先順位が再設定された場合、新しく追加された IPv6 スタティックルートが適用されます。

例

IPv6 スタティックルートのデフォルトの優先順位を 120 に設定します。

<Switch> system-view

[Switch] ipv6 route-static default-preference 120

関連コマンド

display ipv6 routing-table protocol

目次

このセクションのページは **5-x-x** です。

4 章 RIP 4-1
4.1 RIP 設定コマンド 4-1
4.1.1 checkzero 4-1
4.1.2 default cost 4-1
4.1.3 default-route 4-2
4.1.4 display rip 4-3
4.1.5 display rip database 4-6
4.1.6 display rip interface 4-7
4.1.7 display rip non-stop-routing 4-9
4.1.8 display rip route 4-10
4.1.9 filter-policy export 4-13
4.1.10 filter-policy import 4-15
4.1.11 graceful-restart 4-17
4.1.12 host-route 4-18
4.1.13 import-route 4-19
4.1.14 maximum load-balancing 4-20
4.1.15 network 4-21
4.1.16 non-stop-routing 4-22
4.1.17 output-delay 4-23
4.1.18 peer 4-24
4.1.19 preference 4-25
4.1.20 reset rip process 4-26
4.1.21 reset rip statistics 4-26
4.1.22 rip 4-27
4.1.23 rip authentication-mode 4-28
4.1.24 rip bfd enable 4-29
4.1.25 rip default-route 4-30
4.1.26 rip input 4-31
4.1.27 rip metricin 4-32
4.1.28 rip metricout 4-33
4.1.29 rip mib-binding 4-34
4.1.30 rip output 4-35
4.1.31 rip poison-reverse 4-36
4.1.32 rip split-horizon 4-37
4.1.33 rip summary-address 4-37
4.1.34 rip version 4-38

4.1.35 silent-interface 4-40
4.1.36 summary 4-41
4.1.37 timers 4-41
4.1.38 validate-source-address 4-43
4.1.39 version 4-44

4章 RIP

4.1 RIP設定コマンド

4.1.1 checkzero

Syntax

checkzero

undo checkzero

デフォルト

有効

View

RIP view

定義済みユーザロール

network-admin

説明

checkzero を使用して、RIPv1 メッセージのゼロフィールドチェックを有効にします。

undo checkzero を使用して、ゼロフィールドチェックを無効にします

0 フィールドチェックが有効な場合、ルータは 0 フィールドに 0 以外の値が含まれる RIPv1 メッセージを破棄します。すべてのメッセージが信頼できる場合は、この機能を無効にして CPU の負荷を軽減します。

例

RIP プロセス 1 の RIPv1 メッセージのゼロフィールドチェックを無効にします。

<Switch> system-view

[Switch] rip

[Switch-rip-1] undo checkzero

4.1.2 default cost

Syntax

default cost *cost-value*

undo default cost

デフォルト

0

View

RIP view

定義済みユーザロール

network-admin

パラメータ

cost-value: 再配信されたルートのデフォルトメトリックを指定します。設定範囲は 0～16 です。

説明

default cost コマンドは再配信されたルートのデフォルトメトリックを設定します。

undo default cost コマンドはデフォルトに戻します。

メトリックを指定しないで別のルーティングプロトコルからルートを再配信するため、**import-route** コマンドを使用するとき、**default cost** コマンドによって指定されたメトリックが適用されます。

例

再配信されたルートのデフォルトメトリックを 3 に設定します。

<Switch> system-view

[Switch] rip 1

[Switch-rip-1] default cost 3

関連コマンド

import-route

4.1.3 default-route

Syntax

default-route { **only** | **originate** } [**cost** *cost*]

undo default-route

デフォルト

デフォルトルートは RIP ネイバに送信されません。

View

RIP view

定義済みユーザロール

network-admin

パラメータ

only: デフォルトルートだけを配信します。

originate: デフォルトルートと他のルートの両方を配信します。

cost-value: デフォルトルートのコストを 1～15 の範囲で指定します。デフォルトは 1 です。

説明

default-route コマンドは RIP プロセスを実行するすべてのインタフェースを設定し、指定されたメトリックを持つデフォルトルートを RIP ネイバルータに配信します。

undo default-route コマンドはデフォルトに戻します。

この機能で設定された RIP ルータは、RIP ネイバルータからデフォルトルートを受信しません。

例

RIP プロセス 100 を実行しているすべてのインタフェースが、メトリック 2 のデフォルトルートだけを RIP ネイバに送信するように設定します

<Switch> system-view

[Switch] rip 100

[Switch-rip-100] default-route only cost 2

関連コマンド

rip default-route

4.1.4 display rip

Syntax

display rip [*process-id*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

process-id: 1～65535 の ID で RIP プロセスを指定します。プロセスが指定されていない場合、このコマンドはすべての RIP プロセスの状態と構成情報を表示します。

説明

display rip コマンドは RIP プロセスの状態と構成情報を表示します。

例

すべての RIP プロセスの現在の状態と構成情報を表示します。

<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
```

表 4-1 コマンド出力

フィールド	説明
Public VPN-instance name	RIPプロセスは、パブリックネットワーク上で実行されます。
Private VPN-instance name	RIPプロセスが実行されるVPNインスタンス。
RIP process	RIPプロセスIDです。
RIP version	RIPバージョン1または2です。
Preference	RIPプリファレンスです。
Fast-reroute	RIP FRRです。
Checkzero	0フィールドチェックがRIPv1メッセージに対して有効かどうかを示します。(有効または無効)
Default cost	再配信されたルートのデフォルトコストです。
Summary	ルート要約が有効かどうかを示します。(有効または無効)
Host routes	ホストルートを受信するかどうかを示します。(有効または無効)
Maximum number of load balanced routes	ロードバランスへのECMPルートの最大数です。
Update time	RIP更新間隔です。(秒単位)
Timeout time	RIPタイムアウト時間です。(秒単位)
Suppress time	RIP抑制間隔です。(秒単位)
Garbage-collect time	RIPガーベッジ・コレクション間隔です。(秒単位)
Update output delay	RIPパケット送信間隔です。(秒単位)
Output count	各間隔で送信されるRIPパケットの最大数です。
Graceful-restart interval	GR間隔です。(秒単位)
Triggered Interval	更新の送信間隔がトリガされました。
Silent interfaces	サイレントインタフェース。定期的に更新を送信しません。

フィールド	説明
Default routes	デフォルトルートがRIPネイバルータに送信されるかどうかを示します。 ● **only**—デフォルトルートのみが配信されます。 ● **originate**—デフォルトルートが他のルートとともに配信されます。 ● **disable**—デフォルトルートは配信されません。
Default routes cost	デフォルトルートのメトリックです。
Verify-source	受信したRIPルーティング更新について送信元IPアドレスがチェックされているかどうかを示します。(有効または無効)
Networks	RIPで有効になっているネットワークです。
Configured peers	設定されたネイバです。
Triggered updates sent	送信されたトリガ更新の数です。
Number of routes changes	ルート変更の数です。
Number of replies to queries	RIP応答の数です。

4.1.5 display rip database

Syntax

display rip *process-id* **database** [*ip-address* { *mask-length* | *mask* }]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

process-id: 1~65535 の範囲の ID で RIP プロセスを指定します。

ip-address { *mask-length* | *mask* }: 指定された IP アドレスのアクティブなルートを表示します。この引数を指定しないと、RIP プロセスのすべてのアクティブルートが表示されます。

説明

display rip database コマンドは RIP プロセスのアクティブルートを表示します。

例

RIP プロセス 100 のアクティブルートを表示します。

<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
```

RIP プロセス 100 の宛先 IP アドレス 1.1.1.0 およびマスク長 24 のアクティブなルートを表示します。

```
<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
```

表 4-2 コマンド出力

フィールド	説明
cost	ルートのコストです。
auto-summary	ルートがRIP自動要約ルートであることを示します。
interface summary	ルートがRIPインタフェース集約ルートであることを示します。
nexthop	ネクストホップのアドレスです。
RIP-interface	RIP対応インタフェースへの直接ルートです。
imported	ルートが別のルーティングプロトコルから再配信されることを示します。

4.1.6 display rip interface

Syntax

display rip *process-id* **interface** [*interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

process-id: 1～65535 の範囲内の ID で RIP プロセスを指定します。

interface-type interface-number: インタフェースをタイプと番号で指定します。インタフェースが指定されていない場合は、RIP プロセスのすべての RIP インタフェースに関する情報が表示されます。

説明

display rip interface コマンドは RIP プロセスの RIP インタフェース情報を表示します。

例

RIP プロセス 1 のすべてのインタフェースに関する情報を表示します。

<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
```

表 4-3 コマンド出力

フィールド	説明
Total	RIPを実行しているインタフェースの数です。
Interface	RIP を実行しているインタフェースの名前です。
Address/Mask	インタフェースのIPアドレスとマスクです。
Version	インタフェースで実行されているRIPバージョンです。
MetricIn	受信ルートに追加された追加メトリックです。
MetricIn route policy	受信ルートにメトリックを追加するために使用されるルーティングポリシーの名前。ルーティングポリシーが使用されていない場合は、**Not designated**と表示されます。

フィールド	説明
MetricOut	送信ルートに追加された追加メトリックです。
MetricOut route policy	送信ルートに追加のルーティングメトリックを追加するために使用されるルーティングポリシーの名前。ルーティングポリシーが使用されていない場合は、**Not designated**と表示されます。
Split-horizon	スプリットホライズンが有効かどうかを示します: ● **on**—有効. ● **off**—無効.
Poison-reverse	ポイズンリバースが有効かどうかを示します: ● **on**—有効. ● **off**—無効.
Input/Output	インタフェースがRIPメッセージを送受信できるようになっているかどうかを示します: ● **on**—有効. ● **off**—無効.
Default route	デフォルトルートをRIPネイバルータに送信するかどうかを示します: ● **Only**—デフォルトルートのみを配信します。 ● **Originate**—デフォルトルートと他のルートの両方を配信します。 ● **No-originate**—デフォルト以外のルートだけを配信します。 ● **Off**—デフォルトルートを配信しません。
Default route cost	デフォルトルートのメトリックです。
Update output delay	RIPパケット送信間隔です。
Output count	各間隔で送信できるRIPパケットの最大数です。
Current number of packets /Maximum number of packets	送信するRIPパケットの数/一定の間隔内に送信できるRIPパケットの最大数です。

4.1.7 display rip non-stop-routing

Syntax

display rip [*process-id*] **non-stop-routing**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

process-id: RIP プロセスを ID で指定します。設定範囲は 1～65535 です。指定しない場合、すべての RIP プロセスの NSR ステータスが表示されます。

説明

display rip non-stop-routing コマンドは RIP プロセスの NSR ステータスを表示します。

例

RIP プロセス 1 の NSR ステータスを表示します。

<Switch> display rip 1 non-stop-routing

```
RIP process: 1
 Nonstop Routing capability: Enabled
 Current NSR state        : Finish
```

表 4-4 コマンド出力

フィールド	説明
Nonstop Routing capability	NSRが有効かどうかを示します（**Enabled**または**Disabled**）。
Current NSR state	NSRの状態です。 ● Initialization–初期化します。 ● **Smooth**–データをアップグレードします。 ● **Advertising**–配信ルートです。 ● **Redistribution**–ルートを再配信します。 ● Finish–完了です。

4.1.8 display rip route

Syntax

display rip *process-id* **route** [*ip-address* { *mask-length* | *mask* } [**verbose**] | **peer** *ip-address* | **statistics**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

process-id: RIP プロセスの ID を指定します。設定範囲は 1～65535 です。

ip-address { *mask-length* | *mask* }: 指定された IP アドレスのルート情報を表示します。

verbose: 指定された宛先 IP アドレスのすべてのルーティング情報を表示します。指定しない場合、指定された宛先 IP アドレスの最適ルートのみを表示します。

peer *ip-address*: 指定されたネイバから学習したルート情報を表示します。

statistics: ルートの総数、各ネイバからのルート数を含むルートの統計情報を表示します。

説明

display rip route コマンドは RIP プロセスのルーティング情報を表示します。

オプションのパラメータが指定されていない場合、**display rip process-id route** コマンドは、RIP プロセスのすべてのルーティング情報を表示します。

例

RIP プロセス 1 のすべてのルーティング情報を表示します。

<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    -
```

RIP プロセス 1 の指定されたルーティング情報を表示します。

<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
```

表 4-5 コマンド出力

フィールド	説明
Route Flags	• **R**—RIPルートです。 • **P**—ルートはエージングアウトしません。 • **A**—ルートはエージング中です。 • **S**—ルートは抑制されます。 • **G**—ルートはガーベッジコレクト状態です。 • **O**—ルートは最適なルートです。 • **F**—ルートはRIBにフラッシュされました。
Peer *X.X.X.X* on *interface-type interface-number*	RIP インタフェース上のネイバから学習したルーティング情報。
Local route	ローカルに生成された直接ルート。
Destination/Mask	宛先 IP アドレスとサブネットマスク。
Nexthop	ルートのネクストホップ。
OrigNexthop/RealNexthop	直接接続されているネイバからのルートである場合、もとのネクストホップは実際のネクストホップです。 直接接続されていないネイバからのルートである場合、RealNexthop フィールドはルートの再帰ネクストホップを表示します。そうでない場合、このフィールドは表示されません。
Cost	ルートのコストです。
Tag	ルートのタグです。
Flags	ルートの状態です。
Sec	ルート状態に対応するタイマの残り時間です。

RIP プロセス 1 のルーティング統計情報を表示します。

<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
```

表 4-6 コマンド出力

フィールド	説明
Peer	ネイバのIPアドレスです。
Optimal	最適ルートの総数です。
Aging	エージングルートの総数です。
Permanent	エージングアウトしないルートの総数です。
Garbage	Garbage-collection状態のルートの総数です。
Local	ローカルで生成された直接ルートの総数です。
Total	すべてのRIPネイバルータから学習されたルートの総数です。

4.1.9 filter-policy export

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*]

デフォルト

RIP は再配信されたルートをフィルタリングしません。

View

RIP view

定義済みユーザロール

network-admin

パラメータ

ipv4-acl-number: 再配信されたルートをフィルタするために、IPv4 ACL を 2000～3999 の範囲の番号で指定します。

prefix-list *prefix-list-name*: P プレフィックスリストを名前で指定します。大文字と小文字が区別される 1～63 文字の文字列で、再配信されたルートをフィルタリングします。

protocol: 指定されたルーティングプロトコルから再配信されたルートをフィルタリングします

process-id: 指定されたルーティングプロトコルのプロセス ID を 1～65535 の範囲で指定します。ルーティングプロトコルが rip、ospf、または isis の場合はプロセス ID を指定します。プロセス ID が指定されていない場合、デフォルトのプロセス ID は 1 です。

interface-type interface-number: インタフェースをタイプと番号で指定します。

説明

filter-policy export コマンドは RIP を設定して再配信されたルートをフィルタリングします。

undo filter-policy export を使用してフィルタリングを削除します。

ルーティングプロトコルまたはインタフェースから再配信されたルートをフィルタするフィルタリングポリシーは 1 つだけ設定できます。プロトコルまたはインタフェースが指定されていない場合、フィルタリングポリシーはグローバルに適用されます。このコマンドを複数回実行すると、最新の設定が有効になります。

指定したプロトコルまたはインタフェースで **undo filter-policy export** コマンドは、プロトコルまたはインタフェースに対して設定されたフィルタリングポリシーを削除します。

コマンドで拡張 ACL（番号が 3000～3999）を参照するには、次のいずれかの方法を使用して ACL を設定します。

- **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* コマンドは、指定した宛先のルートを拒否または許可します。
- **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* **destination** *dest-addr dest-wildcard* コマンドは、指定された宛先およびマスクを持つルートを拒否または許可します。

source キーワードはルートの宛先アドレスを指定し、**destination** キーワードはルートのサブネットマスクを指定します。マスク設定を有効にするには、連続したサブネットマスクを指定します。

例

#ACL 2000 を使用して、再配信されたルートをフィルタリングします。

```
<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
```

IP プレフィックスリスト abc を使用して、再配信されたルートをフィルタリングします。

<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

拡張 ACL 3000 を設定して、ルート 113.0.0.0/16 のみが通過できるようにします。ACL 3000 を使用して、再配信されたルートをフィルタリングします。

<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

関連コマンド

- **acl** (コマンドマニュアルのセクション 8 *ACL and QoS*)
- import-route
- ip prefix-list

4.1.10 filter-policy import

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*]

デフォルト

RIP は受信したルートをフィルタリングしません。

View

RIP view

定義済みユーザロール

network-admin

パラメータ

ipv4-acl-number: 受信したルートをフィルタするために、IPv4 ACL を 2000～3999 の範囲の番号で指定します。

prefix-list *prefix-list-name*: 受信したルートをフィルタするために、IP プレフィックスリストをその名前（大文字と小文字を区別する 1～63 文字の文字列）で指定します

gateway *prefix-list-name*: 次のホップに基づいてルートをフィルタするために、IP プレフィックスリストをその名前（大文字小文字を区別する 1～63 文字の文字列）で指定します。

interface-type interface-number: インタフェースのタイプと番号で指定します

説明

filter-policy import コマンドは受信したルートをフィルタするように RIP を設定します。

undo filter-policy import コマンドはフィルタリングを削除します。

インタフェースで受信したルートをフィルタするために、1 つのフィルタリングポリシーのみを設定できます。インタフェースが指定されていなければ、フィルタリングポリシーはグローバルに適用されます。このコマンドを複数回実行すると、最新の設定が有効になります。

インタフェースを指定して **undo filter-policy import** コマンドは、インタフェースに設定されたフィルタリングポリシーを削除します。

コマンドで拡張 ACL（番号が 3000～3999）を参照するには、次のいずれかの方法を使用して ACL を設定します

- **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* コマンドは、指定された宛先のルートを拒否または許可します。
- **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* **destination** *dest-addr dest-wildcard* コマンドは、指定された宛先とマスクを持つルートを拒否または許可します。

source キーワードはルートの宛先アドレスを指定し、**destination** キーワードはルートのサブネットマスクを指定します。マスク設定を有効にするには、連続したサブネットマスクを指定します。

例

受信した RIP ルートをフィルタするには、標準 ACL 2000 を使用します。

<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

受信した RIP ルートをフィルタするには、IP プレフィックスリスト **abc** を使用します。

<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

拡張 ACL 3000 を設定して、ルート 113.0.0.0/16 のみが通過できるようにします。ACL 3000 を使用して、受信したルートをフィルタリングします。

<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

関連コマンド

- **acl** (コマンドマニュアルのセクション 8 *ACL and QoS*)
- ip prefix-list

4.1.11 graceful-restart

Syntax

graceful-restart

undo graceful-restart

デフォルト

RIP GR は無効です。

View

RIP view

定義済みユーザロール

network-admin

説明

graceful-restart コマンドは RIP に GR を有効にします。

undo graceful-restart コマンドは RIP GR を無効にします。

graceful-restart コマンドと **non-stop-routing** コマンドは相互排他的です。

例

RIP プロセス 1 に GR を有効にします。

<Switch> system-view

[Switch] rip 1

[Switch-rip-1] graceful-restart

4.1.12 host-route

Syntax

host-route

undo host-route

デフォルト

有効

View

RIP view

定義済みユーザロール

network-admin

説明

host-route コマンドはホストルートの受信を有効にします。

undo host-route コマンドはホストルートの受信を無効にします。

ルータは同一サブネットから多くのホストルートを受信する可能性があります。これらのルートはルーティングに役立ちません。また多くのリソースを消費します。この問題を解決するため、**undo host-route** コマンドでホストルートの受信を無効にします。

このコマンドは RIPv2 ルートのみ適用します。

例

RIP でホストルートの受信を無効にします。

<Switch> system-view

[Switch] rip 1

[Switch-rip-1] undo host-route

4.1.13 import-route

Syntax

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**] [**allow-direct** | **cost** *cost-value* | **route-policy** *route-policy-name* | **tag** *tag*] *

undo import-route { **ospf** | **rip** } [*process-id* | **all-processes**]

デフォルト

RIP は、他のルーティングプロトコルからのルートを再配信しません。

View

RIP view

定義済みユーザロール

network-admin

パラメータ

direct: 直接ルートを再配信します。

ospf: OSPF ルートを再配信します。

rip: RIP ルートを再配信します。

static: 静的ルートを再配信します。

process-id: OSPF、IS-IS、または RIP のプロセス ID を 1～65535 の範囲で指定します。デフォルトは 1 です。

all-processes: すべての OSPF、RIP プロセスからのルート再配信を有効にします。

allow-direct: 指定されたルーティングプロトコルで有効になっているローカルインタフェースのネットワークを再配信します。 **allow-direc** キーワードを指定しないと、ローカルインタフェースのネットワークは再配信されません。**allow-direct** キーワードと **route-policy** *route-policy-name* オプションの両方を指定する場合は、ルーティングポリシーで定義されている **if-match** ルールが **allow-direct** キーワードと競合していないことを確認してください。たとえば、**allow-direct** キーワードを指定する場合は、ルーティングポリシーに **if-match route-type** を設定しないでください。それ以外の場合、**allow-direct** キーワードは有効になりません。

cost *cost-value*: 再配信されたルートのコストを 0～16 の範囲で指定します。デフォルトコストは 0 です。

route-policy *route-policy-name*: ルーティングポリシーを名前で指定します。大文字と小文字が区別される 1～63 文字の文字列です。

tag *tag*: 再配信されたルートをマーキングするタグを 0～65535 の範囲で指定します。デフォルトは 0 です。

説明

import-route コマンドは、他のルーティングプロトコルからのルート再配信を有効にします。

undo import-route を使用して、別のルーティングプロトコルから再配信されたルートを削除します。

このコマンドは、アクティブなルートだけを再配信します。**display ip routing-table protocol** コマンドは、ルート状態情報を表示します。

コマンドの元に戻す形式を実行すると、プロセスごとの設定がすべてのプロセスの設定よりも優先されます。 **undo import-route** { **ospf** | **rip** } **all-processess** コマンドでは、**import-route** { **ospf** | **rip** } *process-id* コマンドを使用して、プロセスに設定されている設定を削除することはできません。 そのプロセスの設定を削除するには、コマンドの元に戻す形式でプロセス ID を指定する必要があります。

例

スタティックルートを RIP に再配信し、再配信ルートのコストを 4 に設定します。

<Switch> system-view

[Switch] rip 1

[Switch-rip-1] import-route static cost 4

関連コマンド

default cost

4.1.14 maximum load-balancing

Syntax

maximum load-balancing *number*

undo maximum load-balancing

デフォルト

RIP ECMP ルートの最大数は、ECMP ルートの最大数に等しく、**max-ecmp-num** コマンドを使用して設定できます。

View

RIP view

定義済みユーザロール

network-admin

パラメータ

number: RIP ECMP ルートの最大数を指定します。値が 1 の場合、ロードバランシングは実装されません。この引数の値の範囲は 1～8 です。

説明

maximum load-balancing コマンドは負荷分散のための RIP 等価コストマルチパス（ECMP）ルートの最大数を設定します。

undo maximum load-balancing コマンドはデフォルトに戻します。

例

RIP ECMP ルートの最大数を 2 に設定します。

<Switch> system-view

[Switch] rip

[Switch-rip-1] maximum load-balancing 2

4.1.15 network

Syntax

network *network-address* [*wildcard-mask*]

undo network *network-address*

デフォルト

無効

View

RIP view

定義済みユーザロール

network-admin

パラメータ

network-address: インタフェースが存在するサブネットアドレスを指定します。

wildcard-mask: IP アドレスワイルドカードマスクを指定します。ワイルドカードマスクは、1 と 0 を反転したサブネットマスクと見なすことができます。たとえば、ワイルドカードマスク 255.255.255.0 は、サブネットマスク 0.0.0.255 に対応します。この引数を指定しない場合、コマンドは自然マスクを使用します。

説明

network コマンドは指定したネットワークに接続しているインタフェースの RIP を有効にします。

undo network コマンドは指定したネットワークに接続しているインタフェースの RIP を無効にします。

RIP は、指定したネットワークに接続されたインタフェース上でのみ実行されます。ワイルドカードマスクを使用して設定できます。指定されたネットワーク上にないインタフェースは、RIP ルートを送受信したり、直接ルートを配信しません。

単一の RIP プロセスの場合、**network** 0.0.0.0 コマンドはすべてのインタフェースで RIP を有効にすることができます。複数の RIP プロセスが存在する場合、このコマンドは適用されません。

物理インタフェースが複数のネットワークに接続されている場合、これらのネットワークを異なる RIP プロセスで配信することはできません。

例

ネットワーク 129.102.0.0 に接続されているインタフェースで RIP プロセス 100 を有効にします。

<Switch> system-view

[Switch] rip 100

[Switch-rip-100] network 129.102.0.0

4.1.16 non-stop-routing

Syntax

non-stop-routing

undo non-stop-routing

デフォルト

無効

View

RIP view

定義済みユーザロール

network-admin

説明

non-stop-routing コマンドは RIP NSR を有効にします。

undo non-stop-routing コマンドは RIP NSR を無効にします。

RIP プロセスに対して有効な RIP NSR は、そのプロセスでのみ有効になります。複数の RIP プロセスが存在する場合は、各プロセスの RIP NSR を有効にすることを推奨します。

non-stop-routing コマンドと **graceful-restart** コマンドは相互に排他的です。

例

#RIP プロセス 1 の NSR を有効にします。

<Switch> system-view

[Switch] rip 1

[Switch-rip-1] non-stop-routing

4.1.17 output-delay

Syntax

output-delay *time* **count** *count*

undo output-delay

デフォルト

インタフェースは 20 ミリ秒ごとに最大 3 つの RIP パケットを送信します。

View

RIP view

定義済みユーザロール

network-admin

パラメータ

time: 送信間隔を指定します。設定範囲は 10～100 ミリ秒です。

count: 各送信間隔で RIP パケットを送信する最大数を指定します。設定範囲は 1～30 です。

説明

output-delay コマンドはインタフェースが RIP パケットを送信するレートを設定します。

undo output-delay コマンドはデフォルトに戻します。

例

RIP プロセス 1 を実行するすべてのインタフェースが 60 ミリ秒ごとに最大 10 の RIP パケットを送信するように設定します。

<Switch> system-view

[Switch] rip 1

[Switch-rip-1] output-delay 60 count 10

4.1.18 peer

Syntax

peer *ip-address*

undo peer *ip-address*

デフォルト

RIP はネイバのユニキャストアップデートを行いません。

View

RIP view

定義済みユーザロール

network-admin

パラメータ

ip-address: ネイバの IP アドレスを指定します。ドットで区切り、10 進数で指定します。

説明

NBMA ネットワークでは、**peer** を使用して RIP ネイバを指定します。ネイバ向けのルーティングアップデートはユニキャストであり、マルチキャストまたはブロードキャストではありません。

undo peer コマンドは、RIP ネイバを削除します。

ネイバが直接接続されている場合は、**peer** *ip-address* コマンドを使用しないでください。それ以外の場合、ネイバは、同じルーティング情報を持つユニキャストおよびマルチキャスト（またはブロードキャスト）メッセージの両方を受信する可能性があります。

このコマンドは **undo validate-source-address** コマンドとともに実行する必要があり、インバウンド RIP ルーティングアップデートの送信元 IP アドレスチェックをディセーブルにします。

例

ピア 202.38.165.1 にユニキャストアップデートを送信するよう設定します。

<Switch> system-view

[Switch] rip 1

[Switch-rip-1] peer 202.38.165.1

関連コマンド

validate-source-address

4.1.19 preference

Syntax

preference { *preference* | **route-policy** *route-policy-name* } *

undo preference

デフォルト

100

View

RIP view

定義済みユーザロール

network-admin

パラメータ

preference: RIP ルートのプリファレンスを 1～255 の範囲で指定します。値が小さいほど優先度が高くなります。

route-policy *route-policy-name*: ルーティングポリシーを名前で指定します。大文字と小文字が区別される 1～63 文字の文字列です。

説明

preference コマンドは RIP ルートのプリファレンスを指定します。

undo preference コマンドはデフォルトに戻します。

キーワード **route-policy** を使用して、一致する RIP ルートのプリファレンスを設定することにより、ルーティングポリシーを指定できます。

- ルーティングポリシーによって設定されたプリファレンスは、一致するすべての RIP ルートに適用されます。他のルートの優先順位は、**preference** コマンドで設定します。
- ルーティングポリシーによって優先順位が設定されていない場合、すべての RIP ルートのプリファレンスは **preference** コマンドによって設定されます。

例

RIP ルートに 120 の優先度を設定します。

<Switch> system-view

[Switch] rip 1

[Switch-rip-1] preference 120

4.1.20 reset rip process

Syntax

reset rip *process-id* **process**

View

User view

定義済みユーザロール

network-admin

パラメータ

process-id: 1～65535 の範囲内の ID で RIP プロセスを指定します。

説明

reset rip process コマンドは RIP プロセスをリセットします。

コマンドを実行すると、操作を確認するプロンプトが表示されます。

例

RIP プロセス 100 をリセットします。

<Switch> reset rip 100 process

```
Reset RIP process? [Y/N]:y
```

4.1.21 reset rip statistics

Syntax

reset rip *process-id* **statistics**

View

User view

定義済みユーザロール

network-admin

パラメータ

process-id: Specifies a RIP process by its ID in the range of 1 to 65535.

説明

reset rip statistics コマンドは RIP プロセスの統計情報をクリアします。

例

RIP プロセス 100 の統計情報をクリアします。

<Switch> reset rip 100 statistics

4.1.22 rip

Syntax

rip [*process-id*] [**vpn-instance** *vpn-instance-name*]

undo rip [*process-id*]

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

パラメータ

process-id: 1～65535 の範囲内の ID で RIP プロセスを指定します。デフォルトは 1 です。

vpn-instance *vpn-instance-name*: 名前で MPLS L3VPN インスタンスを指定します。大文字と小文字が区別される 1～31 文字の文字列です。 VPN インスタンスを指定しない場合、RIP プロセスはパブリックネットワーク上で実行されます。

説明

rip コマンドは RIP を有効にし RIP view に入ります。

undo rip コマンドは RIP を無効にします。

RIP プロセスのグローバルパラメータを設定する前に、RIP プロセスを有効にする必要があります。 この制限は、インタフェースパラメータの設定には適用されません。

RIP プロセスを無効にすると、設定されたインタフェースパラメータは無効になります。

例

RIP プロセス 1 を有効にし、RIP view を入ります。

<Switch> system-view

[Switch] rip

[Switch-rip-1]

4.1.23 rip authentication-mode

Syntax

rip authentication-mode { **md5** { **rfc2082** { **cipher** | **plain** } *string key-id* | **rfc2453** { **cipher** | **plain** } *string* } | **simple** { **cipher** | **plain** } *string* }

undo rip authentication-mode

デフォルト

設定なし

View

Interface view

定義済みユーザロール

network-admin

パラメータ

md5: MD5 認証を指定します。

rfc2082: RFC2082 で定義されるメッセージフォーマットを使用します。

cipher: 暗号化された形式でパスワードを指定します。

plain: プレーンテキスト形式のパスワードを指定します。セキュリティ上の理由から、プレーンテキスト形式で指定されたパスワードは暗号化された形式で保存されます。

string: パスワードを指定します。そのプレーンテキスト形式は、大文字と小文字が区別される 1～16 文字の文字列です。その暗号化された形式は、33～53 文字の大文字小文字を区別する文字列です。

key-id: 1～255 の範囲のキーID を指定します。

rfc2453: RFC 2453（IETF 標準）で定義されているメッセージ形式を使用します

simple: 簡易認証モードを指定します。

説明

rip authentication-mode コマンドは RIPv2 認証を設定します。

undo rip authentication-mode コマンドはデフォルトに戻します。

新しく構成されたキーは、古いキーがあれば上書きします。

interface view で RIPv1 の認証モードを指定することはできますが、RIPv1 は認証をサポートしていないため、設定は有効になりません。

例

VLAN インタフェース 10 で MD5 認証を設定し、プレーンテキストキーが RFC 2453 で定義されている形式で設定されていることを指定します

<Switch> system-view

[Switch] interface vlan-interface 10

[Switch-Vlan-interface10] rip version 2

[Switch-Vlan-interface10] rip authentication-mode md5 rfc2453 plain rose

関連コマンド

rip version

4.1.24 rip bfd enable

Syntax

rip bfd enable

undo rip bfd enable

デフォルト

無効

View

Interface view

定義済みユーザロール

network-admin

説明

rip bfd enable コマンドはインタフェース上の RIP 用 BFD を有効にします。

undo rip bfd enable コマンドはデフォルトに戻します。

RIP は、直接接続されたネイバの BFD エコーモード検出と、間接ネイバの BFD 制御モード検出をサポートします。

BFD エコーモード検出は、1 ホップ離れた RIP ネイバにのみ適用されます。

undo peer コマンドを使用しても、ネイバ関係はすぐに削除されず、すぐに BFD セッションを停止することはできません。

rip bfd enable コマンドと **rip bfd enable destination** コマンドは相互排他的であり、装置上で同時に設定することはできません。**rip bfd enable destination** コマンドは未サポートです。

例

VLAN インタフェース 11 上で RIP に BFD を有効にします。

<Switch> system-view

[Switch] interface vlan-interface 11

[Switch-Vlan-interface11] rip bfd enable

4.1.25 rip default-route

Syntax

rip default-route { { **only** | **originate** } [**cost** *cost*] | **no-originate** }

undo rip default-route

デフォルト

RIP プロセスにデフォルトルートの配信が設定されている場合、RIP インタフェースはデフォルトルートを配信します。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

only: デフォルトルートのみ配信します。

originate: デフォルトルートと他のルートを配信します。

cost: デフォルトルートのコストを指定します。設定範囲は 1～15 です。デフォルトは 1 です。

no-originate: デフォルトルート以外のルートのみを配信します。

説明

rip default-route コマンドは指定したメトリックのデフォルトルートを配信する RIP インタフェースを設定します。

undo rip default-route コマンドはデフォルトルートを送信する RIP インタフェースを無効にします。

デフォルトルートを配信するように設定されたインタフェースは、RIP ネイバからデフォルトルートを受信しません。

例

VLAN インタフェース 10 にメトリック 2 のデフォルトルートのみを配信するように設定します。

<Switch> system-view

[Switch] interface vlan-interface 10

[Switch-Vlan-interface10] rip default-route only cost 2

VLAN インタフェース 10 にメトリック 2 のデフォルトルートと他のルートを配信するように設定します。

<Switch> system-view

[Switch] interface vlan-interface 10

[Switch-Vlan-interface10] rip default-route originate cost 2

関連コマンド

default-route

4.1.26 rip input

Syntax

rip input

undo rip input

デフォルト

有効

View

Interface view

定義済みユーザロール

network-admin

説明

rip input コマンドは RIP メッセージを受信するインタフェースを有効にします。

undo rip input コマンドは RIP メッセージを受信するインタフェースを無効にします。

例

RIP メッセージを受信する VLAN インタフェース 10 を無効にします。

<Switch> system-view

[Switch] interface vlan-interface 10

[Switch-Vlan-interface10] undo rip input

4.1.27 rip metricin

Syntax

rip metricin [**route-policy** *route-policy-name*] *value*

undo rip metricin

デフォルト

0

View

Interface view

定義済みユーザロール

network-admin

パラメータ

route-policy *route-policy-name*: メトリックを追加するルーティングポリシー名を指定します。設定範囲は 1～63 文字です。大文字、小文字を区別します。

value: 受信ルートに追加するメトリックを指定します。設定範囲は 0～16 です。

説明

rip metricin コマンドは受信ルートにメトリックを追加するようにインタフェースを設定します。

undo rip metricin コマンドはデフォルトに戻します。

有効な RIP ルートが受信されると、システムはそのルートにメトリックを追加した後にルーティングテーブルに組み入れます。設定されたインタフェースで受信したルートのメトリックは増加します。追加メトリックともとのメトリックの合計が 16 以上の場合、そのルートのメトリックは 16 になります。

route-policy によりルーティングポリシーが参照された場合、以下の動作を実行することができます。

- ポリシーに適合するルートは、ポリシー内の **apply cost** コマンドにより指定されたメトリックが追加されます。ポリシーに適合しないルートは、**rip metricin** コマンドにより指定されたメトリックが追加されます。**rip metricin** コマンドは **apply cost** コマンドで指定される、＋または－キーワード（メトリックの増減に使用される）をサポートしていません。
- ポリシーに **apply cost** コマンドが設定されていない場合、すべての配信メントルートは、**rip metricin** コマンドで指定されたメトリックが追加されます。

例

VLAN インタフェース 10 で、受信ルート 1.0.0.0/8 にメトリック 6 を追加します。それ以外の受信ルートにメトリック 2 を追加します。

<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

関連コマンド

apply cost

4.1.28 rip metricout

Syntax

rip metricout [**route-policy** *route-policy-name*] *value*

undo rip metricout

デフォルト

1

View

Interface view

定義済みユーザロール

network-admin

パラメータ

route-policy *route-policy-name*: 追加メトリックを加えるルーティングポリシー名を指定します。設定範囲は 1～63 文字です。大文字、小文字を区別します。

このオプションを指定すると、ルーティングポリシーに一致するルートのメトリックが追加されます。

value: 送信ルートに加える追加メトリックを指定します。設定範囲は 1～16 です。

説明

rip metricout コマンドは送信ルートに追加メトリックを加えるようにインタフェースを設定します。

undo rip metricout コマンドはデフォルトに戻します。

インタフェースでコマンドが設定されると、インタフェース上の送信された RIP ルートのメトリックが増加します。

route-policy によりルーティングポリシーが参照された場合、以下の動作を実行することができます。

- ポリシーに適合するルートは、ポリシー内の **apply cost** コマンドにより指定されたメトリックが追加されます。ポリシーに適合しないルートは、**rip metricout** コマンドにより指定されたメトリックが追加されます。**rip metricout** コマンドは **apply cost** コマンドで指定される、＋または－キーワード（メトリックの増減に使用される）をサポートしていません。
- ポリシーに **apply cost** コマンドが設定されていない場合、すべての配信メントルートは、**rip metricout** コマンドで指定されたメトリックが追加されます。

例

VLAN インタフェース 10 で、送信ルート 1.0.0.0/8 にメトリック 6 を追加します。それ以外の送信ルートにメトリック 2 を追加します。

```
<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
```

関連コマンド

apply cost

4.1.29 rip mib-binding

Syntax

rip mib-binding *process-id*

undo rip mib-binding

デフォルト

MIB オペレーションはもっとも小さいプロセス ID の RIP プロセスに割り当てられます。

View

System view

定義済みユーザロール

network-admin

パラメータ

process-id: RIP プロセスの ID を指定します。設定範囲は 1～65535 です。

説明

rip mib-binding コマンドは RIP プロセスを MIB のオペレーションに割り当てます。RIP プロセスは SNMP リクエストで受信できます。

undo rip mib-binding コマンドはデフォルトに戻します。

指定したプロセス ID が存在しない場合、MIB のオペレーションへの追加が失敗します。

MIB のオペレーションに割り当てた RIP プロセスを削除すると、MIB のオペレーションの割り当て設定が削除されます。

RIP プロセスが削除されたのち、MIB のオペレーションは、RIP プロセスがもっとも小さいプロセス ID に割り当てます。

例

MIB オペレーションを RIP プロセス 100 に割り当てます。

<Switch> system-view

[Switch] rip mib-binding 100

4.1.30 rip output

Syntax

rip output

undo rip output

デフォルト

有効

View

Interface view

定義済みユーザロール

network-admin

説明

rip output コマンドは RIP メッセージを送信するインタフェースを有効にします。

undo rip output コマンドは RIP メッセージを送信するインタフェースを無効にします。

例

RIP メッセージを送信する VLAN インタフェース 10 を無効にします。

<Switch> system-view

[Switch] interface vlan-interface 10

[Switch-Vlan-interface10] undo rip output

4.1.31 rip poison-reverse

Syntax

rip poison-reverse

undo rip poison-reverse

デフォルト

無効

View

Interface view

定義済みユーザロール

network-admin

説明

rip poison-reverse コマンドはポイズンリバースを有効にします。

undo rip poison-reverse コマンドはポイズンリバースを無効にします。

例

VLAN インタフェース 10 でポイズンリバースを有効にします。

<Switch> system-view

[Switch] interface vlan-interface 10

[Switch-Vlan-interface10] rip poison-reverse

4.1.32 rip split-horizon

Syntax

rip split-horizon

undo rip split-horizon

デフォルト

有効

View

Interface view

定義済みユーザロール

network-admin

説明

ip split-horizon コマンドはスプリットホライズンを有効にします。

undo rip split-horizon コマンドはスプリットホライズンを無効にします。

- スプリットホライズンはルーティングループを防ぎます。この機能を無効にする場合、必要不可欠であるかどうかを確認してください。
- スプリットホライズンとポイズンリバースの両方が有効である場合、ポイズンリバースのみが適用されます。

例

VLAN インタフェース 10 でスプリットホライズンを有効にします。

<Switch> system-view

[Switch] interface vlan-interface 10

[Switch-Vlan-interface10] rip split-horizon

4.1.33 rip summary-address

Syntax

rip summary-address *ip-address* { *mask-length* | *mask* }

undo rip summary-address *ip-address* { *mask-length* | *mask* }

デフォルト

インタフェースに集約ルートが設定されていません。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

ip-address: 集約ルートの宛先 IP アドレスを指定します。

mask-length: 集約ルートのサブネットマスク長を指定します。設定範囲は 0～32 です。

mask: 集約ルートのサブネットマスクを指定します。ドットで区切り、10 進数で指定します。

説明

rip summary-address コマンドはインタフェース上の集約ルートを設定します。

undo rip summary-address コマンドはインタフェース上の集約ルートを削除します。

このコマンドは自動ルート集約が無効であるときのみ、適用されます。

例

VLAN インタフェース 10 で集約ルートを配信します。

<Switch> system-view

[Switch] interface vlan-interface 10

[Switch-Vlan-interface10] rip summary-address 10.0.0.0 255.255.255.0

関連コマンド

summary

4.1.34 rip version

Syntax

rip version { **1** | **2** [**broadcast** | **multicast**] }

undo rip version

デフォルト

インタフェースで RIP バージョンは設定されていません。インタフェースは RIPv1 ブロードキャストメッセージを送信し、RIPv1 ブロードキャストメッセージ、RIPv1 ユニキャストメッセージ、RIPv2 ブロードキャストメッセージ、RIPv2 マルチキャストメッセージ、RIPv2 ユニキャストメッセージを受信します

View

Interface view

定義済みユーザロール

network-admin

パラメータ

1: RIP のバージョンを RIPv1 に指定します。

2: RIP のバージョンを RIPv2 に指定します。

[**broadcast** | **multicast**]: ブロードキャストモードあるいはマルチキャストモード（デフォルト）で RIPv2 メッセージを送信します。

説明

rip version コマンドはインタフェースで RIP バージョンを指定します。

undo rip version コマンドはデフォルトに戻します。

インタフェースで RIP バージョンが設定されていない場合、グローバルの RIP バージョンを使用します。インタフェースで RIP バージョンが設定されている場合、インタフェースで設定された RIP バージョンを使用します。

RIPv1 で動作するインタフェースは以下の動作を行うことができます。

- RIPv1 ブロードキャストメッセージを送信します。
- RIPv1 ブロードキャストメッセージ、RIPv1 ユニキャストメッセージを受信します。

ブロードキャストモードで RIPv2 が動作するインタフェースは以下の動作を行うことができます。

- RIPv2 ブロードキャストメッセージを送信します。
- RIPv1 ブロードキャストメッセージ、RIPv1 ユニキャストメッセージ、RIPv2 ブロードキャストメッセージ、RIPv2 マルチキャストメッセージ、RIPv2 ユニキャストメッセージを受信します。

マルチキャストモードで RIPv2 が動作するインタフェースは以下の動作を行うことができます。

- RIPv2 ブロードキャストメッセージを送信します。
- RIPv2 ブロードキャストメッセージ、RIPv2 マルチキャストメッセージ、RIPv2 ユニキャストメッセージを受信します。

例

VLAN インタフェース 10 で RIPv2 がブロードキャストモードで動作するように設定します。

<Switch> system-view

[Switch] interface vlan-interface 10

[Switch-Vlan-interface10] rip version 2 broadcast

関連コマンド

version

4.1.35 silent-interface

Syntax

silent-interface { *interface-type interface-number* | **all** }

undo silent-interface { *interface-type interface-number* | **all** }

デフォルト

すべてのインタフェースで RIP メッセージの送信が有効です。

View

RIP view

定義済みユーザロール

network-admin

パラメータ

interface-type interface-number: 指定されたインタフェースで RIP メッセージの送信を無効にします。

all: すべてのインタフェースで RIP メッセージの送信を無効にします。

説明

silent-interface コマンドはインタフェースで RIP メッセージの送信を無効にします。インタフェースは RIP メッセージの受信は行うことができます。

undo silent-interface コマンドはデフォルトに戻します。

例

VLAN インタフェース 10 を除いたすべてのインタフェースで RIP メッセージの送信を無効にします。

<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

4.1.36 summary

Syntax

summary

undo summary

デフォルト

有効

View

RIP view

定義済みユーザロール

network-admin

説明

summary コマンドは RIPv2 ルートの自動集約を有効にします。ナチュラルマスクは、ルーティングテーブルのサイズを減少するために、集約ルートを配信するのに使用します。

undo summary コマンドはすべてのサブネットルートを配信するため、RIPv2 ルートの自動集約を無効にします。

RIPv2 ルートの自動集約は大規模ネットワークの拡張性と効率性の効率を向上するため、ルーティングテーブルのサイズを減少することができます。

例

RIPv2 ルートの自動集約を無効にします。

<Switch> system-view

[Switch] rip

[Switch-rip-1] undo summary

関連コマンド

rip summary-address

rip version

4.1.37 timers

Syntax

timers { **garbage-collect** *garbage-collect-value* | **suppress** *suppress-value* | **timeout** *timeout-value* | **update** *update-value* } *

undo timers { **garbage-collect** | **suppress** | **timeout** | **update** } *

デフォルト

ガーベッジコレクトタイマが 120 秒、サプレスタイマが 120 秒、タイムアウトタイマが 180 秒、アップデートタイマが 30 秒です。

View

RIP view

定義済みユーザロール

network-admin

パラメータ

garbage-collect-value: ガーベッジコレクト時間を指定します。設定範囲は 1～3600 秒です。

suppress-value: サプレス状態（到達不能状態）にとどまる時間のサプレスタイマを指定します。設定範囲は 0～3600 秒です。

timeout-value: エージングタイムを指定します。設定範囲は 1～3600 秒です。

update-value: アップデートタイマを指定します。設定範囲は 1～3600 秒です。

説明

timers コマンドは RIP タイマを設定します。

undo timers コマンドはデフォルトに戻します。

RIP は以下のタイマを使用します。

- **アップデートタイマ**－ルーティングテーブルのアップデート間隔を指定します。
- **タイムアウトタイマ**－ルートエージングタイムを指定します。もしエージング時間内にルートのアップデートを受信しない場合、RIP はルートのメトリックを 16 に設定します。
- **サプレスタイマ**－RIP ルートがサプレス状態(到達不能状態)にとどまる時間を指定します。ルートのメトリックが 16 のとき、ルータはサプレス状態になります。停止した到達不能ルートは、アップデートされたルートによって置き換わります。このアップデートされたルートはサプレスタイマが満了する前に同一のネイバ装置から受信したルートで、メトリックは 16 より小さい値を持ちます。
- **ガーベッジコレクトタイマ**–ルートのメトリックが 16 になる時点から、そのルートがルーティングテーブルから削除されるまでの間隔を指定します。RIP はメトリックが 16 のルートを配信します。タイマの時間が過ぎた後も、そのルートへのルーティングアップデートが行われない場合、ルートはルーティグテーブルから削除されます。

これらのタイマの値は特に必要がない限りデフォルトから変更しないことを推奨します。

タイマの値はネットワークのすべてのルータで統一する必要があります。

タイムアウトタイマはアップデートタイマよりも大きくしてください。

例

アップデートタイマを 5 秒、タイムアウトタイマを 15 秒、サプレスタイマを 15 秒、ガーベッジコレクトタイマを 30 秒に設定します。

<Switch> system-view

[Switch] rip 100

[Switch-rip-100] timers update 5 timeout 15 suppress 15 garbage-collect 30

4.1.38 validate-source-address

Syntax

validate-source-address

undo validate-source-address

デフォルト

Source IP address check on inbound RIP routing updates is enabled.

View

RIP view

定義済みユーザロール

network-admin

説明

validate-source-address コマンドは受信 RIP ルーティングアップデートの送信元 IP アドレスチェックを有効にします。

undo validate-source-address コマンドは受信 RIP ルーティングアップデートの送信元 IP アドレスチェックを無効にします。

例

受信 RIP ルーティングアップデートの送信元 IP アドレスのチェックを無効にします。

<Switch> system-view

[Switch-rip] rip 100

[Switch-rip-100] undo validate-source-address

4.1.39 version

Syntax

version { **1** | **2** }

undo version

デフォルト

グローバルの RIP バージョンは設定されていません。インタフェースは RIPv1 ブロードキャストメッセージを送信し、RIPv1 ブロードキャストメッセージ、RIPv1 ユニキャストメッセージ、RIPv2 ブロードキャストメッセージ、RIPv2 マルチキャストメッセージ、RIPv2 ユニキャストメッセージを受信します。

View

RIP view

定義済みユーザロール

network-admin

パラメータ

1: RIP のバージョンを RIPv2 に指定します。

2: RIP のバージョンを RIPv2 に指定します。RIPv2 メッセージはマルチキャストです。

説明

version コマンドはグローバルの RIP バージョンを指定します。

undo version コマンドはデフォルトに戻します。

インタフェースは、グローバルの RIP バージョンより、インタフェースで設定された RIP バージョンを優先します。

インタフェースに RIP バージョンが指定されておらず、グローバルバージョンが RIPv1 の場合、インタフェースは RIPv1 を使用し、次の操作を実行できます。

- RIPv1 ブロードキャストを送信します。
- RIPv1 ブロードキャストとユニキャストを受信する。

インタフェースに RIP バージョンが指定されておらず、グローバルバージョンが RIPv2 の場合、インタフェースは RIPv2 マルチキャストモードを使用し、次の操作を実行できます。

- RIPv2 マルチキャストを送信します。
- RIPv2 ブロードキャスト、マルチキャスト、およびユニキャストを受信します。

例

グローバルの RIP のバージョンを RIPv2 に指定します。

<Switch> system-view

[Switch] rip 100

[Switch-rip-100] version 2

関連コマンド

rip version

目次

このセクションのページは **5-x-x** です。

5 章 OSPF 5-1
5.1 OSPF 設定コマンド 5-1
5.1.1 abr-summary (OSPF area view) 5-1
5.1.2 area (OSPF view) 5-2
5.1.3 asbr-summary 5-3
5.1.4 authentication-mode 5-4
5.1.5 bandwidth-reference (OSPF view) 5-6
5.1.6 default 5-7
5.1.7 default-cost (OSPF area view) 5-8
5.1.8 default-route-advertise (OSPF view) 5-9
5.1.9 description (OSPF/OSPF area view) 5-11
5.1.10 display ospf 5-12
5.1.11 display ospf abr-asbr 5-19
5.1.12 display ospf abr-summary 5-21
5.1.13 display ospf asbr-summary 5-23
5.1.14 display ospf event-log 5-25
5.1.15 display ospf graceful-restart 5-31
5.1.16 display ospf interface 5-34
5.1.17 display ospf lsdb 5-37
5.1.18 display ospf nexthop 5-41
5.1.19 display ospf non-stop-routing status 5-42
5.1.20 display ospf peer 5-43
5.1.21 display ospf peer statistics 5-47
5.1.22 display ospf request-queue 5-48
5.1.23 display ospf retrans-queue 5-50
5.1.24 display ospf routing 5-51
5.1.25 display ospf statistics 5-54
5.1.26 display ospf vlink 5-57
5.1.27 display router id 5-58
5.1.28 dscp 5-59
5.1.29 enable link-local-signaling 5-60
5.1.30 enable out-of-band-resynchronization 5-60
5.1.31 event-log 5-61
5.1.32 fast-reroute (OSPF view) 5-62
5.1.33 filter (OSPF area view) 5-63
5.1.34 filter-policy export (OSPF view) 5-64

5.1.35 filter-policy import (OSPF view)....5-66
5.1.36 graceful-restart (OSPF view)....5-67
5.1.37 graceful-restart helper enable....5-69
5.1.38 graceful-restart helper strict-lsa-checking....5-70
5.1.39 graceful-restart interval (OSPF view)....5-71
5.1.40 host-advertise....5-71
5.1.41 import-route (OSPF view)....5-72
5.1.42 log-peer-change....5-74
5.1.43 lsa-arrival-interval....5-75
5.1.44 lsa-generation-interval....5-76
5.1.45 lsdb-overflow-interval....5-77
5.1.46 lsdb-overflow-limit....5-78
5.1.47 maximum load-balancing (OSPF view)....5-79
5.1.48 network (OSPF area view)....5-80
5.1.49 non-stop-routing....5-81
5.1.50 nssa(OSPF area view)....5-81
5.1.51 opaque-capability enable....5-83
5.1.52 ospf....5-84
5.1.53 ospf authentication-mode....5-85
5.1.54 ospf bfd enable....5-87
5.1.55 ospf cost....5-88
5.1.56 ospf dr-priority....5-89
5.1.57 ospf mib-binding....5-89
5.1.58 ospf mtu-enable....5-90
5.1.59 ospf network-type....5-91
5.1.60 ospf timer dead....5-92
5.1.61 ospf timer hello....5-93
5.1.62 ospf timer poll....5-94
5.1.63 ospf timer retransmit....5-95
5.1.64 ospf trans-delay....5-96
5.1.65 peer....5-97
5.1.66 preference....5-98
5.1.67 reset ospf event-log....5-99
5.1.68 reset ospf statistics....5-100
5.1.69 reset ospf process....5-100
5.1.70 reset ospf redistribution....5-101
5.1.71 rfc1583 compatible....5-102
5.1.72 router id....5-103
5.1.73 silent-interface (OSPF view)....5-104
5.1.74 snmp-agent trap enable ospf....5-105
5.1.75 spf-schedule-interval....5-106
5.1.76 stub (OSPF area view)....5-107
5.1.77 stub-router....5-108

5.1.78 transmit-pacing 5-110
5.1.79 vlink-peer (OSPF area view) 5-111

5章 OSPF

5.1 OSPF設定コマンド

5.1.1 abr-summary (OSPF area view)

Syntax

abr-summary *ip-address* { *mask-length* | *mask* } [**advertise** | **not-advertise**] [**cost** *cost*]

undo abr-summary *ip-address* { *mask-length* | *mask* }

デフォルト

設定なし

View

OSPF area view

定義済みユーザロール

network-admin

パラメータ

ip-address: ドットで区切られた 10 進数で集約ルートの宛先 IP アドレスを指定します。

mask-length: マスク長を指定します。設定範囲は 0～32 です。

mask: ドットで区切られた 10 進数で IP アドレスのマスクを指定します。

advertise | **not-advertise**: 集約ルートを配信するか、あるいは配信しないかを指定します。デフォルトで **abr-summary** コマンドは集約ルートを配信します。

cost *cost*: 集約ルートのコストを指定します。設定範囲は 1～16777215 です。デフォルトのコストは集約されるルートのなかでもっとも大きい値です。

説明

abr-summary コマンドは ABR（area border router）の集約ルートを設定します。

undo abr-summary コマンドは設定を削除します。

このコマンドは複数の連続するネットワークを 1 つのネットワークに集約するため、ABR でのみ有効です。

指定したルートを配信する ABR を有効にする場合、**undo abr-summary** コマンドを使用します。

例

エリア 1 のネットワーク 36.42.10.0/24、36.42.110.0/24 を 36.42.0.0.16 に集約します。

<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

5.1.2 area (OSPF view)

Syntax

area *area-id*

undo area *area-id*

デフォルト

設定なし

View

OSPF view

定義済みユーザロール

network-admin

パラメータ

area-id: エリアを IP アドレスあるいは 10 進数の整数のエリア ID で指定します。10 進数の整数の設定範囲は 0～4294967295 です。この 10 進数の整数はシステムで IP アドレスの形式に変換されます。

説明

area コマンドはエリアを作成し、area view に移行します。

undo area コマンドはエリアを削除します。

例

エリア 0 を作成し、area 0 view に移行します。

<Switch> system-view

[Switch] ospf 100

[Switch-ospf-100] area 0

[Switch-ospf-100-area-0.0.0.0]

5.1.3 asbr-summary

Syntax

asbr-summary *ip-address* { *mask-length* | *mask* } [**cost** *cost* | **not-advertise** | **nssa-only** | **tag** *tag*] *

undo asbr-summary *ip-address* { *mask-length* | *mask* }

デフォルト

設定なし

View

OSPF view

定義済みユーザロール

network-admin

パラメータ

ip-address: 集約ルートの宛先 IP アドレスを指定します。

mask-length: マスク長を指定します。設定範囲は 0～32 です。

mask: ドットで区切られた 10 進数でマスクを指定します。

cost *cost*: 集約ルートのコストを指定します。設定範囲は 1～16777214 です。指定しない場合、Type-1 の外部ルートのデフォルトコストは、集約されるルートのなかでもっとも大きいコストとなります。Type-2 の外部ルートのデフォルトコストは、集約されるルートのなかでもっとも大きいコスト＋1 となります。

not-advertise: 集約ルートの配信を無効にします。パラメータを指定しない場合、ルートを配信します。

nssa-only: Type-7 の LSA の P ビットを 0 に設定することで NSSA へのルートの配信を制限します。デフォルトで Type-7 の LSA の P ビットは 1 です。もし ASBR が ABR で、バックボーンエリアで FULL 状態である場合、ASBR は Type-7 LSA の P ビットを 0 にします。このパラメータは NSSAASBR に適用します。

tag *tag*: 集約ルートを作成するためにタグを指定します。設定範囲は 0～4294967295 です。デフォルトは 1 です。タグは集約ルートの配信を管理するため、ルーティングポリシーで使用することができます。

説明

asbr-summary コマンドは ASBR（autonomous system boundary router）の集約ルートを設定します。

undo asbr-summary コマンドは設定を削除します。

ASBR は以下の LSA のルートを集約することができます。

- Type-5 LSA
- NSSA エリアの Type-7 LSA
- NSSA エリアの Type-7 LSA から ASBR（ABR を含みます）によって変換された Type-5 LSA

ASBR（ABR）が変換していない場合、Type-7 LSA から変換された Type-5 LSA のルートを集約することはできません。

ASBR が集約された指定のルートを配信するようにする場合、**undo asbr-summary** コマンドを使用します。

例

再配信されたスタティックルートを 1 つのルートに集約し、集約ルートのタグを 2、コストを 100 に設定します。

<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

関連コマンド

display ospf asbr-summary

5.1.4 authentication-mode

Syntax

MD5/HMAC-MD5 認証：

authentication-mode { **hmac-md5** | **md5** } *key-id* { **cipher** | **plain** } *password*

undo authentication-mode [{ **hmac-md5** | **md5** } *key-id*]

simple 認証：

authentication-mode simple { **cipher** | **plain** } *password*

undo authentication-mode

デフォルト

設定なし

View

OSPF area view

定義済みユーザロール

network-admin

パラメータ

hmac-md5: HMAC-MD5 認証モードを指定します。

md5: MD5 認証モードを指定します。

simple: 簡易認証モードを指定します。

key-id: キーの ID を指定します。設定範囲は 0～255 です。

cipher: 暗号テキストキーを指定します。

plain: プレーンテキストキーを指定します。

password: パスワードを指定します。簡易認証モードのプレーンテキストの設定範囲は 1～8 文字です。大文字、小文字を区別します。簡易認証モードの暗号テキストの設定範囲は 33～41 文字です。大文字、小文字を区別します。MD5/HMAC-MD5 認証モードのプレーンテキストの設定範囲は 1～16 文字です。大文字、小文字を区別します。MD5/HMAC-MD5 認証モードの暗号テキストの設定範囲は 33～53 文字です。大文字、小文字を区別します。

説明

authentication-mode コマンドは OSPF エリアの認証モードを設定します。

undo authentication-mode コマンドはデフォルトに戻します。

同一エリアにあるルータは認証モードとパスワードを同一にする必要があります。

セキュリティのため、プレーンテキストで設定されたキーを含むすべてのキーは暗号テキストで保存されます。

OSPF エリアで MD5/HMAC-MD5 認証あるいは簡易認証のいずれかを指定することができます。MD5/HMAC-MD5 認証では **authentication-mode** コマンドを複数実行することで複数のキーを設定することができます。各コマンドは固有のキーID とキーの文字列にする必要があります。

OSPF エリアのキーを修正する場合、以下の交換の設定を実行してください。

1) ローカル装置のエリア用に新規の MD5/HMAC-MD5 認証キーを設定します。隣接装置で新しいキーが設定されていない場合、MD5/HMAC-MD5 認証のキーの交換が開始します。キーの交換が行われている間、OSPF は新しい MD5/HMAC-MD5 認証キーと古い MD5/HMAC-MD5 認証キーが含まれる複数のパケットを送信します。すべての隣接装置で認証がパスすることを確認してください。
2) すべての隣接装置の新しい MD5/HMAC-MD5 認証キーを設定します。ローカル装置がすべての隣接装置から新しいキーのパケットを受信するとき、MD5 キーの交換が行われます。
3) ローカル装置とすべての隣接装置から古い MD5/HMAC-MD5 認証キーを削除します。この処理を行うことで、通信を行うために古いキーを使用している装置が攻撃されることを防ぎ、キーの交換によって引き起こされるシステムリソース、帯域幅の消費を削減することができます。

例

MD5 認証モードを使用する OSPF エリア 0 を設定し、キーID を 15、プレーンテキストで、認証パスワードを abc に設定します。

<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

関連コマンド

ospf authentication-mode

5.1.5 bandwidth-reference (OSPF view)

Syntax

bandwidth-reference *value*

undo bandwidth-reference

デフォルト

100 Mbps

View

OSPF view

定義済みユーザロール

network-admin

パラメータ

value: リンクコストの計算に必要な帯域幅の基準値を指定します。設定範囲は 1～4294967 Mbps です。

説明

bandwidth-reference コマンドはリンクコストの計算に必要な帯域幅の基準値を設定します。

undo bandwidth-reference コマンドはデフォルトに戻します。

リンクにコストが設定されていない場合、OSPF は以下の計算式を使用してコストを計算します。

コスト＝帯域幅の基準値（100Mbps）／インタフェースの帯域幅（Mbps）

計算した値が 65535 よりも大きい場合、コストは 65535 となります。計算した値が 1 よりも小さい場合、コストは 1 となります。デフォルトのコストを以下に示します。

- 56kbps シリアルインタフェース ：1785
- 64kbps シリアルインタフェース ：1562
- 2.048 Mbps インタフェース ：48
- 100 Mbps Ethernet インタフェース：1
- loopback インタフェース ：0

例

帯域幅の基準値を 1000 Mbps に設定します。

<Switch> system-view

[Switch] ospf 100

[Switch-ospf-100] bandwidth-reference 1000

関連コマンド

ospf cost

5.1.6 default

Syntax

default { **cost** *cost* | **tag** *tag* | **type** *type* } *

undo default { **cost** | **tag** | **type** } *

デフォルト

コストは 1、タグは 1、ルートタイプは 2 です。

View

OSPF view

定義済みユーザロール

network-admin

パラメータ

cost *cost*: 再配信ルートのデフォルトコストを指定します。設定範囲は 0～16777214 です。

tag *tag*: 再配信ルートをマーキングするタグを指定します。設定範囲は 0～4294967295 です。

type *type*: 再配信ルートのタイプを指定します。設定範囲は 1 あるいは 2 です。

説明

default コマンドは再配信ルートのデフォルトパラメータを設定します。

undo default コマンドは設定を削除します。

例

外部ルートのデフォルトコストを 10、デフォルトタグを 100、タイプを 2 に設定します。

<Switch> system-view

[Switch] ospf 100

[Switch-ospf-100] default cost 10 tag 100 type 2

関連コマンド

import-route

5.1.7 default-cost (OSPF area view)

Syntax

default-cost *cost*

undo default-cost

デフォルト

1

View

OSPF area view

定義済みユーザロール

network-admin

パラメータ

cost: スタブあるいは NSSA エリアに配信されるデフォルトルートのコストを指定します。設定範囲は 0～16777214 です。

説明

default-cost コマンドはスタブあるいは NSSA エリアに配信されるデフォルトルートのコストを設定します。

undo default-cost コマンドはデフォルトに戻します。

このコマンドはスタブエリアの ABR、あるいは NSSA エリアの ABR/ASBR でのみ適用します。

例

スタブエリアとしてエリア 1 を設定し、スタブエリアに配信されるデフォルトルートのコストを 20 に設定します。

```
<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
```

関連コマンド

- **nssa**
- **stub**

5.1.8 default-route-advertise (OSPF view)

Syntax

default-route-advertise [[[**always** | **permit-calculate-other**] | **cost** *cost* | **route-policy** *route-policy-name* | **type** *type*] * | **summary cost** *cost*]

undo default-route-advertise

デフォルト

設定なし

View

OSPF view

定義済みユーザロール

network-admin

パラメータ

always: ルーティングテーブルにデフォルトルートが存在するかどうかにかかわらず、Type-5 LSA のデフォルトルートを OSPF ルーティングドメインに作成します。指定しない場合、現在の OSPF プロセスが所属していないアクティブなデフォルトルートが IP ルーティングテーブルに存在するときのみ、デフォルトルートを作成します。

permit-calculate-other: ほかのルータから受信したデフォルトルートを計算するために OSPF を有効にします。指定しない場合、OSPF はほかのルータからデフォルトルートを計算しません。ルータが Type-5 LSA のデフォルトルートを OSPF ルーティングドメインに作成しない場合、ルータはほかのルータからデフォルトルートを計算します。OSPF は **permit-calculate-other** パラメータが指定されているかどうかにかかわらず、ルートを計算します。

cost *cost*: デフォルトルートのコストを指定します。設定範囲は 0～16777214 です。指定しない場合、**default-cost** コマンドで指定されたデフォルトルートが適用されます。

route-policy *route-policy-name*: ルーティングポリシーの名前を指定します。設定範囲は 1～63 です。大文字、小文字を区別します。ルーティングテーブルにデフォルトルートが存在し、指定したルーティングポリシーが一致する場合、Type-5 LSA のデフォルトルートを OSPF ルーティングドメインに配信します。ルーティングポリシーは Type-5 LSA の値を変更します。**route-policy** パラメータと同時に **always** パラメータが指定された場合、指定したルーティングポリシーが一致するとき、Type-5 LSA のデフォルトルートを OSPF ルーティングドメインに配信します。このコマンドはルーティングテーブルにデフォルトルートが存在するかどうかにかかわらず、ルートを配信します。ルーティングポリシーは Type-5 LSA の値を変更します。

type *type*: Type-5 LSA のタイプを指定します。設定範囲は 1 あるいは 2 です。指定しない場合、**default type** コマンドによって指定された Type-5 LSA のデフォルトタイプが適用されます。

summary: Type-3 LSA の指定されたデフォルトルートを配信します。このパラメータは VPN でのみ有効です。

説明

default-route-advertise コマンドはデフォルトルートを OSPF ルーティングドメインに再配信します。

undo default-route-advertise コマンドはデフォルトに戻します。

このコマンドは Type-5 LSA のデフォルトルートを再配信します。**import-route** コマンドでデフォルトルートを再配信することはできません。ローカルのルーティングテーブルにデフォルトルートがない場合、**always** パラメータを適用する必要があります。

default-route-advertise summary cost コマンドは VPN でのみ有効です。**default-route-advertise summary cost** コマンドを設定することで、PE ルータは Type-3 LSA のデフォルト外部ルートを CE ルータに再配信します。

例

ローカルのルーティングテーブルにデフォルトルートがあるかどうかにかかわらずデフォルトルートを OSPF ルーティングドメインに作成します。

<Switch> system-view

[Switch] ospf 100

[Switch-ospf-100] default-route-advertise always

関連コマンド

- **default**
- **import-route**

5.1.9 description (OSPF/OSPF area view)

Syntax

description *description*

undo description

デフォルト

設定なし

View

OSPF view, OSPF area view

定義済みユーザロール

network-admin

パラメータ

description: OSPF view の OSPF プロセス、あるいは OSPF area view の OSPF エリアの説明を設定します。設定範囲は 1～80 文字です。

説明

description コマンドは OSPF プロセスあるいは OSPF エリアの説明を設定します。

undo description コマンドはデフォルトに戻します。

このコマンドで設定された説明は OSPF プロセスあるいは OSPF エリアを識別するために使用します。

例

OSPF プロセス 100 に説明 abc を設定します。

<Switch> system-view

[Switch] ospf 100

[Switch-ospf-100] description abc

OSPF エリア 0 に説明 bone area を設定します。

<Switch> system-view

[Switch] ospf 100

[Switch-ospf-100] area 0

[Switch-ospf-100-area-0.0.0.0] description bone area

5.1.10 display ospf

Syntax

display ospf [*process-id*] [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

process-id: OSPF プロセスを指定します。設定範囲は 1～65535 です。指定しない場合、すべての OSPF プロセスの情報を表示します。

verbose: OSPF プロセスの詳細情報を表示します。指定しない場合、OSPF プロセスの概要情報を表示します。

説明

display ospf コマンドは OSPF プロセスの情報を表示します。

例

OSPF プロセスの詳細情報を表示します。

<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
Opaque capable
Originating router-LSAs with maximum metric
   Condition: On startup while BGP is converging, 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-interface1)
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
```

表 5-1 コマンド出力

フィールド	説明
OSPF Process 1 with Router ID 192.168.1.2	OSPFプロセスID、OSPFルータIDです。
RouterID	ルータIDです。
Router type	ルータタイプです。 ● **ABR**－ABRタイプです。 ● **ASBR**－ASBRタイプです。 ● **NSSA**－NSSAタイプです。 ● **Null**－ルータタイプがありません。
Route tag	再配信ルートのタグです。
Multi-VPN-Instance is not enabled	OSPFプロセスがマルチVPNインスタンスをサポートしていません。
Ext-community type	OSPF拡張コミュニティ属性タイプのコードです。 ● **domain ID**—ドメインIDのコードです。 ● **router type**—ルータタイプのコードです。 ● **router ID**—ルータIDのコードです。
Opaque capable	Opaque LSAの配信と受信が有効です。
Originating router-LSAs with maximum metric	スタブリンクを除くルータLSAの最大コストの値が使用されています。
Condition	スタブルータの状態です。 ● Alway状態です。 ● *xxx*秒間、起動します。*xxx*はユーザによって指定されます。
State	スタブルータがアクティブかどうかを示します。
SPF-schedule-interval	SPFを計算する間隔です。
LSA generation interval	LSAを作成する間隔です。
LSA arrival interval	LSA到着間隔です。
Transmit pacing	インタフェースのLSUパケットの転送レートです。 ● **Interval**–インタフェースのLSU転送間隔です。 ● **Count**–毎回、LSUパケットの最大数が送信されました。
Default ASE Parameter	デフォルトASEパラメータです。メトリック、タグ、ルートタイプがあります。
Route preference	内部ルートの優先順位です。

フィールド	説明
ASE route preference	外部ルートの優先順位です。
SPF computation count	OSPFプロセスのSPF計算回数です。
RFC1583 compatible	RFC1583と互換性があります。
SNMP trap rate limit interval	SNMP notificationの送信間隔です。
Count	SNMP notificationを送信した回数です。
ExChange/Loading neighbors	ExChange/Loading状態の隣接です。
Full neighbors	FULL状態の隣接です。
Calculation trigger type	ルート計算の起動タイプです。 ● **Full**–すべてのルートの計算が開始します。 ● **Area topology change**－エリアのトポロジが変更します。 ● **Intra router change**－incremental内部エリアのルートが変更します。 ● **ASBR change**－incrementalのASBRルートが変更します。 ● **7to5 translator**－Type-7からType-5にLSAの役割が変更します。 ● **Full IP prefix**－すべてのIPプレフィックスの計算が開始します。 ● **N/A**－ルートの計算が開始しません。
Current calculation type	現在のルート計算のタイプです。 ● SPFの計算です。 ● **Intra router calculation**－エリア内のルート計算です。 ● **ASBR calculation**－エリア間のASBRルート計算です。 ● **Inc intra router**－Incrementalエリア内のルート計算です。 ● **Inc ASBR calculation**－Incrementalエリア間のASBRルート計算です。 ● **7to5 translator**－Type-7からType-5へのLSAを変換する計算です。 ● **Forward address**－転送するアドレスの計算です。 ● **N/A**－ルート計算が開始しません。

フィールド	説明
Current calculation phase	現在のルート計算のフェーズです。 ● **Calculation area topology**－エリアトポロジを計算しています。 ● **Calculation router**－ルータのルートを計算しています。 ● **7to5 translator**－Type-7からType-5へLSAの変換を計算しています。 ● **Forward address**－転送するアドレスを計算しています。 ● **Calculation end**－計算の終了フェーズです。 ● **N/A**－ルート計算が開始していません。
Process reset state	プロセスのリセット状態です。 ● **N/A**－プロセスがリセットしていません。 ● **Under reset**－プロセスがリセットしています。 ● **Under RIB smooth**－プロセスがRIBの同期化を行っています。
Current reset type	現在のプロセスリセットタイプです。 ● **N/A**－プロセスがリセットしていません。 ● **Normal**－通常のリセットです。 ● **GR quit**－GRが異常終了したとき、通常リセットを行います。 ● **Delete**－OSPFプロセスを削除します。 ● **VPN delete**－VPNを削除します。
Nextreset type	次回のプロセスリセットタイプです。 ● **N/A**－プロセスがリセットしていません。 ● **Normal**－通常のリセットです。 ● **GR quit**－GRが異常終了したとき、通常リセットを行います。 ● **Delete**－OSPFプロセスを削除します。 ● **VPN delete**－VPNを削除します。
Reset prepare message replied	リセット準備のメッセージを応答するモジュールです。 ● **P**－隣接メンテナンスモジュールです。 ● **L**－LSDB同期モジュールです。 ● **C**－ルート計算モジュールです。 ● **R**－ルート再配信モジュールです。

フィールド	説明
Reset process message replied	リセットプロセスメッセージを応答するモジュールです。 • **P**－隣接メンテナンスモジュールです。 • **L**－LSDB同期モジュールです。 • **C**－ルート計算モジュールです。 • **R**－ルート再配信モジュールです。

Reset phase of module	各モジュールのリセットフェーズです。
	• メインコントロールモジュールです。
	  • **N/A**－リセットしません。
	  • エリアを削除します。
	  • プロセスを削除します。
	• 隣接メンテナンスモジュール(P)です。
	  • **N/A**－リセットしません。
	  • 隣接を削除します。
	  • インタフェースを削除します。
	  • **Delete vlink**－仮想リンクを削除します。
	  • **Delete shamlink**－shamリンクを削除します。
	• LSDB 同期(L) モジュールです。
	  • **N/A**－リセットしません。
	  • タイマを停止します。
	  • **Delete ASE**－すべてのASE LSAを削除します。
	  • **Delete ASE maps**－ASE LSAマップを削除します。
	  • プロセスデータをクリアします。
	  • **Delete area LSA**－エリアからLSAとマップを削除します。
	  • **Delete area interface**－エリアからインタフェースを削除します。
	  • **Delete process**－プロセスに関連するリソースを削除します。
	  • **Restart**－プロセスに関連するリソースを再起動します。
	• ルート計算(C) モジュールです。
	  • **N/A**－リセットしません。
	  • **Delete topology**－エリアトポロジを削除します。
	  • **Delete router**－ルータのルートを削除します。
	  • **Delete forward address**－転送アドレスリストを削

フィールド	説明
	除します。 • **Delete advertise**－配信するルータリストを削除します。 ● ルート再配信(R) モジュールです。 • **N/A**－リセットしません。 • **Delete ABR summary**－ABRの集約ルートを削除します。 • **Delete ASBR summary**－ASBRの集約ルートを削除します。 • **Delete import**－再配信されたルートを削除します。
7/5 translator state	Type-7 LSAからType-5 LSAに変換する状態です。状態は以下の1つになることができます ● **Enabled**－変換はコマンドによって指定されます。 ● **Elected**－変換は選択によって定義されます。 ● **Disabled**–装置は変換しません。
7/5 translate stability timer interval	Type-7 LSAからType-5 LSAに変換する安定間隔です。
ExChange/Loading Neighbors	ExChange/Loading状態の隣接です。
Area	IPアドレスフォーマットのエリアIDです。
Authtype	エリアの認証タイプです。 ● **None**－認証を行いません。 ● **Simple**－Simple認証です。 ● **MD5**－MD5認証です。
Area flag	エリアのタイプです。 ● **Normal**－通常エリアです。 ● **Stub**－スタブエリアです。 ● **StubNoSummary (totally stub area)**－StubNoSummaryエリアです。 ● **NSSA**－NSSAエリアです。 ● **NSSANoSummary (totally NSSA area)**－NSSANoSummaryエリアです。
SPF scheduled Count	OSPFエリアでSFPを計算した回数です。
Interface	エリアのインタフェースです。
Cost	インタフェースコストです。

フィールド	説明
State	インタフェースの状態です。
Type	インタフェースのネットワークタイプです。
MTU	インタフェースのMTUです。
Priority	ルータの優先順位です。
Timers	OSPFのタイマです。 ● **Hello**－Helloパケットを送信する間隔です。 ● **Dead**－隣接がダウンしている間隔です。 ● **Poll**－pollパケットを送信する間隔です。 ● **Retransmit**－LSAを再配信する間隔です。
FRR backup	インタフェースでLSA（Loop Free Alternate）の計算が有効かどうかを示します。
Packet size	インタフェースが送信できるOSPFパケットの最大長です。

5.1.11 display ospf abr-asbr

Syntax

display ospf [*process-id*] **abr-asbr** [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

process-id: OSPF プロセスを指定します。設定範囲は 1～65535 です。指定しない場合、すべての OSPF プロセスの ABR、ASBR へのルート情報を表示します。

verbose: 詳細情報を表示します。指定しない場合、概要情報を表示します。

説明

display ospf abr-asbr コマンドは ABR あるいは ASBR へのルートを表示します。

スタブエリアのルータで **display ospf abr-asbr** コマンドを実行した場合、ASBR の情報は表示しません。

例

#ABR、ASBR へのルートの概要情報を表示します。

<Switch> display ospf abr-asbr

```
        OSPF Process 1 with Router ID 192.168.1.2
              Routing Table to ABR and ASBR

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
```

#ABR、ASBR へのルートの詳細情報を表示します。

<Switch> display ospf abr-asbr verbose

```
        OSPF Process 10 with Router ID 101.1.1.11
              Routing Table to ABR and ASBR

Destination: 1.1.1.1           RtType   : ASBR
Area       : 0.0.0.1           Type     : Intra
Nexthop    : 150.0.1.12        BkNexthop: 0.0.0.0
Cost       : 1000
```

表 5-2 コマンド出力

フィールド	説明
Type	ABRあるいはASBRへのルートタイプです。 ● **Intra**–エリア内ルートです。 ● **Inter**–エリア間ルートです。
Destination	ABR/ASBRのルータIDです。
Area	ネクストホップのエリアのIDです。
Cost	ルータからABR/ASBRへのコストです。
Nexthop	ネクストホップアドレスです。
BkNexthop	バックアップネクストホップアドレスです。
RtType	ルータタイプです。ABRあるいはASBRがあります。

5.1.12 display ospf abr-summary

Syntax

display ospf [*process-id*] [**area** *area-id*] **abr-summary** [*ip-address* { *mask-length* | *mask* }] [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

process-id: OSPF プロセスを指定します。設定範囲は 1～65535 です。指定しない場合、すべての OSPF プロセスの ABR の集約ルート情報を表示します。

area *area-id*: エリアを IP アドレスあるいは 10 進数の整数のエリア ID で指定します。10 進数の整数の設定範囲は 0～4294967295 です。この 10 進数の整数はシステムで IP アドレスの形式に変換されます。指定しない場合、すべての OSPF エリアの ABR の集約ルート情報を表示します。

ip-address: 集約ルートを IP アドレスで指定します。

mask-length: マスク長を指定します。設定範囲は 0～32 です。

mask: ドットで区切られた 10 進数で IP アドレスのマスクを指定します。

verbose: ABR の集約ルートの詳細情報を表示します。指定しない場合、ABR の集約ルートの概要情報を表示します。

説明

display ospf abr-summary コマンドは ABR の集約ルートの情報を表示します。

IP アドレスを指定しない場合、すべての ABR の集約ルートの情報を表示します。

例

ABR の集約ルートの集約ルートの概要情報を表示します。

<Switch> display ospf abr-summary

```
        OSPF Process 1 with Router ID 2.2.2.2
               ABR Summary Addresses

                        Area: 0.0.0.1
 Total summary addresses: 1
 Net             Mask            Status       Count     Cost
 100.0.0.0       255.0.0.0       Advertise    1         (Not Configured)
```

表 5-3 コマンド出力

フィールド	説明
Area	集約ルートが所属しているエリアです。
Total summary addresses	集約ルートの総数です。
Net	集約ルートのアドレスです。
Mask	集約ルートアドレスのマスクです。
Status	集約ルートの配信状態です。
Count	集約されたルートの数です。
Cost	集約ネットワークへのコストです。

#ABR の集約ルータの詳細情報を表示します。

<Switch> display ospf abr-summary verbose

```
        OSPF Process 1 with Router ID 2.2.2.2
               ABR Summary Addresses

 Total summary address count: 1

                      Area: 0.0.0.1
Total summary addresses: 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
```

表 5-4 コマンド出力

フィールド	説明
Destination	集約されたルートの宛先アドレスです。
NetMask	集約されたルータのネットワークマスクです。

フィールド	説明
Metric	集約されたルートのメトリックです。

5.1.13 display ospf asbr-summary

Syntax

display ospf [*process-id*] **asbr-summary** [*ip-address* { *mask-length* | *mask* }]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

process-id: OSPF プロセスを指定します。設定範囲は 1～65535 です。指定しない場合、すべての OSPF プロセスの ASBR の集約ルート情報を表示します。

ip-address: ドットで区切られた 10 進数で IP アドレスを指定します。

mask-length: マスク長を指定します。設定範囲は 0～32 です。

mask: ドットで区切られた 10 進数で IP アドレスのマスクを指定します。

説明

display ospf asbr-summary コマンドは ASBR の集約ルート情報を表示します。

IP アドレスを指定しない場合、すべての ASBR の集約ルートの情報を表示します。

例

OSPF プロセス 1 の ASBR の集約ルート情報を表示します。

<Switch> display ospf 1 asbr-summary

```
        OSPF Process 1 with Router ID 2.2.2.2
               Summary Addresses

 Total Summary Address Count: 1

               Summary Address

 Net         : 30.1.0.0
 Mask        : 255.255.0.0
```

```
Tag         : 20
Status      : Advertise
Cost        : 10 (Configured)
The Count of Route is : 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
```

表 5-5 コマンド出力

フィールド	説明
Total Summary Address Count	集約ルートの総数です。
Net	集約ルートのアドレスです。
Mask	集約ルートアドレスのマスクです。
Tag	集約ルートのタグです。
Status	集約ルートの配信状態です。
Cost	集約ネットワークへのコストです。
The Count of Route	集約されたルートの数です。
Destination	集約ルートの宛先アドレスです。
Net Mask	集約ルートのネットワークマスクです。
Proto	ルートが再配信されたルーティングプロトコルです。
Process	ルートが再配信されたルーティングプロトコルのプロセス IDです。
Type	集約ルートのタイプです。
Metric	集約ルートのメトリックです。

関連コマンド

asbr-summary

5.1.14 display ospf event-log

Syntax

display ospf [*process-id*] **event-log** { **lsa-flush** | **peer** | **spf** }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

process-id: OSPF プロセスを ID で指定します。設定範囲は 1～65535 です。指定しない場合、すべてのプロセスの OSPF ログ情報を表示します。

lsa-flush: LSA エージングログ情報を指定します。

peer: 隣接ログ情報を指定します。

spf: ルート計算ログ情報を指定します。

説明

display ospf event-log コマンドは、OSPF ログ情報を表示します。

ルート計算ログには、IP ルーティングテーブルに新しくインストールされたルートの数が表示されます。

隣接ログには、次のイベントの情報が含まれます。

- OSPF 隣接ステートがダウンします。
- ローカルエンドが BadLSReq、SeqNumberMismatch、および 1-Way イベントを受信したため、OSPF 隣接ステートが逆方向になります。

例

すべてのプロセスの OSPF LSA エージングログ情報を表示します。

<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
```

表 5-6 コマンド出力

フィールド	説明
Date/Time	装置が最大経過時間に達したLSAを受信する時間です。
Received MaxAge LSA from X.X.X.X	装置は、X.X.X.Xから最大経過時間に達したLSAを受信しました。
Flushed MaxAge LSA by the self	装置は、最大経過時間に達したLSAをフラッシュしました。
Type	LSAタイプです。
LS ID	LSAリンクステートIDです。
AdvRtr	配信ルータです。
Seq#	LSAシーケンス番号です。

すべてのプロセスの OSPF ルート計算ログ情報を表示します。

<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
```

表 5-7 コマンド出力

フィールド	説明
Topology	このフィールドは、現在のソフトウェアバージョンではサポートされていません。 トポロジ名です。ベーストポロジのトポロジ名は**base**です。
MTID	このフィールドは、現在のソフトウェアバージョンではサポートされていません。 トポロジIDです。値0は、ベーストポロジを示します。
Date/Time	ルート計算が開始される時刻です。
Duration	ルート計算の継続時間です(秒単位)。
Intra	IPルーティングテーブルに新しく設置されたエリア内ルートの数です。
Inter	IPルーティングテーブルに新しく設置されたエリア間ルートの数です。
External	IPルーティングテーブルに新しくインストールされた外部ルートの数です。
Reason	ルート計算が実行される理由です。 ● **Intra-area LSA**–領域内LSAの変更です。 ● **Inter-area LSA**–エリア間LSAの変更です。 ● **External LSA**–外部LSAの変更です。 ● **Configuration**–コンフィギュレーションの変更です。 ● **Area 0 full neighbor**–Area0でFULL状態になっている隣接ルータの数が変化します。 ● **Area 0 up interface**–Area0でup状態のインタフェースの数が変化します。 ● **LSDB overflow state**–オーバーフロー状態の変更です。 ● **ABR summarization**–ABR要約の変更です。 ● **GR end**–GRの終了です。 ● **Routing policy**–ルーティングポリシーの変更です。 ● **Intra-area tunnel**–エリア内トンネルの変更です。 ● **Others**–その他の理由です。

OSPF プロセス 1 の OSPF 隣接ログ情報を表示します。

<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
```

表 5-8 コマンド出力

フィールド	説明
Date/Time	隣接状態が変わる時刻です。
Local Address	隣接関係のローカルアドレスです。
Remote Address	隣接関係のピアアドレスです。
Router ID	隣接ルータIDです。

フィールド	説明
	隣接状態が変更された理由です。 ● **ResetConnect**–メモリ不足のため接続が失われました。 ● **IntChange**–インタフェースパラメータが変更されました。 ● **VlinkChange**–仮想リンクパラメータが変更されました。 ● **ResetOspf**–OSPFプロセスがリセットされます。 ● **UndoOspf**–OSPFプロセスが削除されます。 ● **UndoArea**–OSPFエリアが削除されます。 ● **UndoNetwork**–インタフェースが無効になっています。 ● **SilentInt**–インタフェースは、サイレントインタフェースとして設定されています。 ● **IntLogChange**–インタフェースの論理属性が変更されました。 ● **IntPhyChange**–インタフェースの物理属性が変更されました。 ● **IntVliChange**–インタフェースの仮想リンク属性が変更されました。 ● **VlinkDown**–仮想リンクが停止します。 ● **DeadExpired**–deadタイマの有効期限が切れます。 ● **ConfStubArea**–インタフェースはスタブエリアパラメータで設定されます。 ● **ConfNssaArea**–インタフェースにはNSSAエリアパラメータが設定されています。 ● **AuthChange**–認証タイプが変更されました。 ● **OpaqueChange**–Opaque機能が変更されました。 ● **Retrans**–過剰な再送信です。 ● **LLSChange**–LLS機能が変更されました。 ● **OOBChange**–OOB機能が変更されました。 ● **GRChange**–GR機能が変更されました。 ● **BFDDown**–インタフェースはBFDによってシャットダウンされます。 ● **BadLSReq**–インタフェースはBadLSReqイベントを受信します。 ● **SeqMismatch**–インタフェースはSeqNumberMismatchイベントを受け取ります。

フィールド	説明
	• **1-Way**–インタフェースは1-Wayイベントを受け取ります。 • **LocalNoLSA**–要求されたLSAは存在しません。 • **SameLSAReq**–受信したLSAはローカル要求キューにあります。 • **OldLSAReq**–受信したLSAのエージングタイムが、ローカル要求キュー内の要求されたLSAのエージングタイムより長いです。 • **DdTimerOut**–helloタイマの期限が切れた後でDDパケットを受信します。 • **EAChange**–外部属性ビットが変更されました。 • **RecvNoDupPkt**–重複していないDDパケットをロード状態またはフル状態で受信します。 • **EbitChange**–Eビットが変更されました。 • **MSbitChange**–MSビットが変更されました。 • **IbitChange**–Iビットが変更されました。 • **MSeqNumError**–プライマリルータがセカンダリルータから予期しないシリアル番号を受信しました。 • **SSeqNumError**–セカンダリルータがプライマリルータから予期しないシリアル番号を受信しました。 • **RecvOpqIntf**–タイプ9のLSAを含むDDパケットは、opaque LSA受信および通知機能が無効になっている場合に受信されます。 • **RecvOpqArea**–タイプ10のLSAを含むDDパケットは、opaque LSA受信および配信機能が無効になっている場合に受信されます。 • **RecvOpqAs**–タイプ11LSAを含むDDパケットは、opaque LSA受信およびメッセージ機能が無効になっている場合に受信されます。 • **RecvNSSA**–タイプ7LSAを含むDDパケットが、非NSSAエリアで受信されます。 • **InvalidLSA**–無効なLSAを含むDDパケットを受信します。 • **RecvASE**–タイプ5LSAを含むDDパケットが、仮想リンクまたはスタブエリアで受信されます。

関連コマンド

reset ospf event-log

5.1.15 display ospf graceful-restart

Syntax

display ospf [*process-id*] **graceful-restart** [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

process-id: OSPF プロセスを指定します。設定範囲は 1～65535 です。指定しない場合、すべての OSPF プロセスの GR 情報を表示します。

verbose: GR の詳細情報を表示します。指定しない場合、GR の概要情報を表示します。

説明

display ospf graceful-restart コマンドは GR 情報を表示します。

例

GR の詳細情報を表示します。

<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
```

表 5-9 コマンド出力

フィールド	説明
OSPF Process 1 with Router ID 1.1.1.1 Graceful Restart information	ルータIDが1.1.1.1、OSPFプロセス1のGR情報です。
Graceful Restart capability	GRが有効かどうかを示します。 ● **Enable(IETF)**–IETF準拠のGR が有効です。 ● **Enable(Nonstandard)**– 非IETF準拠のGR が有効です。 ● **Disable**–GRが無効です。
Graceful Restart support	プロセスがサポートしているGRモードです（GRが有効である場合のみ表示されます）。 ● **Planned and un-planned**–planned GR、unplanned GRの両方をサポートします。 ● **Planned only**–planned GRをサポートします。 ● **Partial**– partial GRをサポートします。 ● **Global**–すべてのGRをサポートします。

フィールド	説明
Helper capability	プロセスがサポートするヘルパーです。 ● **Enable (IETF)**–IETF準拠のGRヘルパーをサポートします。 ● **Enable (Nonstandard)**–非IETF準拠のGRヘルパーをサポートします。 ● **Enable (IETF and nonstandard)**– IETF準拠と非IETF準拠のGRヘルパーの両方をサポートします。 ● **Disable**–GRヘルパーをサポートしません。
Helper support	ヘルパーがサポートするポリシーです（GRヘルパーが有効である場合のみ表示されます）。 ● **Strict lsa check**–ヘルパーはstrict LSA確認をサポートします。 ● **Planned and un-planned**–ヘルパーはplanned GRとunplanned GRの両方をサポートします。 ● **Planned only**–planned GRのみサポートします。
Current GR state	GRの状態です。 ● **Normal**–GRが処理中でない、あるいは完了しました。 ● **Under GR**–GRが処理中です。 ● **Under Helper**–プロセスがGRヘルパーとして動作しています。
Last exit reason	最新の終了した理由です。 ● **Restarter**–リスタータがもっとも最後に終了した理由です。 ● **Helper**–ヘルパーがもっとも最後に終了した理由です。
Area	IPアドレス形式のエリアIDです。
Authtype	エリアの認証タイプです。 ● **None**－認証を行いません。 ● **Simple**－Simple認証です。 ● **MD5**－MD5認証です。
Area flag	エリアのタイプです。 ● **Normal**－通常エリアです。 ● **Stub**－スタブエリアです。 ● **StubNoSummary (totally stub area)**－StubNoSummaryエリアです。 ● **NSSA**－NSSAエリアです。 ● **NSSANoSummary (totally NSSA area)**－NSSANoSummaryエリアです。

フィールド	説明
Area up Interface count	エリアのup状態のインタフェース数です。
Interface	エリアのインタフェースです。
Restarter state	インタフェースのリスタートの状態です。
State	インタフェースの状態です。
Type	インタフェースのネットワークタイプです。
Neighbor count of this interface	インタフェースの隣接です。
Neighbor	隣接のルータIDです。
IP address	隣接のIPアドレスです。
GR state	隣接のGR状態です。 ● **Normal**–GRが処理中でない、あるいは完了しました。 ● **Under GR**–GRが処理中です。 ● **Under Helper**–プロセスがGRヘルパーとして動作しています。
Last Helper exit reason	ヘルパーがもっとも最後に終了した理由です。
Virtual-link Neighbor-ID	仮想リンクの隣接のルータIDです。
Neighbor-State	隣接状態です。Down、Init、2-Way、ExStart、Exchange、Loading、Fullがあります。
Interface	仮想リンクの出力インタフェースです。

5.1.16 display ospf interface

Syntax

display ospf [*process-id*] **interface** [*interface-type interface-number* | **verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

process-id: OSPF プロセスを指定します。設定範囲は 1～65535 です。指定しない場合、すべての OSPF プロセスの OSPF インタフェースの情報を表示します。

interface-type interface-number: インタフェースのタイプと番号を指定します。

verbose: すべてのインタフェースの OSPF の詳細情報を表示します。

説明

display ospf interface コマンドは OSPF インタフェースの情報を表示します。

interface-type interface-number あるいは **verbose** パラメータを指定しない場合、すべての OSPF インタフェースの情報を表示します。

例

すべての OSPF インタフェースの情報を表示します。

<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
```

表 5-10 コマンド出力

フィールド	説明
Area	インタフェースのエリアIDです。
IP address	インタフェースのIPアドレスです（TEが有効/無効にかかわらず表示します）
Type	インタフェースのネットワークタイプです。PTP (P2P)、PTMP (P2MP)、Broadcast、 NBMAがあります。

フィールド	説明
State	インタフェースの状態です。 ● **DOWN**–インタフェース上で送受信できるプロトコルトラフィックはありません。 ● **Loopback**–インタフェースがloopback状態です。トラフィックを転送することができません。 ● **Waiting**–インタフェースはHello パケットの送受信を開始します。ルータはネットワークの代表ルータ/バックアップ代表ルータを決定します。 ● **P-2-P**–インタフェースは、Hello Interval の間隔でHelloパケットを送信し、隣接との隣接関係を確立しようと試みます。 ● **DR**–ルータ自身が接続されたネットワークのDRルータになります。 ● **BDR**–ルータ自身が接続されたネットワークのバックアップDRルータになります。 ● **DROther**–DR otherルータがネットワーク上にいます。
Cost	インタフェースのコストです。
Pri	ルータの優先順位です。
DR	インタフェースのネットワークセグメントのDRです。
BDR	インタフェースのネットワークセグメントのバックアップDRです。

VLAN インタフェース 1 の詳細情報を表示します。

<Switch> display ospf interface Vlan-interface 1

```
        OSPF Process 1 with Router ID 192.168.1.1
               Interfaces


Interface: 172.16.0.1 (Vlan-interface1)
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
```

```
Enabled by interface configuration (including secondary IP addresses)
MD5 authentication enabled.
   The last key is 3.
   The rollover is in progress, 2 neighbor(s) left.
```

表 5-11 コマンド出力

フィールド	説明
Interface	IPアドレスのようなインタフェースの情報です。
Timers	OSPFタイマです。hello、dead、poll、retransmit、transmit delay があります。
FRR backup	インタフェースでLFAの計算が有効かどうかを示します。
Enabled by interface configuration (including secondary IP addresses)	インタフェースでOSPFが有効です（セカンダリIPアドレスを含みます）。
MD5 authentication enabled	認証モードです。
The last key	最新のMD5認証キーIDです。
neighbor(s)	キーの交換が完了していない隣接の数です。

5.1.17 display ospf lsdb

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**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

process-id: OSPF プロセスを指定します。設定範囲は 1～65535 です。指定しない場合、すべての OSPF プロセスの LSDB の情報を表示します。

area *area-id*: OSPF エリアを IP アドレスあるいは 10 進数の整数のエリア ID で指定します。10 進数の整数の設定範囲は 0～4294967295 です。この 10 進数の整数はシステムで IP アドレスの形式に変換されます。指定しない場合、すべての OSPF エリアの LSDB の情報を表示します。

brief: LSDB の概要情報を表示します。

asbr: LSDB の Type-4 LSA（ASBR 集約 LSA）の情報を表示します。

ase: LSDB の Type-5 LSA（AS 外部 LSA）の情報を表示します。

network: LSDB の Type-2 LSA（ネットワーク LSA）の情報を表示します。

nssa: LSDB の Type-7 LSA（NSSA 外部 LSA）の情報を表示します。

opaque-area: LSDB の Type-10 LSA（Opaque エリア LSA）の情報を表示します。

opaque-as: LSDB の Type-11 LSA（Opaque AS LSA）の情報を表示します。

opaque-link: LSDB の Type-9 LSA（Opaque リンク LSA）の情報を表示します。

router: LSDB の Type-1 LSA（ルータ LSA）の情報を表示します。

summary: LSDB の Type-3 LSA（ネットワーク集約 LSA）の情報を表示します。

link-state-id: IP アドレス形式のリンクステート ID を指定します。

originate-router *advertising-router-id*: 配信ルータの ID を指定します。

self-originate: ここで作成された LSA の情報を表示します。

standby slot *slot-number*: IRF スタックメンバ装置のバックアップ OSPF LSDB の情報を表示します。指定しない場合、OSPF LSDB 情報を表示します。

例

OSPF の LSDB の情報を表示します。

<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
```

表 5-12 コマンド出力

フィールド	説明
Area	エリアのLSDBの情報です。
Type	LSAタイプです。
LinkState ID	リンクステートのIDです。
Adv Router	配信ルータです。
Age	LSAのエージング時間です。
Len	LSAの長さです。
Sequence	LSAのシーケンス番号です。
Metric	LSAのコストです。
*Opq-Link	仮想リンクによって作成されたOpaque LSAです。

LSDB の Type-2 LSA（ネットワーク LSA）の情報を表示します。

<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
```

表 5-13 コマンド出力

フィールド	説明
Type	LSAタイプです。
LS ID	DRのIPアドレスです。
Adv Rtr	LSAに配信されたルータです。
LS age	LSAのエージング時間です。
Len	LSAの長さです。
Options	LSAのオプションです。 ● **O**—Opaque LSAを配信できます。 ● **E**—AS 外部LSAを受信できます。 ● **EA**—外部拡張LSAを受信できます。 ● **DC**—オンデマンドリンクをサポートします。 ● **N**—NSSA拡張LSAをサポートします。 ● **P**—Type-7 LSAをType-5 LSAに変換するNSSAのABRです。
Seq#	LSAのシーケンス番号です。
Checksum	LSAタイプです。

フィールド	説明
Net mask	DRのIPアドレスです。
Attached router	LSAに配信されたルータです。

5.1.18 display ospf nexthop

Syntax

display ospf [*process-id*] **nexthop**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

process-id: OSPF プロセスを指定します。設定範囲は 1～65535 です。指定しない場合、すべての OSPF プロセスのネクストホップの情報を表示します。

説明

display ospf nexthop コマンドは OSPF のネクストホップの情報を表示します。

例

OSPF のネクストホップの情報を表示します。

<Switch> display ospf nexthop

```
        OSPF Process 1 with Router ID 1.1.1.2
               Neighbor Nexthop Information

 NbrID          Nexthop        Interface             RefCount   Status
 1.1.1.2        4.4.4.4        Loop1                 1          Valid
 1.1.1.1        1.1.1.1        Vlan2                 3          Valid
 1.1.1.2        1.1.1.2        Vlan2                 4          Valid
```

表 5-14 コマンド出力

フィールド	説明
Nbrld	隣接ルータIDです。

フィールド	説明
Nexthop	ネクストホップアドレスです。
Interface	出力インタフェースです。
RefCount	参照回数です（ネクストホップを参照するルートです）。
Status	ネクストホップの状態です。有効、無効があります。

5.1.19 display ospf non-stop-routing status

Syntax

display ospf [*process-id*] **non-stop-routing status**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

process-id: OSPF プロセスを指定します。設定範囲は 1～65535 です。指定しない場合、すべての OSPF プロセスの OSPF NSR 情報を表示します。

説明

display ospf non-stop-routing status コマンドは、OSPF NSR 情報を表示します。

例

OSPF NSR 情報を表示します。

<Switch> display ospf non-stop-routing status

```
OSPF Process 1 with Router ID 192.168.33.12
Non Stop Routing information

Non Stop Routing capability : Enabled
Upgrade phase : Normal
```

表 5-15 コマンド出力

フィールド	説明
Non Stop Routing capability	NSRステータス: 有効または無効です。
Upgrade phase	アップグレードフェーズです。: ● **Prepare**–アップグレード準備フェーズです。 ● **Restore Smooth**–アップグレードフェーズです。 ● **Preroute**–ルート事前計算フェーズです。 ● **Calculating**–ルート計算フェーズです。 ● **Redisting**–ルート再配分フェーズです。 ● **Original and age**–:LSAの生成と経過時間のフェーズです。 ● **Normal**–標準ステータスです。

5.1.20 display ospf peer

Syntax

display ospf [*process-id*] **peer** [**verbose**] [*interface-type interface-number*] [*neighbor-id*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

process-id: OSPF プロセスを指定します。設定範囲は 1～65535 です。指定しない場合、すべての OSPF プロセスの OSPF の隣接情報を表示します。

verbose: 詳細な隣接情報を表示します。指定しない場合、OSPF の隣接情報の概要を表示します。

interface-type interface-number: インタフェースのタイプと番号を指定します。指定しない場合、すべてのインタフェースの OSPF の隣接情報を表示します。

neighbor-id: 隣接ルータの ID を指定します。指定しない場合、すべての隣接情報を表示します。

説明

display ospf peer コマンドは OSPF の隣接情報を表示します。

例

OSPF の詳細な隣接情報を表示します。

<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-interface1)'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

Sham link 11.11.11.11 -> 22.22.22.22's neighbor in area 0.0.0.1
Router ID: 22.22.22.22     Address: 22.22.22.22
  State: Full  Mode: Nbr is master  Priority: 1
  BFD status: Disabled
```

表 5-16 コマンド出力

フィールド	説明
Area *areaID* interface *IPAddress*(*InterfaceName*)'s neighbors	指定エリアのインタフェースの隣接情報です。 ● **areaID**–隣接が所属しているエリアです。 ● **IPAddress**–インタフェースのIPアドレスです。 ● **InterfaceName**–インタフェース名です。
Router ID	隣接ルータのIDです。
Address	隣接ルータのアドレスです。
GR State	GRの状態です。 ● **Normal**–正常です。 ● **Restarter**ーリスタータです。 ● **Complete**ー完了しました。 ● **Helper**ーヘルパーです。

フィールド	説明
State	隣接状態です。 ● **Down**–隣接との通信の初期状態です。 ● **Init**–ルータは隣接からHelloパケットを受信しましたが、ルータは隣接と双方向の通信を確立していません。ルータは隣接のHelloパケットを表示しません。 ● **Attempt**–NBMAネットワークでのみ有効です。この状態ではOSPFルータは一定の期間、隣接から情報を受信しません。ルータは隣接との関係を保持するためにhelloパケットを長い間隔で送信することができます。 ● **2-Way**–2つのルータ間の通信は双方向です。ローカルルータは隣接のHelloパケットに表示します。 ● **Exstart**–ルータがマスタで、初期のDD（Database Description）シーケンス番号を決定します。 ● **Exchange**–ルータは全体のリンクステートデータベースを記載したDDパケットを隣接に送信しています。 ● **Loading**–ルータは隣接に、最新のLSAを要求するLSAパケットを送信します。 ● **Full**–隣接ルータが完全に隣接関係となります。
Mode	LSDBの同期を行うための隣接モードです。
Priority	隣接ルータの優先順位です。
DR	インタフェースのネットワークセグメントのDRです。
BDR	インタフェースのネットワークセグメントのBDRです。
MTU	インタフェースのMTUです。
Options	LSAオプションです。 ● **O**–Opaque LSAを配信できます。 ● **E**–AS外部LSA を受信できます。 ● **EA**–外部拡張LSAを受信できます。 ● **DC**–オンデマンドリンクをサポートします。 ● **N**–NSSA拡張LSAをサポートします。 ● **P**–Type-7 LSAをType-5 LSAに変換するNSSAのABRです。
Dead timer due in 33 sec	deadタイマが33秒後に終了します。
Neighbor is up for 02:03:35	隣接が02:03:35の間、up状態です。
Authentication Sequence	認証シーケンス番号です。

フィールド	説明
Neighbor state change count	隣接状態を変更した回数です。
Sham link 11.11.11.11 -> 22.22.22.22's neighbor in area 0.0.0.1	エリア1のshamリンク（11.11.11.11から22.22.22.22）の隣接です。
BFD status	BFDの状態です。 ● **Disabled**－無効です。 ● **Enabled (Control mode)**－有効です（コントロールモード）。 ● **Enabled (Echo mode)**－有効です（エコーモード）。

OSPF の隣接情報を表示します。

<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         Vlan1

Sham link: 11.11.11.11 -> 22.22.22.22
Router ID      Address        Pri Dead-Time  State
22.22.22.22    22.22.22.22    1   36         Full
```

表 5-17 コマンド出力

フィールド	説明
Area	隣接エリアです。
Router ID	隣接ルータのIDです。
Address	隣接インタフェースのアドレスです。
Pri	隣接ルータの優先順位です。
Dead-Time	deadタイマの残り時間です。
Interface	隣接に接続されたインタフェースです。
State	隣接状態です。 Down、Init、Attempt、2-Way、Exstart、Exchange、Loading、Full があります。

フィールド	説明
Sham link 11.11.11.11 -> 22.22.22.22	11.11.11.11から22.22.22.22へのshamリンクです。

5.1.21 display ospf peer statistics

Syntax

display ospf [*process-id*] **peer statistics**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

process-id: OSPF プロセスを指定します。設定範囲は 1～65535 です。指定しない場合、すべての OSPF プロセスの OSPF の隣接の統計情報を表示します。

説明

display ospf peer statistics コマンドは OSPF の隣接の統計情報を表示します。

例

OSPF の隣接の統計情報を表示します。

<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

 Sham links' neighbors (Total: 1):
   Down: 0, Init: 0, 2-Way: 0, ExStart: 0, Exchange: 0, Loading: 0, Full: 1
```

表 5-18 コマンド出力

フィールド	説明
Area ID	ルータが所属しているエリアのすべてのルータの状態の統計情報が表示されます。

フィールド	説明
Down	同一エリアのdown状態の隣接ルータの数です。
Attempt	同一エリアのAttempt状態の隣接ルータの数です。
Init	同一エリアのInit状態の隣接ルータの数です。
2-Way	同一エリアの2-Way状態の隣接ルータの数です。
ExStart	同一エリアのExStart状態の隣接ルータの数です。
Exchange	同一エリアのExchange状態の隣接ルータの数です。
Loading	同一エリアのLoading状態の隣接ルータの数です。
Full	同一エリアのFull状態の隣接ルータの数です。
Total	同一状態における隣接の総数です。Down、Attempt、Init、2-Way、ExStart、Exchange、Loading、Fullがあります。
Sham links' neighbors	shamリンクの隣接の統計情報です。

5.1.22 display ospf request-queue

Syntax

display ospf [*process-id*] **request-queue** [*interface-type interface-number*] [*neighbor-id*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

process-id: OSPF プロセスを指定します。設定範囲は 1～65535 です。指定しない場合、すべての OSPF プロセスの OSPF 要求キューの情報を表示します。

interface-type interface-number: インタフェースのタイプと番号を指定します。指定しない場合、すべてのインタフェースの OSPF 要求キューの情報を表示します。

neighbor-id: 隣接のルータの ID を指定します。指定しない場合、すべての OSPF の隣接の OSPF 要求キューの情報を表示します。

説明

display ospf request-queue コマンドは OSPF 要求キューの情報を表示します。

例

OSPF 要求キューの情報を表示します。

<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
```

表 5-19 コマンド出力

フィールド	説明
The Router's Neighbor is Router ID	隣接ルータのIDです。
Address	隣接インタフェースのIPアドレスです。
Interface	ローカルインタフェースのIPアドレスです。
Area	エリアIDです。
Request list	要求リスト情報です。
Type	LSAタイプです。
LinkState ID	リンクステートのIDです。
AdvRouter	配信するルータです。
Sequence	LSAシーケンス番号です。
Age	LSAのエージング時間です。

5.1.23 display ospf retrans-queue

Syntax

display ospf [*process-id*] **retrans-queue** [*interface-type interface-number*] [*neighbor-id*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

process-id: OSPF プロセスを指定します。設定範囲は 1～65535 です。指定しない場合、すべての OSPF プロセスの OSPF 再送キューの情報を表示します。

interface-type interface-number: インタフェースのタイプと番号を指定します。指定しない場合、すべてのインタフェースの OSPF 再送キューの情報を表示します。

neighbor-id: 隣接のルータの ID を指定します。指定しない場合、すべての OSPF の隣接の OSPF 再送キューの情報を表示します。

説明

display ospf retrans-queue コマンドは OSPF 再送キューの情報を表示します。

例

OSPF 再送キューの情報を表示します。

<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
```

表 5-20 コマンド出力

フィールド	説明
The Router's Neighbor is Router ID	隣接ルータのIDです。
Address	隣接インタフェースのIPアドレスです。
Interface	ルータのインタフェースのアドレスです。
Area	エリアIDです。
Retrans List	再送リストです。
Type	LSAタイプです。
LinkState ID	リンクステートのIDです。
Adv Router	配信するルータです。
Sequence	LSAシーケンス番号です。
Age	LSAエージング時間です。

5.1.24 display ospf routing

Syntax

display ospf [*process-id*] **routing** [*ip-address* { *mask-length* | *mask* }] [**interface** *interface-type interface-number*] [**nexthop** *nexthop-address*] [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

process-id: OSPF プロセスを指定します。設定範囲は 1～65535 です。指定しない場合、すべての OSPF プロセスのルーティング情報を表示します。

ip-address: 宛先 IP アドレスを指定します。

mask-length: マスク長を指定します。設定範囲は 0～32 です。

mask: ドットで区切られた 10 進数でマスクを指定します。

interface *interface-type interface-number*: 指定された出力インタフェースにパスするルートを表示します。指定しない場合、すべてのインタフェースのルーティング情報を表示します。

nexthop *nexthop-address*: 指定されたネクストホップにパスするルートを表示します。指定しない場合、すべてのルーティング情報を表示します。

verbose: OSPF の詳細なルーティング情報を表示します。指定しない場合、OSPF のルーティング情報の概要を表示します。

説明

display ospf routing コマンドは OSPF のルーティング情報を表示します。

OSPF プロセスを指定しない場合、すべての OSPF プロセスのルーティング情報を表示します。

インタフェースを指定しない場合、すべてのインタフェースのルーティング情報を表示します。

ネクストホップを指定しない場合、すべての OSPF のルーティング情報を表示します。

例

OSPF のルーティング情報を表示します。

<Switch> display ospf routing

```
        OSPF Process 1 with Router ID 192.168.1.2
               Routing Tables

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
```

表 5-21 コマンド出力

フィールド	説明
Destination	宛先ネットワークです。
Cost	宛先へのコストです。
Type	ルートタイプです。 intra-area、transit、stub、inter-area、Type-1 external、Type-2 external があります。
NextHop	ネクストホップアドレスです。

フィールド	説明
AdvRouter	配信するルータです。
Area	エリアIDです。
Total nets	ネットワークの総数です。
Intra area	エリア内ルートの総数です。
Inter area	エリア間ルートの総数です。
ASE	ASEルートの総数です。
NSSA	NSSAルートの総数です。

OSPF の詳細なルーティング情報を表示します。

<Switch> display ospf routing verbose

```
        OSPF Process 2 with Router ID 192.168.1.112
                Routing Tables

Routing for Network

Destination: 192.168.1.0/24
      Cost: 1562                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: Vlan10         BkInterface: N/A
      NibID: 0x0               Status: Local

Destination: 172.16.0.0/16
      Cost: 1563                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: Vlan20         BkInterface: N/A
      NibID: 0x0               Status: Local

Total Nets: 2
```

```
Intra Area: 2  Inter Area: 0  ASE: 0  NSSA: 0
```

表 5-22 コマンド出力

フィールド	説明
SubProtoID	サブプロトコルのIDです。
Preference	OSPFルートの優先順位です。
NbrId	隣接ルータのIDです。
NextHop	プライマリネクストホップのIPアドレスです。
BkNextHop	バックアップネクストホップのIPアドレスです。
IfType	プライマリネクストホップが所属しているネットワークのタイプです。
BkIfType	バックアップネクストホップが所属しているネットワークのタイプです。
Interface	出力インタフェースです。
BkInterface	バックアップ出力インタフェースです。
NibID	ネクストホップのIDです。
Status	ルートの状態です。 ● **Local**–ルートがローカルエンドです。ルートマネジメントモジュールにルートを送信しません。 ● **Invalid**–ネクストホップが無効です。 ● **Stale**–ネクストホップが古いです。 ● **Normal**–ルートが有効です。 ● **Delete**–ルートが削除されました。 ● **Host-Adv**–ルートがホストルートです。 ● **Rely**–ルートが再帰ルートです。

5.1.25 display ospf statistics

Syntax

display ospf [*process-id*] **statistics** [**error** | **packet** [*interface-type interface-number*]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

process-id: OSPF プロセスを指定します。設定範囲は 1～65535 です。指定しない場合、すべての OSPF プロセスの OSPF 統計情報を表示します。

error: エラー統計情報が表示されます。このキーワードを指定しない場合、コマンドは OSPF パケット、LSA、およびルート統計情報を表示します。

packet: OSPF パケットの統計情報を表示します。

interface-type interface-number: インタフェースをタイプと番号で指定します。指定しない場合、すべてのインタフェースの統計情報が表示されます。

説明

display ospf statistics コマンドは、OSPF 統計情報を表示します。

例

OSPF 統計情報を表示します。

<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
```

表 5-23 コマンド出力

フィールド	説明
I/O statistics	入出力パケットとLSAに関する統計情報です。
Type	OSPFパケットタイプです。
Input	受信したパケットです。
Output	送信されたパケットです。
Hello	Helloパケットです。
DB Description	データベース記述パケットです。
Link-State Req	リンク状態要求パケットです。
Link-State Update	リンクステート更新パケットです。
Link-State Ack	Link-State Acknowledgeパケットです。
LSAs originated by this router	このルータによって発信されたLSAです。
Router	発信されたType-1LSAの数です。
Network	発信されたType-2LSAの数です。
Sum-Net	発信されたType-3LSAの数です。
Sum-Asbr	発信されたType-4LSAの数です。
External	発信されたType-5LSAの数です。
NSSA	発信されたType-7LSAの数です。
Opq-Link	発信されたType-9LSAの数です。
Opq-Area	発信されたType-10LSAの数です。
Opq-As	発信されたType-11LSAの数です。
LSA originated	発信されたLSAの数です。

フィールド	説明
LSA received	受信したLSAの数です。
Routing table	ルーティングテーブル情報です。
Intra area	エリア内ルートの数です。
Inter area	エリア間ルートの数です。
ASE/NSSA	ASE/NSSAルートの数です。

5.1.26 display ospf vlink

Syntax

display ospf [*process-id*] **vlink**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

process-id: OSPF プロセスを指定します。設定範囲は 1～65535 です。指定しない場合、すべての OSPF プロセスの OSPF 仮想リンクの情報を表示します。

説明

display ospf vlink コマンドは OSPF 仮想リンクの情報を表示します。

例

OSPF 仮想リンクの情報を表示します。

<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-interface1)
 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.
```

表 5-24 コマンド出力

フィールド	説明
Virtual-link Neighbor-ID	仮想リンクの隣接のIDです。
Neighbor-State	隣接状態です。 Down、Init、2-Way、ExStart、Exchange、Loading、Fullがあります。
Interface	仮想リンクのローカルインタフェースのIPアドレスと名前です。
Cost	インタフェースのルートのコストです。
State	インタフェースの状態です。
Type	仮想リンクです。
Transit Area	通過するエリアIDです。
Timers	タイマの値です。hello、dead、retransmit、interface transmission delayがあります。
MD5 authentication enabled	認証モードです。
The last key	最新のMD5認証キーIDです。
neighbor(s)	キーの交換が完了していない隣接の数です。

5.1.27 display router id

Syntax

display router id

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display router id コマンドはグローバルルータの ID を表示します。

例

グローバルルータの ID を表示します。

<Switch> display router id

```
Configured router ID is 1.1.1.1
```

5.1.28 dscp

Syntax

dscp *dscp-value*

undo dscp

デフォルト

48

View

OSPF view

定義済みユーザロール

network-admin

パラメータ

dscp-value: 送信する OSPF パケットの DSCP を指定します。設定範囲は 0～63 です。

説明

dscp コマンドは送信する OSPF パケットの DSCP を設定します。

undo dscp コマンドはデフォルトに戻します。

例

OSPF プロセス 1 の送信する OSPF パケットの DSCP を 63 に設定します。

<Switch> system-view

[Switch] ospf 1

[Switch-ospf-1] dscp 63

5.1.29 enable link-local-signaling

Syntax

enable link-local-signaling

undo enable link-local-signaling

デフォルト

無効

View

OSPF view

定義済みユーザロール

network-admin

説明

enable link-local-signaling コマンドは OSPF リンクローカルシグナリング（LLS（link-local signaling)）を有効にします。

undo enable link-local-signaling コマンドは OSPF リンクローカルシグナリングを無効にします。

例

OSPF プロセス 1 のリンクローカルシグナリングを有効にします。

<Switch> system-view

[Switch] ospf 1

[Switch-ospf-1] enable link-local-signaling

5.1.30 enable out-of-band-resynchronization

Syntax

enable out-of-band-resynchronization

undo enable out-of-band-resynchronization

デフォルト

無効

View

OSPF view

定義済みユーザロール

network-admin

説明

enable out-of-band-resynchronization コマンドは OSPF の帯域外の再同期機能（OOB-Resynch（out-of-band resynchronization））を有効にします。

undo enable out-of-band-resynchronization コマンドは OSPF の帯域外の再同期機能を無効にします。

この設定を行う前に、リンクローカルシグナリングを有効にしてください。

例

OSPF プロセス 1 の OSPF の帯域外の再同期機能を有効にします。

<Switch> system-view

[Switch] ospf 1

[Switch-ospf-1] enable link-local-signaling

[Switch-ospf-1] enable out-of-band-resynchronization

関連コマンド

enable link-local-signaling

5.1.31 event-log

Syntax

event-log { **lsa-flush** | **peer** | **spf** } **size** *count*

undo event-log { **lsa-flush** | **peer** | **spf** } **size**

デフォルト

装置は、ルート計算ログ、LSA エージングログ、隣接ログなど、各タイプごとに最大 10 個のログを作成できます。

View

OSPF view

定義済みユーザロール

network-admin

パラメータ

lsa-flush: LSA エージングログの数を指定します。

peer: 隣接ログの数を指定します。

spf: ルート計算ログの数を指定します。

size *count*: OSPF ログの数を 0～65535 の範囲で指定します。

説明

event-log コマンドは、OSPF ログの数を設定します。

undo event-log コマンドは、設定を削除します。

例

OSPF プロセス 100 でルート計算ログの数を 50 に設定します。

<Switch> system-view

[Switch] ospf 100

[Switch-ospf-100] event-log spf size 50

5.1.32 fast-reroute (OSPF view)

Syntax

fast-reroute { **lfa** [**abr-only**] | **route-policy** *route-policy-name* }

undo fast-reroute

デフォルト

無効

View

OSPF view

定義済みユーザロール

network-admin

パラメータ

lfa: すべてのルートのバックアップネクストホップを計算するため LSA アルゴリズムを使用します。

abr-only: バックアップネクストホップとして ABR へのルートのネクストホップを使用します。

route-policy *route-policy-name*: バックアップネクストホップを決定するルーティングポリシーを使用します。設定範囲は 1～63 文字です。大文字、小文字を区別します。

説明

fast-reroute コマンドは OSPF FRR を設定します。

undo fast-reroute コマンドはデフォルトに戻します。

OSPF FRR と OSPF の BFD を同時に設定しないでください。同時に設定した場合、OSPF FRR は動作しません。

vlink-peer コマンドと一緒にコマンドを使用しないでください。

OSPF FRR と PIC が設定されている場合、OSPF FRR が優先されます。

例

OSPF プロセス 1 で、LSA アルゴリズムを使用して、すべてのルートのバックアップネクストホップを計算するように FRR を有効にします。

<Switch> system-view

[Switch] ospf 1

[Switch-ospf-1] fast-reroute lfa

5.1.33 filter (OSPF area view)

Syntax

filter { *acl-number* | **prefix-list** *prefix-list-name* | **route-policy** *route-policy-name* } { **export** | **import** }

undo filter { **export** | **import** }

デフォルト

設定なし

View

OSPF area view

定義済みユーザロール

network-admin

パラメータ

acl-number: 送信/受信 Type-3 LSA をフィルタするため ACL の番号を指定します。設定範囲は 2000～3999 です。

prefix-list-name: 送信/受信 Type-3 LSA をフィルタするため IP プレフィックスリストの名前を指定します。設定範囲は 1～63 文字です。大文字、小文字を区別します。

route-policy-name: 送信/受信 Type-3 LSA をフィルタするためルーティングポリシーの名前を指定します。設定範囲は 1～63 文字です。大文字、小文字を区別します。

export: ほかのエリアに配信する Type-3 LSA をフィルタします。

import: ローカルエリアに配信する Type-3 LSA をフィルタします。

説明

filter コマンドは ABR の送信/受信 Type-3 LSA をフィルタするため、OSPF を設定します。

undo filter コマンドは Type-3 LSA のフィルタリングを無効にします。

このコマンドは ABR でのみ有効です。

例

OSPF エリア 1 で、受信 Type-3 LSA をフィルタするため IP プレフィックスリスト my-prefix-list を設定し、送信 Type-3 LSA をフィルタするため ACL 2000 を設定します。

<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

5.1.34 filter-policy export (OSPF view)

Syntax

filter-policy { *acl-number* | **prefix-list** *prefix-list-name* } **export** [*protocol* [*process-id*]]

undo filter-policy export [*protocol* [*process-id*]]

デフォルト

設定なし

View

OSPF view

定義済みユーザロール

network-admin

パラメータ

acl-number: 再配信されるルートを宛先アドレスでフィルタするため ACL の番号を指定します。設定範囲は 2000～3999 です。

prefix-list-name: 再配信されるルートを宛先アドレスでフィルタするため IP プレフィックスリストの名前を指定します。設定範囲は 1～63 文字です。大文字、小文字を区別します。

protocol: 指定したルーティングプロトコルから再配信されるルートをフィルタします。ルーティングプロトコルは **ospf**、**rip**、**static** を指定できます。指定しない場合、すべての再配信されるルートをフィルタします。

process-id: プロセス ID を指定します。設定範囲は 1～65535 です。*process-id* は *protocol* パラメータが **rip**、**ospf** であるときのみ有効です。

説明

filter-policy export コマンドは再配信されるルートをフィルタするため OSPF を設定します。

undo filter-policy export コマンドは設定を削除します。

コマンドで拡張 ACL（ACL 番号が 3000～3999）を参照する場合、以下の方法の 1 つを使用して ACL を設定します。

- 指定した宛先でルートを拒否/許可する場合、**rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* コマンドを使用します。
- 指定した宛先とマスクでルートを拒否/許可する場合、**rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* **destination** *dest-addr dest-wildcard* コマンドを使用します。

source はルートの宛先アドレスを指定し、**destination** はルートのサブネットマスクを指定します。指定したサブネットマスクは連続している必要があります。連続していない場合、設定は適用しません。

例

再配信されるルートをフィルタするため ACL 2000 を設定します。

<Switch> system-view

[Switch] acl number 2000

[Switch-acl-basic-2000] rule deny source 192.168.10.0 0.0.0.255

[Switch-acl-basic-2000] quit

[Switch] ospf 100

[Switch-ospf-100] filter-policy 2000 export

ルート 113.0.0.0/16 のみ許可するように ACL 3000 を設定します。再配信されるルートをフィルタするため ACL 3000 を設定します。

<Switch> system-view

[Switch] acl number 3000

[Switch-acl-adv-3000] rule 10 permit ip source 113.0.0.0 0 destination 255.255.0.0 0

[Switch-acl-adv-3000] rule 100 deny ip

[Switch-acl-adv-3000] quit

[Switch] ospf 100

[Switch-ospf-100] filter-policy 3000 export

関連コマンド

import-route

5.1.35 filter-policy import (OSPF view)

Syntax

filter-policy { *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

デフォルト

設定なし

View

OSPF view

定義済みユーザロール

network-admin

パラメータ

acl-number: 受信したルートを宛先アドレスでフィルタするため ACL の番号を指定します。設定範囲は 2000～3999 です。

gateway *prefix-list-name*: ネクストホップで受信したルートをフィルタするため IP プレフィックスリストを指定します。設定範囲は 1～63 文字です。大文字、小文字を区別します。

prefix-list *prefix-list-name*: 受信したルートを宛先アドレスでフィルタするため IP プレフィックスリストの名前を指定します。設定範囲は 1～63 文字です。大文字、小文字を区別します。

route-policy *route-policy-name*: 受信したルートをフィルタするためルーティングポリシーを指定します。設定範囲は 1～63 文字です。大文字、小文字を区別します。

説明

filter-policy import コマンドは受信した LSA を使用して計算したルートをフィルタするため OSPF を設定します。

undo filter-policy import コマンドはデフォルトに戻します。

filter-policy import コマンドあるいは指定したルーティングポリシーで拡張 ACL（ACL 番号が 3000～3999）を参照する場合、以下の方法の 1 つを使用して ACL を設定します。

- 指定した宛先でルートを拒否/許可する場合、**rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* コマンドを使用します。

- 指定した宛先とマスクでルートを拒否/許可する場合、**rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* **destination** *dest-addr dest-wildcard* コマンドを使用します。

source はルートの宛先アドレスを指定し、**destination** はルートのサブネットマスクを指定します。指定したサブネットマスクは連続している必要があります。連続していない場合、設定は適用しません。

例

受信したルートをフィルタするため ACL 2000 を設定します。

<Switch> system-view

[Switch] acl number 2000

[Switch-acl-basic-2000] rule deny source 192.168.10.0 0.0.0.255

[Switch-acl-basic-2000] quit

[Switch] ospf 100

[Switch-ospf-100] filter-policy 2000 import

ルート 113.0.0.0/16 のみ許可するように ACL 3000 を設定します。受信されるルートをフィルタするため ACL 3000 を設定します。

<Switch> system-view

[Switch] acl number 3000

[Switch-acl-adv-3000] rule 10 permit ip source 113.0.0.0 0 destination 255.255.0.0 0

[Switch-acl-adv-3000] rule 100 deny ip

[Switch-acl-adv-3000] quit

[Switch] ospf 100

[Switch-ospf-100] filter-policy 3000 import

5.1.36 graceful-restart (OSPF view)

Syntax

graceful-restart [**ietf** | **nonstandard**] [**global** | **planned-only**] *

undo graceful-restart

デフォルト

無効

View

OSPF view

定義済みユーザロール

network-admin

パラメータ

ietf: IETF 準拠 GR を有効にします。

nonstandard: 非 IETF 準拠 GR を有効にします。

global: グローバルで GR を有効にします。すべての GR ヘルパーが存在するときのみ、GR プロセスを完了することができます。GR ヘルパーが故障した場合（たとえば、GR ヘルパーに接続したインタフェースがダウンしました）、GR プロセスは失敗します。**global** を指定しない場合、partial GR が有効です。partial GR モードでは GR ヘルパーが存在するとき、GR プロセスを完了することができます。

planned-only: planned GR のみ有効にします。指定しない場合、planned GR と unplanned GR の両方を有効にします。

説明

graceful-restart コマンドは OSPF GR を有効にします。

undo graceful-restart コマンドは OSPF GR を無効にします。

GR は planned GR と unplanned GR があります。

- **Planned GR**–手動で OSPF を再起動する、あるいはアクティブ/スタンドバイの切り替えを実行します。OSPF の再起動、あるいはアクティブ/スタンドバイの切り替えを行う前に、GR リスタータは grace LSA を GR ヘルパーに送信します。
- **Unplanned GR**–装置が故障したため、OSPF は、OSPF の再起動、あるいはアクティブ/スタンドバイの切り替えを行います。OSPF の再起動、あるいはアクティブ/スタンドバイの切り替えを行う前、GR リスタータは grace LSA を GR ヘルパーに送信しません。

IETF 準拠 GR を有効にする前に、**opaque-capability enable** コマンドで Opaque LSA の配信と受信を有効にしてください。

OSPF の非 IETF 準拠 GR を有効にする前に **enable link-local-signaling** コマンドで LLS を有効にし、**enable out-of-band-resynchronization** コマンドで OOB-Resynch を有効にしてください。

nonstandard パラメータ、あるいは **ietf** パラメータを指定しない場合、OSPF の非 IETF 準拠 GR を有効にします。

OSPF GR と OSPF NSR は相互に排他的です。**graceful-restart** コマンドと **non-stop-routing** コマンドは同時に設定しないでください。

例

OSPF プロセス 1 の IETF 準拠 GR を有効にします。

<Switch> system-view

[Switch] ospf 1

[Switch-ospf-1] opaque-capability enable

[Switch-ospf-1] graceful-restart ietf

OSPF プロセス 1 の非 IETF 準拠 GR を有効にします。

<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

関連コマンド

- **enable link-local-signaling**
- **enable out-of-band-resynchronization**
- **opaque-capability enable**

5.1.37 graceful-restart helper enable

Syntax

graceful-restart helper enable [**planned-only**]

undo graceful-restart helper enable

デフォルト

有効

View

OSPF view

定義済みユーザロール

network-admin

パラメータ

planned-only: GR ヘルパーの planned GR のみ有効にします。指定しない場合、planned GR と unplanned GR の両方を有効にします。

説明

graceful-restart helper enable コマンドは OSPF GR ヘルパーを有効にします。

undo graceful-restart helper enable コマンドは OSPF GR ヘルパーを無効にします。

planned-only パラメータは IETF 準拠 GR ヘルパーでのみ有効です。

例

OSPF プロセス 1 で OSPF GR ヘルパーを有効にします。

<Switch> system-view

[Switch] ospf 1

[Switch-ospf-1] graceful-restart helper enable

5.1.38 graceful-restart helper strict-lsa-checking

Syntax

graceful-restart helper strict-lsa-checking

undo graceful-restart helper strict-lsa-checking

デフォルト

無効

View

OSPF view

定義済みユーザロール

network-admin

説明

graceful-restart helper strict-lsa-checking コマンドは GR ヘルパーの strict LSA 確認を有効にします。

undo graceful-restart helper strict-lsa-checking コマンドは GR ヘルパーの strict LSA 確認を無効にします。

GR ヘルパーで LSA の変更が検出されたとき、GR ヘルパーは GR ヘルパーモードを終了します。

例

OSPF プロセス 1 の GR ヘルパーの strict LSA 確認を有効にします。

<Switch> system-view

[Switch] ospf 1

[Switch-ospf-1] graceful-restart helper strict-lsa-checking

5.1.39 graceful-restart interval (OSPF view)

Syntax

graceful-restart interval *interval-value*

undo graceful-restart interval

デフォルト

120 秒

View

OSPF view

定義済みユーザロール

network-admin

パラメータ

interval-value: GR 間隔を指定します。設定範囲は 40～1800 秒です。

説明

graceful-restart interval コマンドは GR 間隔を設定します。

undo graceful-restart interval コマンドはデフォルトに戻します。

GR を再起動する間隔の値は、すべての OSPF インタフェースの OSPF 隣接の dead タイマの最大値よりも小さくすることはできません。小さい場合、GR の再起動は失敗します。

例

OSPF プロセス 1 の GR 間隔を 100 秒に設定します。

<Switch> system-view

[Switch] ospf 1

[Switch-ospf-1] graceful-restart interval 100

関連コマンド

ospf timer dead

5.1.40 host-advertise

Syntax

host-advertise *ip-address cost*

undo host-advertise *ip-address*

デフォルト

設定なし

View

OSPF area view

定義済みユーザロール

network-admin

パラメータ

ip-address: ホストの IP アドレスを指定します。

cost: ルートのコストを指定します。設定範囲は 1～65535 です。

説明

host-advertise コマンドはホストルートを配信します。

undo host-advertise コマンドはホストルートを削除します。

例

コスト 100 のホストルート 1.1.1.1 を配信します。

<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

5.1.41 import-route (OSPF view)

Syntax

import-route *protocol* [*process-id* | **all-processes**] [**allow-direct** | **cost** *cost* | **nssa-only** | **route-policy** *route-policy-name* | **tag** *tag* | **type** *type*] *

undo import-route *protocol* [*process-id* | **all-processes**]

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**]

デフォルト

設定なし

View

OSPF view

定義済みユーザロール

network-admin

パラメータ

direct: direct ルートを再配信します。

ospf: OSPF ルートを再配信します。

rip: RIP ルートを再配信します。

static: static ルートを再配信します。

process-id: プロセスの ID を指定します。設定範囲は 1～65535 です。デフォルトは 1 です。*process-id* は *protocol* が **rip**、**ospf** であるときのみ有効です。

all-processes: 指定されたルーティングプロトコルのすべてのプロセスからルートを再配信します。**all-processes** は *protocol* が **rip**、**ospf** であるときのみ有効です。

allow-direct: 指定したルーティングプロトコルが有効なローカルインタフェースのネットワークを再配信します。指定しない場合、ローカルインタフェースのネットワークは再配信しません。**allow-direct** パラメータと **route-policy** *route-policy-name* パラメータの両方を指定した場合、ルーティングポリシーで定義した **if-match** のルールが **allow-direct** と競合していないことを確認してください。たとえば、**allow-direct** を指定した場合、ルーティングポリシーの **if-match route-type** のルールを設定しないでください。設定した場合、**allow-direct** パラメータは適用しません。

cost *cost*: ルートコストを指定します。設定範囲は 0～16777214 です。デフォルトは 1 です。

nssa-only: Type-7 LSA の P ビットを 0 に設定することで NSSA エリアへのルートの配信を制限します。指定しない場合、Type-7 LSA の P ビットは 1 となります。ルータが ASBR および ABR として動作し、バックボーンエリアに FULL 状態のネイバが存在する場合、ルータによって開始した Type-7 LSA の P ビットは 0 に設定されます。このパラメータは NSSA ルータに適用します。

route-policy *route-policy-name*: 再配信するルートをフィルタするためルーティングポリシーを指定します。設定範囲は 1～63 文字です。大文字、小文字を区別します。

tag *tag*: 外部 LSA を作成するタグを指定します。設定範囲は 0～4294967295 です。デフォルトは 1 です。

type *type*: コストタイプを指定します。デフォルトは 2 です。

説明

import-route コマンドは別のルーティングプロトコルから AS 外部ルートを再配信することを有効にします。

undo import-route コマンドは別のルーティングプロトコルから AS 外部ルートを再配信することを無効にします。

このコマンドは別のプロトコルからほかの AS へのルートを再配信します。AS 外部ルートは以下のタイプがあります。

- Type-1 外部ルート
- Type-2 外部ルート

Type-1 外部ルートは高い信頼性を持ちます。Type-1 外部ルートのコストは OSPF 内部ルートのコストと同等です。OSPF ルータから Type-1 外部ルータの宛先へのコストは、ルータから ASBR までのコストと ASBR から外部ルートの宛先までのコストを加えたものと等しくなります。

Type-1 外部ルートは低い信頼性を持ちます。OSPF では、ASBR から Type-2 外部ルートまでのコストは ASBR から OSPF 内部ルータまでのコストよりもはるかに大きいと認識します。このため、内部ルータから Type-2 の外部ルート宛先までのコストは、ASBR から Type-2 の外部ルートの宛先までのコストと等しくなります。

import-route コマンドはアクティブルートだけを再配信します。**display ip routing-table protocol** コマンドはアクティブルートに関する情報を表示します。**import-route** コマンドは、デフォルトの外部ルートを再配信することはできません。

import-route nssa-only コマンドは Type-7 LSA の AS 外部ルートを NSSA エリアにのみ再配信します。

undo-import-route { **ospf** | **rip** } **all-processes** コマンドは、**import-route** { **ospf** | **rip** } *process-id* コマンドで作成された設定ではなく、**import-route** { **ospf** | **rip** } **all-processes** コマンドで作成された設定のみを削除します。

例

RIP プロセス 40 からルートを再配信します。再配信するルートのタイプを 2、タグを 33、コストを 50 に設定します。

<Switch> system-view

[Switch] ospf 100

[Switch-ospf-100] import-route rip 40 type 2 tag 33 cost 50

関連コマンド

default-route-advertise (OSPF view)

5.1.42 log-peer-change

Syntax

log-peer-change

undo log-peer-change

デフォルト

有効

View

OSPF view

定義済みユーザロール

network-admin

説明

log-peer-change コマンドは OSPF 隣接状態の変更に伴うログの作成を有効にします。

undo log-peer-change コマンドは OSPF 隣接状態の変更に伴うログの作成を無効にします。

このコマンドは OSPF 隣接状態の変更のログを information center に送信します。

information center はユーザが定義した出力ルール（ログを出力するか、どこにログを出力するか）に従ってログを処理します。information center の詳細は、オペレーションマニュアルのセクション 11 *システム管理* "*Information Center*"を参照してください。

例

OSPF プロセス 100 の隣接状態の変更に伴うログの作成を無効にします。

<Switch> system-view

[Switch] ospf 100

[Switch-ospf-100] undo log-peer-change

5.1.43 lsa-arrival-interval

Syntax

lsa-arrival-interval *interval*

undo lsa-arrival-interval

デフォルト

1000 ミリ秒

View

OSPF view

定義済みユーザロール

network-admin

パラメータ

interval: LSA の到達間隔を指定します。設定範囲は 0～60000 ミリ秒です。

説明

lsa-arrival-interval コマンドは LSA の到達間隔を設定します。

undo lsa-arrival-interval コマンドはデフォルトに戻します。

OSPF が LSA 到達間隔以内に、先に受信した LSA と同一の、LSA タイプ、LS ID、ルータ ID の LSA を受信した場合、OSPF は LSA を廃棄します。この機能は頻繁なネットワークの変更によるリソースを節約します。

lsa-arrival-interval コマンドで設定した間隔は、**lsa-generation-interval** コマンドで設定した間隔と同じかそれより小さくしてください。

例

LSA の到達間隔を 200 ミリ秒に設定します。

<Switch> system-view

[Switch] ospf 100

[Switch-ospf-100] lsa-arrival-interval 200

関連コマンド

lsa-generation-interval

5.1.44 lsa-generation-interval

Syntax

lsa-generation-interval *maximum-interval* [*minimum-interval* [*incremental-interval*]]

undo lsa-generation-interval

デフォルト

最大間隔は 5 秒、最小間隔は 50 ミリ秒、増加する間隔は 200 ミリ秒です。

View

OSPF view

定義済みユーザロール

network-admin

パラメータ

maximum-interval: LSA の生成する最大間隔を指定します。設定範囲は 1～60 秒です。

minimum-interval: LSA の生成する最小間隔を指定します。設定範囲は 10～60000 ミリ秒です。

incremental-interval: LSA の生成する間隔が増加する間隔を指定します。設定範囲は 10～60000 ミリ秒です。

説明

lsa-generation-interval コマンドは OSPF LSA を生成する間隔を設定します。

undo lsa-generation-interval コマンドはデフォルトに戻します。

ネットワークが頻繁に変わらないとき、LSA は *minimum-interval* の間隔で生成されます。ネットワークの変更がしばしば起こると、計算の間隔は計算のたびに *incremental-interval* × 2^{n-2} ずつ増え、最後は *maximum-interval* になります。n は生成回数です。

最小間隔と増加する間隔は最大間隔よりも大きくすることができません。

例

LSA の生成する最大間隔を 2 秒、最小間隔を 100 ミリ秒、増加する間隔を 100 ミリ秒に設定します。

<Switch> system-view

[Switch] ospf 100

[Switch-ospf-100] lsa-generation-interval 2 100 100

関連コマンド

lsa-arrival-interval

5.1.45 lsdb-overflow-interval

Syntax

lsdb-overflow-interval *interval*

undo lsdb-overflow-interval

デフォルト

300 秒

View

OSPF view

定義済みユーザロール

network-admin

パラメータ

interval: OSPF がオーバーフロー状態から終了する期間を指定します。設定範囲は 0～2147483647 秒です。

説明

lsdb-overflow-interval コマンドは OSPF がオーバーフロー状態から終了する期間を設定します。

undo lsdb-overflow-interval コマンドはデフォルトに戻します。

LSDB の LSA 数が上限を超えたとき、LSDB はオーバーフロー状態となります。リソースを節約するため、オーバーフロー状態の際、OSPF は外部 LSA の受信を行わず、作成された外部 LSA を削除します。

コマンドで 0 秒に設定した場合、タイマは開始せず、OSPF はオーバーフロー状態から終了しません。

例

OSPF がオーバーフロー状態から終了する期間を 10 秒に設定します。

<Switch> system-view

[Switch] ospf 100

[Switch-ospf-100] lsdb-overflow-interval 10

5.1.46 lsdb-overflow-limit

Syntax

lsdb-overflow-limit *number*

undo lsdb-overflow-limit

デフォルト

制限なし

View

OSPF view

定義済みユーザロール

network-admin

パラメータ

number: LSDB 内の外部 LSA の上限を指定します。設定範囲は 1～1000000 です。

説明

lsdb-overflow-limit コマンドは LSDB 内の外部 LSA の上限を設定します。

undo lsdb-overflow-limit コマンドはデフォルトに戻します。

例

LSDB 内の外部 LSA の上限を 400000 に設定します。

<Switch> system-view

[Switch] ospf 100

[Switch-ospf-100] lsdb-overflow-limit 400000

5.1.47 maximum load-balancing (OSPF view)

Syntax

maximum load-balancing *maximum*

undo maximum load-balancing

View

OSPF view

定義済みユーザロール

network-admin

パラメータ

maximum: ECMP（equal-cost multi-path）ルートの最大数を指定します。1 に指定した場合、ECMP ルートの負荷分散は無効となります。

説明

maximum load-balancing コマンドはロードバランスを行うため ECMP（equal-cost multi-path）の最大数を指定します。

undo maximum load-balancing コマンドはデフォルトに戻します。

OSPF ECMP ルートの最大数のデフォルトはシステムでサポートする ECMP ルートの最大数と同じ、8 です。

例

負荷分散を行うため ECMP の最大数を 2 に設定します。

<Switch> system-view

[Switch] ospf 100

[Switch-ospf-100] maximum load-balancing 2

5.1.48 network (OSPF area view)

Syntax

network *ip-address wildcard-mask*

undo network *ip-address wildcard-mask*

デフォルト

無効

View

OSPF area view

定義済みユーザロール

network-admin

View

OSPF area view

パラメータ

ip-address: ネットワークの IP アドレスを指定します。

wildcard-mask: IP アドレスのワイルドカードマスクを指定します。たとえば、マスク 255.0.0.0 のワイルドカードマスクは 0.255.255.255 です。

説明

network コマンドはエリアの指定したネットワークに接続するインタフェースで OSPF を有効にします。

undo network コマンドはエリアの指定したネットワークに接続するインタフェースで OSPF を無効にします。

インタフェースのプライマリ IP アドレスは指定したネットワークに存在する必要があります。インタフェースのセカンダリ IP アドレスがネットワークにある場合、インタフェースは OSPF を動作させることができません。

例

エリア 2 の OSPF を動作させるため、プライマリ IP アドレスがネットワーク 131.108.20.0/24 にあるインタフェースを設定します。

<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

関連コマンド

ospf

5.1.49 non-stop-routing

Syntax

non-stop-routing

undo non-stop-routing

デフォルト

無効

View

OSPF view

定義済みユーザロール

network-admin

説明

non-stop-routing コマンドは、OSPF NSR を有効にします。

undo non-stop-routing コマンドは、OSPF NSR を無効にします。

non-stop-routing のコマンドは、現在のプロセスに対してのみ有効です。複数の OSPF プロセスが存在する場合は、各プロセスの OSPF NSR を有効にしてください。

OSPF NSR と OSPF GR は互いに排他的です。**non-stop-routing** コマンドと **graceful-restart** コマンドは同時に設定しないでください。

例

OSPF プロセス 100 の NSR を有効にします。

<Switch> system-view

[Switch] ospf 100

[Switch-ospf-100] non-stop-routing

5.1.50 nssa(OSPF area view)

Syntax

nssa [**default-route-advertise** [**cost** *cost-value* | **nssa-only** | **route-policy** *route-policy-name* | **type** *type*] * | **no-import-route** | **no-summary** | **suppress-fa** |

[[[**translate-always**] [**translate-ignore-checking-backbone**]] | **translate-never**] | **translator-stability-interval** *value*] *

undo nssa [**default-route-advertise** [**cost** | **nssa-only** | **route-policy** | **type**] * | **no-import-route** | **no-summary** | **suppress-fa** | [**translate-always** | **translate-never**] | **translator-stability-interval**] *

デフォルト

設定なし

View

OSPF area view

定義済みユーザロール

network-admin

パラメータ

default-route-advertise: NSSA ABR あるいは ASBR でのみ使用します。NSSA ABR で設定した場合、ABR はルーティングテーブルでデフォルトルートが有効かどうかにかかわらず、Type-7 LSA のデフォルトルートを NSSA エリアに作成します。ASBR で設定した場合、ASBR はルーティングテーブルのデフォルトルートが有効であるときのみ、Type-7 LSA のデフォルトルートを NSSA エリアに作成します。

cost *cost-value*:デフォルトルートのコストを 0~16777214 の範囲で指定します。このオプションを指定しない場合は、default-cost コマンドで指定した既定のコストが適用されます。

nssa-only: Type-7 LSA の P ビットを 0 に設定することで NSSA エリアにデフォルトルートの配信を制限します。デフォルトで Type-7 LSA の P ビットは 1 です。ルータが ASBR と ABR の両方で動作し、バックボーンエリアに FULL 状態のネイバが存在する場合、ルータが開始した Type-7 LSA の P ビットは 0 に設定します。

route-policy *route-policy-name*: 名前でルーティングポリシーを指定します。大文字と小文字を区別し、1~63 文字の文字列を指定します。 ルーティングテーブルにデフォルトルートが存在し、ルーティングポリシーが一致する場合、このコマンドは Type-7LSA 内のデフォルトルートを OSPF ルーティングドメインに再配信します。ルーティングポリシーは、Type-7 LSA の値を変更します。

type *type*: Type-7 LSA のタイプ (1 または 2) を指定します。このオプションを指定しない場合は、default type コマンドで指定したデフォルトのタイプが適用されます。

no-import-route: NSSA エリアにルートを再配信しないように、**import-route** コマンドを制御するため、NSSAABR で使用します。

no-summary: Type-3 集約 LSA のデフォルトルートを NSSA エリアに配信し、ほかの集約 LSA をエリアに配信しないようにするため、ABR でのみ使用します。エリアは完全 NSSA エリアです。

suppress-fa: Type-7 LSA のフォワーディングアドレスが Type-5 LSA に配置されないようにします。

translate-always: 常に Type-7 LSA を Type-5 LSA に変換します。NSSA ABR でのみ適用します。

translate-ignore-checking-backbone: NSSA エリアでのトランスレータの選択中に、backbone エリアで FULL 状態のネイバをチェックしません。

translate-never: Type-7 LSA を Type-5 LSA に変換しません。このキーワードは、NSSA ABR でのみ有効です。

translator-stability-interval *value*: トランスレータの安定間隔を指定します。装置が新しいトランスレータになったのち、間隔の間、トランスレータは変換能力を維持することができます。設定範囲は 0～900 秒です。デフォルトは 0 秒です。0 秒に設定すると、新しいトランスレータが作成されたとき、トランスレータは変換能力を維持しません。

説明

nssa コマンドは現在のエリアを NSSA エリアとして設定します。

undo nssa コマンドはデフォルトに戻します。

ABR に translate-ignore-checking-backbone キーワードを指定する場合は、NSSA 領域の他の ABR にもキーワードを指定する必要があります。 これにより、ABR の中から翻訳者を選ぶことができます。

例

エリア 1 を NSSA エリアとして設定します。

<Switch> system-view

[Switch] ospf 100

[Switch-ospf-100] area 1

[Switch-ospf-100-area-0.0.0.1] nssa

関連コマンド

default-cost (OSPF area view)

5.1.51 opaque-capability enable

Syntax

opaque-capability enable

undo opaque-capability

デフォルト

有効

View

OSPF view

定義済みユーザロール

network-admin

説明

opaque-capability enable コマンドは opaque LSA の配信、受信を有効にします。

undo opaque-capability コマンドは opaque LSA の配信、受信を無効にします。

opaque LSA の配信、受信を有効にしたのち、OSPF は Type-9、Type-10、Type-11 opaque LSA の配信、受信を行うことができます。

例

opaque LSA の配信、受信を無効にします。

<Switch> system-view

[Switch] ospf 100

[Switch-ospf-100] undo opaque-capability

5.1.52 ospf

Syntax

ospf [*process-id* | **router-id** *router-id* | **vpn-instance** *vpn-instance-name*] *

undo ospf [*process-id*]

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

パラメータ

process-id: OSPF プロセスを指定します。設定範囲は 1～65535 です。

router-id *router-id*: ドットで区切られた 10 進数で OSPF のルータ ID を指定します。

vpn-instance *vpn-instance-name*: VPN インスタンスを指定します。設定範囲は 1～31 文字です。大文字、小文字を区別します。指定しない場合、パブリックネットワークで OSPF プロセスが動作します。

説明

ospf コマンドは OSPF を有効にし、OSPF view に移行します。

undo ospf コマンドは OSPF を無効にします。

ルータで複数の OSPF プロセスを有効にすることができ、ルータの異なるルータ ID を指定することができます。

ほかの処理を実行する前に、OSPF プロセスを有効にしてください。

例

OSPF プロセス 100 を有効にし、ルータ ID を 10.10.10.1 に指定します。

<Switch> system-view

[Switch] ospf 100 router-id 10.10.10.1

[Switch-ospf-100]

5.1.53 ospf authentication-mode

Syntax

MD5/HMAC-MD5 認証：

ospf authentication-mode { **hmac-md5** | **md5** } *key-id* { **cipher** *cipher-string* | **plain** *plain-string* }

undo ospf authentication-mode { **hmac-md5** | **md5** } *key-id*

simple 認証：

ospf authentication-mode simple { **cipher** *cipher-string* | **plain** *plain-string* }

undo ospf authentication-mode simple

デフォルト

設定なし

View

Interface view

定義済みユーザロール

network-admin

パラメータ

hmac-md5: HMAC-MD5 認証を指定します。

md5: MD5 認証を指定します。

simple: simple 認証を指定します。

key-id: ID のキーを指定します。設定範囲は 1～255 です。

cipher: 暗号テキストのキーを指定します。

cipher-string: 暗号テキストのキーを指定します。大文字、小文字を区別します。**simple** が指定された場合、設定範囲は 33～41 文字です。**md5** あるいは **hmac-md5** が指定された場合、設定範囲は 33～53 文字です。

plain: プレーンテキストのキーを指定します。

plain-string: プレーンテキストのキーを指定します。大文字、小文字を区別します。**simple** が指定された場合、設定範囲は 1～8 文字です。**md5** あるいは **hmac-md5** が指定された場合、設定範囲は 1～16 文字です。

説明

ospf authentication-mode コマンドは認証モードを設定し、インタフェースにキーを設定します。

undo ospf authentication-mode コマンドは設定を削除します。

セキュリティのため、プレーンテキストで設定されたキーを含むすべてのキーは暗号テキストで保存されます。

同一ネットワークセグメントに接続されたインタフェースは同一のキーにする必要があります。OSPF インタフェースで MD5/HMAC-MD5 認証あるいは simple 認証のどちらかを指定することができます。MD5/HMAC-MD5 認証では、**ospf authentication-mode** コマンドを繰り返すことで複数のキーを設定することができます。各コマンドは固有のキーID とキーにする必要があります。

OSPF インタフェースのキーを指定する場合、以下のキーのロールオーバの処理を実行します。

1) インタフェースで MD5/HMAC-MD5 認証キーを設定します。隣接装置で新しいキーが設定されていない場合、MD5/HMAC-MD5 認証キーのロールオーバを開始します。キーのロールオーバを行っている間、OSPF はすべての隣接装置が認証にパスできるように新しい MD5/HMAC-MD5 認証キーと古い MD5/HMAC-MD5 認証キーの両方を含む複数のパケットを送信します。
2) すべての隣接装置で新しい MD5/HMAC-MD5 認証キーを設定します。ローカル装置がすべての隣接装置から新しいキーのパケットを受信すると、MD5 キーのロールオーバを終了します。
3) ローカル装置とすべての隣接装置から古い MD5/HMAC-MD5 認証キーを削除します。この処理を行うことで、通信を行うために古いキーを使用している装置が攻撃されることを防ぎ、キーの交換によって引き起こされるシステムリソース、帯域幅の消費を削減することができます。

例

VLAN インタフェース 10 で、MD5 認証を有効にし、インタフェースのキーID を 15、プレーンテキストキーを 123456 に設定します。

<Switch> system-view

[Switch] interface vlan-interface 10

[Switch-Vlan-interface10] ospf authentication-mode md5 15 plain 123456

VLAN インタフェース 10 で simple 認証を有効にし、プレーンテキストキーを 123456 に設定します。

<Switch> system-view

[Switch] interface vlan-interface 10

[Switch-Vlan-interface10] ospf authentication-mode simple plain 123456

関連コマンド

authentication-mode

5.1.54 ospf bfd enable

Syntax

ospf bfd enable [**echo**]

undo ospf bfd enable

デフォルト

無効

View

Interface view

定義済みユーザロール

network-admin

パラメータ

echo: BFD シングルホップエコー検知を有効にします。指定しない場合、双方向コントロール検知を有効にします。

説明

ospf bfd enable コマンドは OSPF インタフェースで BFD を有効にします。

undo ospf bfd enable コマンドは OSPF インタフェースで BFD を無効にします。

OSPF で OSPF FRR と BFD を同時に設定することはできません。設定した場合、OSPF FRR は適用しません。

例

VLAN インタフェース 11 で OSPF の BFD を有効にします。

<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

5.1.55 ospf cost

Syntax

ospf cost *value*

undo ospf cost

デフォルト

インタフェースの帯域幅に従い、OSPF のコストを計算します。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

value: OSPF のコストを指定します。loopback インタフェースの設定範囲は 0～65535 です。ほかのインタフェースの設定範囲は 1～65535 です。

説明

ospf cost コマンドはインタフェースの OSPF のコストを設定します。

undo ospf cost コマンドはデフォルトに戻します。

ospf cost コマンドはインタフェースの OSPF のコストを設定します。このコマンドを使用しない場合、インタフェースは自動で OSPF のコストを計算します。

例

VLAN インタフェース 10 の OSPF のコストを 65 に設定します。

<Switch> system-view

[Switch] interface vlan-interface 10

[Switch-Vlan-interface10] ospf cost 65

関連コマンド

bandwidth-reference

5.1.56 ospf dr-priority

Syntax

ospf dr-priority *priority*

undo ospf dr-priority

デフォルト

1

View

Interface view

定義済みユーザロール

network-admin

パラメータ

priority: インタフェースのルータの優先順位を指定します。設定範囲は 0～255 です。

説明

ospf dr-priority コマンドはインタフェースの DR/BDR の選出を行うため、ルータの優先順位を設定します。

undo ospf dr-priority コマンドはデフォルトに戻します。

値を大きくすると、DR/BDR を選出する優先順位は高くなります。装置の優先順位を 0 に設定した場合、DR あるいは BDR になりません。

例

VLAN インタフェース 10 のルータの優先順位を 8 に設定します。

<Switch> system-view

[Switch] interface vlan-interface 10

[Switch-Vlan-interface10] ospf dr-priority 8

5.1.57 ospf mib-binding

Syntax

ospf mib-binding *process-id*

undo ospf mib-binding

デフォルト

MIB はもっとも小さいプロセス ID の OSPF プロセスに結びつけられています。

View

System view

定義済みユーザロール

network-admin

パラメータ

process-id: OSPF プロセスを指定します。設定範囲は 1～65535 です。

説明

ospf mib-binding コマンドは OSPF プロセスを MIB に結びつけられています。

undo ospf mib-binding コマンドはデフォルトに戻します。

指定したプロセス ID が存在しない場合、MIB の結びつけの設定が失敗したことを通知するため、notification が表示されます。

MIB に結びつけられている OSPF プロセスを削除した場合、MIB から OSPF プロセスの結びつけを削除し、もっとも小さいプロセス ID の OSPF プロセスに MIB を再度、結びつけます。

例

OSPF プロセス 100 に MIB を結びつけます。

<Switch> system-view

[Switch] ospf mib-binding 100

5.1.58 ospf mtu-enable

Syntax

ospf mtu-enable

undo ospf mtu-enable

デフォルト

0

View

Interface view

定義済みユーザロール

network-admin

説明

ospf mtu-enable コマンドは DD パケットにインタフェース MTU を追加することをインタフェースで有効にします。

undo ospf mtu-enable コマンドはデフォルトに戻します。

仮想リンクがトンネルを通して確立したのち、異なるベンダからのリンクの 2 つの装置は異なる MTU の値を持つ可能性があります。この不一致を解消するため、インタフェースの MTU をデフォルトの値の 0 に戻します。

このコマンドを設定した後、インタフェースは受信した DD パケットの MTU が自身の MTU より大きいかどうかを確認します。大きい場合、インタフェースはパケットを廃棄します。

例

VLAN インタフェース 10 を有効にし、インタフェース MTU の値を DD パケットに追加します。

<Switch> system-view

[Switch] interface vlan-interface 10

[Switch-Vlan-interface10] ospf mtu-enable

5.1.59 ospf network-type

Syntax

ospf network-type { **broadcast** | **nbma** | **p2mp** [**unicast**] | **p2p** }

undo ospf network-type

デフォルト

デフォルトでインタフェースのネットワークタイプは、リンクレイヤプロトコルに依存します。

- Ethernet、FDDI のネットワークタイプは broadcast です。
- ATM、FR、X.25 のネットワークタイプは NBMA です。
- PPP、LAPB、HDLC、POS のネットワークタイプは P2P です。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

broadcast: ネットワークタイプを broadcast に指定します。

nbma: ネットワークタイプを NBMA に指定します。

p2mp: ネットワークタイプを P2MP に指定します。

unicast: OSPF パケットをユニキャストするため、P2MP インタフェースを指定します。デフォルトで P2MP インタフェースは OSPF パケットをマルチキャストします。

p2p: ネットワークタイプを P2P に指定します。

説明

ospf network-type コマンドはインタフェースのネットワークタイプを設定します。

undo ospf network-type コマンドはインタフェースのネットワークタイプをデフォルトに戻します。

ブロードキャストネットワークのルータがマルチキャストをサポートしない場合、インタフェースに接続するネットワークタイプは NBMA に設定します。

NBMA ネットワークの 2 つのルータが仮想リンクを通して直接接続している場合、ネットワークはフルメッシュ構成となります。インタフェースに接続するネットワークタイプを NBMA に設定することができます。2 つのルータが直接接続されていない場合、2 つのルータが別のルータを通してルーティング情報を交換できるように P2MP ネットワークタイプを設定します。

インタフェースのネットワークタイプが NBMA あるいは P2MP ユニキャストであるとき、隣接を指定するため、**peer** コマンドを使用する必要があります。

ネットワークで 2 つのルータのみが OSPF を動作している場合、インタフェースに接続するネットワークタイプを P2P に設定することができます。

インタフェースのネットワークタイプが P2MP ユニキャストである場合、すべての OSPF パケットはインタフェースでユニキャストされます。

例

VLAN インタフェース 10 の OSPF ネットワークタイプを NBMA に設定します。

```
<Switch> system-view
[Switch] interface vlan-interface 10
[Switch-Vlan-interface10] ospf network-type nbma
```

関連コマンド

ospf dr-priority

5.1.60 ospf timer dead

Syntax

ospf timer dead *seconds*

undo ospf timer dead

デフォルト

ブロードキャスト、P2P インタフェースのデフォルト値は 40 秒です。P2MP および NBMA インタフェースのデフォルト値は 120 秒です。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

seconds: dead タイマを指定します。設定範囲は 1～2147483647 秒です。

説明

ospf timer dead コマンドは隣接の dead タイマを設定します。

undo ospf timer dead コマンドはデフォルトに戻します。

インタフェースが隣接から Hello パケットを dead タイマ以内に受信しない場合、インタフェースは隣接がダウンしたと認識します。

インタフェースの dead タイマは少なくとも hello タイマの 4 倍以上にする必要があります。同一セグメントに接続されているルータは同一の dead タイマにする必要があります。

例

VLAN インタフェース 10 の dead タイマを 60 秒に設定します。

<Switch> system-view

[Switch] interface vlan-interface 10

[Switch-Vlan-interface10] ospf timer dead 60

関連コマンド

ospf timer hello

5.1.61 ospf timer hello

Syntax

ospf timer hello *seconds*

undo ospf timer hello

デフォルト

ブロードキャスト、P2P インタフェースのデフォルト値は 10 秒です。P2MP および NBMA インタフェースのデフォルト値は 30 秒です。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

seconds: Hello タイマを指定します。設定範囲は 1～65535 秒です。

説明

ospf timer hello コマンドはインタフェースの Hello タイマを設定します。

undo ospf timer hello コマンドはデフォルトに戻します。

Hello タイマを小さくするとトポロジの収束は早くなりますが、多くのリソースが消費されます。2 つの隣接するインタフェースの Hello タイマは同一にしてください。

例

VLAN インタフェースの Hello タイマを 20 秒に設定します。

<Switch> system-view

[Switch] interface vlan-interface 10

[Switch-Vlan-interface10] ospf timer hello 20

関連コマンド

ospf timer dead

5.1.62 ospf timer poll

Syntax

ospf timer poll *seconds*

undo ospf timer poll

デフォルト

120 秒

View

Interface view

定義済みユーザロール

network-admin

パラメータ

seconds: poll タイマを指定します。設定範囲は 1～2147483647 秒です。

説明

ospf timer poll コマンドは NBMA インタフェースの poll タイマを設定します。

undo ospf timer poll コマンドはデフォルトに戻します。

NBMA インタフェースで隣接がダウンしたことを検出するとき、poll タイマの間隔で Hello パケットを送信します。

poll タイマは少なくとも hello タイマの 4 倍以上にする必要があります。

例

VLAN インタフェース 10 の poll タイマを 130 秒に設定します。

<Switch> system-view

[Switch] interface vlan-interface 10

[Switch-Vlan-interface10] ospf timer poll 130

関連コマンド

ospf timer hello

5.1.63 ospf timer retransmit

Syntax

ospf timer retransmit *interval*

undo ospf timer retransmit

デフォルト

5 秒

View

Interface view

定義済みユーザロール

network-admin

パラメータ

interval: LSA の再送間隔を指定します。設定範囲は 1～3600 秒です。

説明

ospf timer retransmit コマンドはインタフェースで LSA を再送する間隔を設定します。

undo ospf timer retransmit コマンドはデフォルトに戻します。

LSA を送信したのち、インタフェースは acknowledgment パケットを待ちます。インタフェースが再送間隔以内に acknowledgment パケットを受信しない場合、LSA を再送します。

LSA パケットの不必要な再送を防ぐため、適切な再送間隔を設定してください。たとえば低速リンクの再送間隔は大きくします。

例

VLAN インタフェース 10 の LSA 再送間隔を 8 秒に設定します。

<Switch> system-view

[Switch] interface vlan-interface 10

[Switch-Vlan-interface10] ospf timer retransmit 8

5.1.64 ospf trans-delay

Syntax

ospf trans-delay *seconds*

undo ospf trans-delay

デフォルト

1 秒

View

Interface view

定義済みユーザロール

network-admin

パラメータ

seconds: LSA の伝送遅延を指定します。設定範囲は 1～3600 秒です。

説明

ospf trans-delay コマンドはインタフェースの LSA の伝送遅延を設定します。

undo ospf trans-delay コマンドはデフォルトに戻します。

LSDB の各 LSA のエージングタイマは 1 秒ごとに増加しますが、送信する間、エージングタイマは変更しません。低速ネットワークではエージング時間に伝送遅延を追加することが必要となります。

例

VLAN インタフェース 10 の LSA 伝送遅延を 3 秒に設定します。

<Switch> system-view

[Switch] interface vlan-interface 10

[Switch-Vlan-interface10] ospf trans-delay 3

5.1.65 peer

Syntax

peer *ip-address* [**cost** *value* | **dr-priority** *dr-priority*]

undo peer *ip-address*

デフォルト

設定なし

View

OSPF view

定義済みユーザロール

network-admin

パラメータ

ip-address: IP アドレスで隣接を指定します。

cost *value*: 隣接に到達するコストを指定します。設定範囲は 1～65535 です。

dr-priority *dr-priority*: 隣接の DR の優先順位を指定します。設定範囲は 0～255 です。デフォルトの隣接の DR の優先順位は 1 です。

説明

peer コマンドは NBMA あるいは P2MP ネットワークの隣接を指定します。

undo peer コマンドは設定を削除します。

NBMA あるいは P2MP ネットワークでは、OSPF パケットはユニキャストで送信するため、隣接を指定する **peer** コマンドを使用する必要があります。

peer コマンドのコストは P2MP の隣接にのみ適用します。コストが指定されない場合、隣接へのコストはローカルインタフェースのコストと同一となります。

ルータは DR の選出に使用するのではなく、隣接に Hello パケットを送信するかどうかを決定するために **peer** コマンドで設定された優先順位を使用します。**ospf dr-priority** コマンドで設定された DR の優先順位は DR の選出に使用します。

例

隣接 1.1.1.1 を指定します。

<Switch> system-view

[Switch] ospf 100

[Switch-ospf-100] peer 1.1.1.1

関連コマンド

ospf dr-priority

5.1.66 preference

Syntax

preference [**ase**] { *preference* | **route-policy** *route-policy-name* } *

undo preference [**ase**]

デフォルト

OSPF 内部ルートの優先順位は 10 です。OSPF 外部ルート（あるいは ASE ルート）の優先順位は 150 です。

View

OSPF view

定義済みユーザロール

network-admin

パラメータ

ase: OSPF 外部ルートの優先順位を指定します。指定しない場合、OSPF 内部ルートの優先順位を設定します。

preference: OSPF ルートの優先順位を指定します。設定範囲は 1～255 です。値が小さいほど優先順位は高くなります。

route-policy *route-policy-name*: ルーティングポリシーを指定します。設定範囲は 1～63 です。

説明

preference コマンドは OSPF の優先順位を設定します。

undo preference コマンドはデフォルトに戻します。

route-policy *route-policy-name* を指定する場合、以下の優先順位を適用します。

- ルーティングポリシーにマッチするルートの場合、ルーティングポリシーの優先順位を適用します。
- その他のルートの場合、**preference** コマンドの設定を適用します。

複数のルーティングプロトコルが同一宛先への複数のルートを検出した場合、ルータはもっとも高い優先順位のプロトコルのルートを使用します。

例

OSPF 外部ルートの優先順位を 200 に設定します。

<Switch> system-view

[Switch] ospf 100

[Switch-ospf-100] preference ase 200

指定したルーティングポリシーにマッチする OSPF 外部ルートの優先順位を 100 に設定します。ほかのルートの優先順位を 150 に設定します。

<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

5.1.67 reset ospf event-log

Syntax

reset ospf [*process-id*] **event-log** [**lsa-flush** | **peer** | **spf**]

View

User view

定義済みユーザロール

network-admin

パラメータ

process-id: OSPF プロセスを指定します。設定範囲は 1～65535 です。指定しない場合、コマンドはすべての OSPF プロセスの OSPF ログ情報を削除します。

lsa-flush: LSA エージングログ情報を削除します。

peer: 隣接ログ情報を削除します。

spf: ルート計算ログ情報を削除します。

説明

reset ospf event-log コマンドは、OSPF ログ情報を削除します。

例

すべての OSPF プロセスの OSPF ルート計算ログ情報を削除します。

<Switch> reset ospf event-log spf

関連コマンド

display ospf event-log

5.1.68 reset ospf statistics

Syntax

reset ospf [*process-id*] **statistics**

View

User view

定義済みユーザロール

network-admin

パラメータ

process-id: OSPF プロセスで指定した統計情報を削除します。設定範囲は 1～65535 です。

説明

reset ospf statistics コマンドは OSPF の統計情報を削除します。

例

すべてのプロセスの OSPF の統計情報を削除します。

<Switch> reset ospf statistics

関連コマンド

display ospf statistics

5.1.69 reset ospf process

Syntax

reset ospf [*process-id*] **process** [**graceful-restart**]

View

User view

定義済みユーザロール

network-admin

パラメータ

process-id: OSPF プロセスを指定します。設定範囲は 1～65535 です。

graceful-restart: GR を使用して OSPF プロセスを再起動します。

説明

reset ospf process コマンドは OSPF プロセスあるいは指定したプロセスを再起動します。

process-id を指定しない場合、すべての OSPF プロセスを再起動します。

reset ospf process コマンドは以下のアクションを実行します。

- タイマのタイムアウトを待つことなく、すべての異常な LSA を削除します。
- 新しく設定されたルータ ID を適用します。
- 新しい DR、BDR の選定を開始します。
- 以前の OSPF の設定を保持します。

システムは OSPF プロセスの実行を開始するかどうかの選択メッセージを表示します。

例

OSPF プロセスを再起動します。

<Switch> reset ospf process

```
Reset OSPF process? [Y/N]:y
```

5.1.70 reset ospf redistribution

Syntax

reset ospf [*process-id*] **redistribution**

View

User view

定義済みユーザロール

network-admin

パラメータ

process-id: OSPF プロセスを指定します。設定範囲は 1～65535 です。

説明

reset ospf redistribution コマンドはルートの再配信を再スタートします。

process-id を指定しない場合、すべての OSPF プロセスのルートの再配信を再スタートします。

例

ルートの再配信を再スタートします。

<Switch> reset ospf redistribution

5.1.71 rfc1583 compatible

Syntax

rfc1583 compatible

undo rfc1583 compatible

デフォルト

有効

View

OSPF view

定義済みユーザロール

network-admin

説明

rfc1583 compatible コマンドは RFC1583 の互換性を有効にします。

undo rfc1583 compatible コマンドは RFC1583 の互換性を無効にします。

別の AS にある宛先への最適なルートを選択する場合、RFC1583 は RFC2328 と異なります。複数のルートは ASBR で有効なとき、OSPF は以下の優先順位で最適ルートを選択します。

1) もっとも高い優先順位のルートを選択します。
   - □ もし RFC2328 が RFC1583 で互換性がある場合、すべてのルートの優先度は同一です。
   - □ もし RFC2328 が RFC1583 と互換性がない場合、バックボーンエリアの負荷を軽減するために非バックボーンエリアの内部エリアルートが選択されます。バックボーンエリアの内部エリアと外部エリアの優先度は同一です。
2) 2 つのルートの優先度が同一である場合、コストの低いルートを選択します。
3) 2 つのルートのコストが同一である場合、もとのエリア ID が大きい値のルートを選択します。

ルーティングループを回避するために、RFC1583 と互換性があるようにすべてのルータに設定することを推奨します。

例

RFC1583 の互換性を無効にします。

<Switch> system-view

[Switch] ospf 100

[Switch-ospf-100] undo rfc1583 compatible

5.1.72 router id

Syntax

router id *router-id*

undo router id

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

router-id: IPv4 アドレス形式でルータ ID を指定します。

説明

router id コマンドはグローバルでルータ ID を設定します。

undo router id コマンドはデフォルトに戻します。

ルータ ID は AS で OSPF が動作する装置を識別するために使用します。ルータ ID が設定されていない場合、グローバルのルータ ID が使用されます。

グローバルでルータ ID が設定されていない場合、もっとも高い loopback インタフェースの IP アドレスがルータ ID として適用されます。loopback インタフェースの IP アドレスが有効でない場合、インタフェースの状態（up あるいは down）にかかわらず、もっとも高い物理インタフェースの IP アドレスがルータ ID として適用されます。

アクティブ／スタンバイの切り替えの間、新しいアクティブな MPU（main processing unit）はバックアップした以前のルータ ID が有効かどうか確認します。ルータ ID が有効でない場合、新しいルータ ID を選択します。

ルータ ID として選択されたインタフェースの IP アドレスが削除あるいは変更された場合、新しいルータ ID が選択されます。以下のイベントではルータ ID の再選択を開始しません。

- インタフェースがダウンしました。
- 選択した物理インタフェースのアドレスをルータ ID として選択した後、Loopback インタフェースの IP アドレスが設定されました。
- もっとも高いインタフェースの IP アドレスが設定されました。

ルータ ID が変更された後、変更を適用するため、**reset** コマンドを使用します。

例

グローバルでルータ ID を 1.1.1.1 に設定します。

<Switch> system-view

[Switch] router id 1.1.1.1

5.1.73 silent-interface (OSPF view)

Syntax

silent-interface { *interface-type interface-number* | **all** }

undo silent-interface { *interface-type interface-number* | **all** }

デフォルト

設定なし

View

OSPF view

定義済みユーザロール

network-admin

パラメータ

interface-type interface-number: インタフェースのタイプと番号を指定します。

all: すべてのインタフェースを指定します。

説明

silent-interface コマンドは指定したインタフェースあるいはすべてのインタフェースで OSPF パケットの送受信を無効にします。

undo silent-interface コマンドはデフォルトに戻します。

無効に設定されたインタフェースは hello パケットの送受信ができないパッシブインタフェースです。

ネットワークで OSPF ルートの送受信を無効にする場合、ネットワークに接続されたインタフェースで **silent-interface** コマンドを実行します。

例

OSPF プロセス 100 で OSPF パケットの送受信を行う VLAN インタフェース 10 を無効にします。

<Switch> system-view

[Switch] ospf 100

[Switch-ospf-100] silent-interface vlan-interface 10

5.1.74 snmp-agent trap enable 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**]*

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

パラメータ

authentication-failure: インタフェースで認証失敗の通知を指定します。

bad-packet: インタフェースで受信したエラーメッセージの通知を指定します。

config-error: インタフェースのエラー設定の通知を指定します。

grhelper-status-change: GR ヘルパーの状態変更の通知を指定します。

grrestarter-status-change: GR リスタータの変更の通知を指定します。

if-state-change: インタフェースの状態の変更の通知を指定します。

lsa-maxage: LSA の最大エージングタイマの通知を指定します。

lsa-originate: ローカルに作成された LSA の通知を指定します。

lsdb-approaching-overflow: LSDB がオーバーフローに近づいたとき、通知を指定します。

lsdb-overflow: LSDB オーバーフローの通知を指定します。

neighbor-state-change: 隣接状態の変更の通知を指定します。

nssatranslator-status-change: NSSA 転送状態の変更の通知を指定します。

retransmit: インタフェースで受信、転送されたパケットの通知を指定します。

virt-authentication-failure: 仮想インタフェースの認証失敗の通知を指定します。

virt-bad-packet: 仮想インタフェースで受信したエラーメッセージの通知を指定します。

virt-config-error: 仮想インタフェースのエラー設定の通知を指定します。

virt-retransmit: 仮想インタフェースで受信、転送されたパケットの通知を指定します。

virtgrhelper-status-change: 仮想インタフェースの隣接 GR ヘルパーの状態の変更の通知を指定します。

virtif-state-change: 仮想インタフェースの状態の変更の通知を指定します。

virtneighbor-state-change: 仮想インタフェースの隣接状態の変更の通知を指定します。

説明

snmp-agent trap enable ospf コマンドは OSPF の SNMP 通知を有効にします。

undo snmp-agent trap enable ospf コマンドは OSPF の SNMP 通知を無効にします。

例

OSPF の SNMP 通知を無効にします。

<Switch> system-view

[Switch] undo snmp-agent trap enable ospf

5.1.75 spf-schedule-interval

Syntax

spf-schedule-interval *maximum-interval* [*minimum-interval* [*incremental-interval*]]

undo spf-schedule-interval

デフォルト

SPF 計算の最大間隔は 5 秒、最小間隔は 50 ミリ秒、増加する間隔は 200 ミリ秒です。

View

OSPF view

定義済みユーザロール

network-admin

パラメータ

maximum-interval: OSPF SPF 計算の最大間隔を指定します。設定範囲は 1～60 秒です。

minimum-interval: OSPF SPF 計算の最小間隔を指定します。設定範囲は 10～60000 ミリ秒です。

incremental-interval: OSPF SPF 計算の増加する間隔を指定します。設定範囲は 10～60000 ミリ秒です。

説明

spf-schedule-interval コマンドは OSPF SPF 計算の間隔を設定します。

undo spf-schedule-interval コマンドはデフォルトに戻します。

LSDB にもとづいて、OSPF ルータはルートとして OSPF ルータの最小パスツリーを計算するため、SPF を使用します。OSPF は宛先へのネクストホップを決定するため、最小のパスツリーを使用します。SPF 計算間隔を調整することによって、頻繁にトポロジが変更することにより、帯域幅とルータのリソースの過剰な消費を防止することができます。

安定したネットワークでは最小間隔が使用されます。頻繁にネットワークが変更する場合、SPF を計算する間隔は最大間隔に到達するまで、各計算を行う際に増加する間隔を追加していきます。

最小間隔と増加する間隔は、最大間隔よりも小さくする必要があります。

例

SPF 計算の最大間隔を 10 秒、最小間隔を 500 ミリ秒、増加する間隔を 300 ミリ秒に設定します。

<Switch> system-view

[Switch] ospf 100

[Switch-ospf-100] spf-schedule-interval 10 500 300

5.1.76 stub (OSPF area view)

Syntax

stub [**default-route-advertise-always** | **no-summary**] *

undo stub

デフォルト

設定なし

View

OSPF area view

定義済みユーザロール

network-admin

パラメータ

default-route-advertise-always: スタブ ABR でのみ使用します。ABR は、バックボーンエリアに FULL 状態の隣接があるかどうかにかかわらず Type-3 LSA のデフォルトルートをスタブエリアに配信します。指定しない場合、ABR はバックボーンエリアに少なくとも 1 つの FULL 状態の隣接があるときのみ Type-3 LSA のデフォルトルートをスタブエリアに配信します。

no-summary: スタブ ABR でのみ使用します。ABR はほかの Type-3 LSA（スタブエリアが完全スタブエリアです）に配信することなく、Type-3 LSA のデフォルトルートをスタブエリアに配信します。

説明

stub コマンドはスタブエリアとしてエリアを設定します。

undo stub コマンドはデフォルトに戻します。

ABR で **default-route-advertise-always** パラメータあるいは **stub no-summary** パラメータの設定を削除する場合、設定を上書きするため、再度 **stub** コマンドを設定します。

スタブエリアとしてエリアを設定する場合、エリアに接続しているすべてのルータで **stub** コマンドを設定します。

例

スタブエリアとしてエリア 1 を設定します。

<Switch> system-view

[Switch] ospf 100

[Switch-ospf-100] area 1

[Switch-ospf-100-area-0.0.0.1] stub

関連コマンド

default-cost (OSPF area view)

5.1.77 stub-router

Syntax

stub-router [**external-lsa** [*max-metric-value*] | **include-stub** | **on-startup** *seconds* | **summary-lsa** [*max-metric-value*]] *

undo stub-router

デフォルト

設定なし

View

OSPF view

定義済みユーザロール

network-admin

パラメータ

external-lsa *max-metric-value*: 外部 LSA のコストを 1~16777215 の範囲で指定します。デフォルトは 16711680 です。

include-stub: ルータ LSA 内の stub リンク(リンクタイプ 3)のコストを最大値 65535 まで指定します。

on-startup *seconds*: リブート時にルータを stub ルータとして指定し、タイムアウト時間を 5~86400 秒の範囲で指定します。

summary-lsa *max-metric-value*: Type-3 LSA のコストを 1~16777215 の範囲で指定します。デフォルトのコスト値は 16711680 です。

説明

stub-router コマンドはスタブルータとしてルータを設定します。

undo stub-router コマンドはデフォルトに戻します。

スタブルータからのルータ LSA は異なるリンクタイプの値が含まれていることがあります。3 はスタブネットワークへのリンクを意味します。そのため、リンクコストは変更されません。1 はポイントツーポイントリンク、2 は中間ネットワークへのリンク、4 は仮想リンクを示します。1、2、4 の場合、最大コスト値である 65535 が使用されます。ほかの隣接がスタブルータへのリンクはコストが大きいことを検出した場合、小さいコストのルートがある限り、スタブエリアへパケットを送信しません。

例

スタブルータを設定します。

<Switch> system-view

[Switch] ospf 100

[Switch-ospf-100] stub-router

5.1.78 transmit-pacing

Syntax

transmit-pacing interval *interval* **count** *count*

undo transmit-pacing

デフォルト

OSPF インタフェースは 20 ミリ秒ごとに最大 3 つの LSU パケットを送信します。

View

OSPF view

定義済みユーザロール

network-admin

パラメータ

interval *interval*: インタフェースが LSU パケットを送信する間隔を指定します。設定範囲は 10～1000 ミリ秒です。ルータに複数の OSPF インタフェースが設定されている場合、1 秒ごとにルータから送信される LSU パケットの総数を減らすため間隔を増加します。

count *count*: 一回ごとにインタフェースから送信される LSU パケットの最大数を指定します。設定範囲は 1～200 です。ルータに複数の OSPF インタフェースが設定されている場合、一回ごとにルータから送信される LSU パケット総数を減らします。

説明

transmit-pacing コマンドは指定した間隔で送信される LSU パケットの最大数を設定します。

undo transmit-pacing コマンドはデフォルトに戻します。

例

OSPF プロセス 1 が動作するすべてのインタフェースで LSU パケットを 30 ミリ秒ごとに最大 10 のパケットを送信します。

<Switch> system-view

[Switch] ospf 1

[Switch-ospf-1] transmit-pacing interval 30 count 10

5.1.79 vlink-peer (OSPF area view)

Syntax

vlink-peer *router-id* [**dead** *seconds* | **hello** *seconds* | { { **hmac-md5** | **md5** } *key-id* { **cipher** *cipher-string* | **plain** *plain-string* } | **simple** { **cipher** *cipher-string* | **plain** *plain-string* } } | **retransmit** *seconds* | **trans-delay** *seconds*] *

undo vlink-peer *router-id* [**dead** | **hello** | { **hmac-md5** | **md5** } *key-id* | **retransmit** | **simple** | **trans-delay**] *

デフォルト

設定なし

View

OSPF area view

定義済みユーザロール

network-admin

パラメータ

router-id: 仮想リンクの隣接のルータ ID を指定します。

dead *seconds*: dead タイマを指定します。設定範囲は 1～32768 秒です。デフォルトは 40 秒です。dead タイマは仮想リンクの隣接間で同一にする必要があります。少なくとも Hello タイマの 4 倍にする必要があります。

hello *seconds*: hello 間隔を指定します。設定範囲は 1～8192 秒です。デフォルトは 10 秒です。仮想リンクの隣接間で同一にする必要があります。

hmac-md5: HMAC-MD5 認証モードを指定します。

md5: MD5 認証モードを指定します。

simple: simple 認証モードを指定します。

key-id: MD5 あるいは HMAC-MD5 認証のキーID を指定します。設定範囲は 1～255 です。

cipher: 暗号テキストキーを指定します。

cipher-string: 暗号テキストキーを指定します。**simple** が設定された場合の設定範囲は 33～41 文字です。**md5** あるいは **hmac-md5** が設定された場合の設定範囲は 33～53 文字です。

plain: プレーンテキストキーを指定します。

plain-string: プレーンテキストキーを指定します。**simple** が設定された場合の設定範囲は 1～8 文字です。**md5** あるいは **hmac-md5** が設定された場合の設定範囲は 1～16 文字です。

retransmit *seconds*: 再配信する間隔を指定します。設定範囲は 1～3600 秒です。デフォルトは 5 秒です。

trans-delay *seconds*: 伝送遅延を指定します。設定範囲は 1～3600 秒です。デフォルトは 1 秒です。

説明

vlink-peer コマンドは仮想リンクを設定します。

undo vlink-peer コマンドは仮想リンクを削除します。

RFC2328 で定義されているように、すべての非バックボーンエリアはバックボーンエリアへの接続を保持する必要があります。**vlink-peer** コマンドは、エリアをバックボーンに接続するため仮想リンクを設定します。

vlink-peer コマンドを設定するとき、以下のガイドラインに従ってください。

- Hello 間隔が短くなると、ネットワークの収束が早くなりますが、ネットワークのリソースの消費が大きくなります。
- 再配信する間隔が小さすぎる場合、不必要な再配信が発生する可能性があります。低速のリンクの場合、大きい値にしてください。
- **trans-delay** パラメータで適切に伝送遅延を設定してください。

セキュリティのため、プレーンテキストで設定されたキーを含むすべてのキーは暗号テキストで保存されます。

仮想リンクで MD5/HMAC-MD5 認証あるいは simple 認証のどちらかを指定することができます。MD5/HMAC-MD5 認証では **authentication-mode** コマンドを複数実行することで複数のキーを設定することができます。各コマンドは固有のキーID とキーの文字列にする必要があります。

仮想リンクのキーを修正する場合、以下の交換の設定を実行してください。

1) ローカル装置のエリア用に新規の MD5/HMAC-MD5 認証キーを設定します。隣接装置で新しいキーが設定されていない場合、MD5/HMAC-MD5 認証のキーの交換が開始します。キーの交換が行われている間、OSPF は新しい MD5/HMAC-MD5 認証キーと古い MD5/HMAC-MD5 認証キーが含まれる複数のパケットを送信します。すべての隣接装置で認証がパスすることを確認してください。
2) すべての隣接装置の新しい MD5/HMAC-MD5 認証キーを設定します。ローカル装置がすべての隣接装置から新しいキーのパケットを受信するとき、MD5 キーの交換が行われます。
3) ローカル装置とすべての隣接装置から古い MD5/HMAC-MD5 認証キーを削除します。この処理を行うことで、通信を行うために古いキーを使用している装置が攻撃されることを防ぎ、キーの交換によって引き起こされるシステムリソース、帯域幅の消費を削減することができます。

例

仮想リンクをルータ ID が 1.1.1.1 の隣接に設定します。

<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

関連コマンド

- **authentication-mode**
- **display ospf vlink**

目次

このセクションのページは **5-x-x** です。

6 章 ポリシーベースルーティング 6-1
6.1 ポリシーベースルーティング設定コマンド 6-1
6.1.1 apply next-hop 6-1
6.1.2 description 6-2
6.1.3 display ip policy-based-route 6-2
6.1.4 display ip policy-based-route interface 6-3
6.1.5 display ip policy-based-route setup 6-6
6.1.6 if-match acl 6-7
6.1.7 ip local policy-based-route 6-8
6.1.8 ip policy-based-route 6-9
6.1.9 policy-based-route 6-9
6.1.10 reset ip policy-based-route statistics 6-11

6章 ポリシーベースルーティング

6.1 ポリシーベースルーティング設定コマンド

6.1.1 apply next-hop

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>]

デフォルト

設定なし

View

Policy node view

定義済みユーザロール

network-admin

パラメータ

vpn-instance *vpn-instance-name*：VPN インスタンスを名前で指定します。大文字小文字を区別し、設定範囲は 1～31 文字です。指定の VPN インスタンスはすでに存在していなくてはなりません。

ip-address: ネクストホップの IP アドレスを指定します。

direct: 直接接続されているネクストホップを指定します。

track *track-entry-number*: Track エントリを指定します。設定範囲は 1～1024 です。

&<1-2>: 引数を最大 2 回まで設定できることを示します。

説明

apply next-hop コマンドはネクストホップを設定します。

undo apply next-hop コマンドは設定を削除します。

バックアップあるいはロードシェアリングのために、このコマンドを繰り返し設定することで、ネクストホップを複数指定することができます。

ネクストホップを指定して **undo apply next-hop** コマンドを使用すると、ネクストホップを削除します。

ネクストホップを指定せずにこのコマンドを使用すると、すべてのデフォルトのネクストホップを削除します。

例

直接接続された 1.1.1.1 をネクストホップに設定します。

<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 description

Syntax

description *text*

undo description

デフォルト

設定なし

View

Policy node view

定義済みユーザロール

network-admin

パラメータ

text: 説明を指定します。設定範囲は 1～127 文字です。大文字、小文字を区別します。

説明

description コマンドはポリシーノードの説明を設定します。

undo description コマンドはデフォルトに戻します。

例

ポリシーノード 1 の **Officeuse** という記述を設定検索します。

<Switch> system-view

[Switch] policy-based-route 1 permit node 1

[Switch-pbr-1-1] description Officeuse

6.1.3 display ip policy-based-route

Syntax

display ip policy-based-route [**policy** *policy-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

policy *policy-name*: ポリシーの名前を指定します。設定範囲は 1～19 です。大文字、小文字を区別します。ポリシーを指定しない場合、このコマンドはすべての PBR ポリシーの情報を表示します。

説明

display ip policy-based-route コマンドは PBR ポリシー情報を表示します。

例

すべてのポリシーの情報を表示します。

<Switch> display ip policy-based-route

```
Policy name: aaa
  node 1 permit:
    if-match acl 2000
    apply next-hop 1.1.1.1
```

表 6-1 コマンド出力

フィールド	説明
node 1 permit	ノード1にマッチするモードが許可されています。
if-match acl	パケットをACLと比較します。
apply next-hop	許可されたパケットのネクストホップを指定します。

関連コマンド

policy-based-route

6.1.4 display ip policy-based-route interface

Syntax

display ip policy-based-route interface *interface-type interface-number* [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface-type interface-number: インタフェースタイプと番号を指定します。

slot *slot-number*: メンバ ID によって IRF スタックメンバ装置を指定します。メンバ装置を指定しない場合、このコマンドはマスタ装置の情報を表示します。

説明

display ip policy-based-route interface コマンドはインタフェースの PBR 設定情報と統計情報を表示します。

例

VLAN インタフェース 2 の PBR 設定情報と統計情報を表示します。

<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
```

表 6-2 コマンド出力

フィールド	説明
Policy based routing information for interface XXXX(failed)	統計情報のPBR設定とインタフェースです。 🕮 メモ： スロット番号を指定すると、このフィールドには、ドライバに発行できなかったポリシーの「**failed**」が角かっこで囲まれて表示されます。この障害は、PBRポリシー内のすべてのノード設定の発行に失敗したことを意味します。
node 0 deny node 2 permit	ノードのマッチモード、**permit**あるいは**deny**があります。 🕮 メモ： スロット番号を指定すると、このフィールドには有効でないノードの原因が角かっこで囲まれて表示されます。 ● **not support**—ノードで設定されたマッチ基準を装置がサポートしていないことを示します。 ● **no resource**—ノードに十分なリソース（ACLなど）がないことを示します。
if-match acl	パケットをACLと比較します。
apply next-hop	許可されたパケットのネクストホップを指定します。
Matched: 0	ノードでマッチした数です。 🕮 メモ： スロット番号を指定しても、装置にスロット上の統計情報を収集するための十分なリソースがない場合、このフィールドには角カッコで囲まれた統計情報リソースは表示されません。
Total matched	すべてのノードでマッチした総数です。

関連コマンド

reset ip policy-based-route statistics

6.1.5 display ip policy-based-route setup

Syntax

display ip policy-based-route setup

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display ip policy-based-route setup コマンドは PBR 設定を表示します。

例

PBR 設定を表示します。

<Switch> display ip policy-based-route setup

```
Policy name            Type    Interface
pr01                  Forward  Vlan-interface2
aaa                   Local    N/A
```

表 6-3 コマンド出力

フィールド	説明
Type	PBRのタイプです。 ● **Forward**—インタフェースPBRです。 ● **Local**—ローカルPBRです。
Interface	ポリシーが適用されるインタフェースです。

関連コマンド

ip policy-based-route

6.1.6 if-match acl

Syntax

if-match acl { *acl-number* | **name** *acl-name* }

undo if-match acl

デフォルト

設定なし

View

Policy node view

定義済みユーザロール

network-admin

パラメータ

acl-number: ACL の番号を指定します。標準 ACL の設定範囲は 2000～2999 です。拡張 ACL の設定範囲は 3000～3999 です。

name *acl-name*: ACL の名前を指定します。設定範囲は 1～63 です。大文字、小文字を区別しません。ACL の名前の先頭は *a*～*z*、*A*～*Z* の英字です。コマンドを有効にするには、指定した ACL が標準 ACL または拡張 ACL であることを確認してください。

説明

if-match acl コマンドは ACL マッチ基準を設定します。

undo if-match acl コマンドはデフォルトに戻します。

例

ACL 2011 にマッチするパケットを許可するポリシー**aa** のノード 11 を設定します。

<Switch> system-view

[Switch] policy-based-route aa permit node 11

[Switch-pbr-aa-11] if-match acl 2011

ACL 名 **aaa** の ACL にマッチするパケットを許可するポリシー**aa** のノード 11 を設定します。

<Switch> system-view

[Switch] policy-based-route aa permit node 11

[Switch-pbr-aa-11] if-match acl name aaa

6.1.7 ip local policy-based-route

Syntax

ip local policy-based-route *policy-name*

undo ip local policy-based-route

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

policy-name: ポリシー名を指定します。設定範囲は 1～19 です。大文字、小文字を区別します。ポリシーは既に作成されている必要があります。

説明

ip local policy-based-route コマンドはローカル PBR のポリシーを指定します。

undo ip local policy-based-route コマンドはデフォルトに戻します。

ローカル PBR は、**ping** コマンドを使用して生成された ICMP パケットなど、ローカルに生成されたパケットの転送をガイドします。

ローカル PBR は、ping や Telnet などのローカルサービスに影響を与える可能性があります。ローカル PBR を使用する場合は、装置のローカルサービスへの影響を十分に理解してください。

ローカル PBR に指定できるポリシーは 1 つだけで、指定したポリシーがすでに存在することを確認する必要があります。

新しいポリシーを適用する前に、現在のポリシーを削除する必要があります。

例

ポリシー**aaa** にもとづいてローカル PBR を設定します。

<Switch> system-view

[Switch] ip local policy-based-route aaa

関連コマンド

- **display ip policy-based-route setup**
- **policy-based-route**

6.1.8 ip policy-based-route

Syntax

ip policy-based-route *policy-name*

undo ip policy-based-route

デフォルト

設定なし

View

Interface view

定義済みユーザロール

network-admin

パラメータ

policy-name: ポリシー名を指定します。設定範囲は 1～19 です。大文字、小文字を区別します。ポリシーは既に作成されている必要があります。

説明

ip policy-based-route コマンドはインタフェース上のインタフェース PBR のポリシーを指定します。

undo ip policy-based-route コマンドはデフォルトに戻します。

例

VLAN インタフェース 2 にポリシー**aaa** を適用します。

<Switch> system-view

[Switch] interface vlan-interface 2

[Switch-Vlan-interface2] ip policy-based-route aaa

関連コマンド

- **display ip policy-based-route setup**
- **policy-based-route**

6.1.9 policy-based-route

Syntax

policy-based-route *policy-name* [**deny** | **permit**] **node** *node-number*

undo policy-based-route *policy-name* [**deny** | **node** *node-number* | **permit**]

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

policy-name: ポリシー名を指定します。設定範囲は 1～19 です。大文字、小文字を区別します。

deny: ポリシーのマッチモードを **deny** に指定します。

permit: ポリシーのマッチモードを **permit** に指定します。（デフォルトモード）

node *node-number*: ポリシーノードを指定します。設定範囲は 0～255 です。値を小さくすると優先度が高くなります。

説明

policy-based-route コマンドはポリシーノードを作成し、そのビューに移行するか、デフォルトのポリシーノードのビューに移行します。

undo policy-based-route コマンドはポリシーノードを削除します。

インタフェースあるいはローカルに適用されたポリシーは削除することができません。削除する場合、最初にインタフェースあるいはローカルからポリシーベースの PBR の適用を削除してください。

- ポリシーノードが指定されている場合、**undo policy-based-route** コマンドは指定されたノードのポリシーを削除します。
- マッチモードが指定されている場合、コマンドはマッチモードに設定されたすべてのノードを削除します。
- ポリシーノードあるいはマッチモードが指定されていない場合、コマンドはポリシー全体を削除します

例

ノード 10 の許可モードのポリシー**policy1** を作成し、policy node view に移行します。

<Switch> system-view

[Switch] policy-based-route policy1 permit node 10

[Switch-pbr-policy1-10]

関連コマンド

display ip policy-based-route

6.1.10 reset ip policy-based-route statistics

Syntax

reset ip policy-based-route statistics [**policy** *policy-name*]

View

User view

定義済みユーザロール

network-admin

パラメータ

policy *policy-name*: ポリシー名を指定します。設定範囲は 1～19 です。大文字、小文字を区別します。ポリシーを指定しない場合、このコマンドはすべてのポリシーの PBR 統計情報を削除します。

説明

reset ip policy-based-route statistics コマンドは PBR の統計情報を削除します。

例

すべての PBR の統計情報を削除します。

<Switch> reset ip policy-based-route statistics

関連コマンド

- **display ip policy-based-route interface**

目次

このセクションのページは **5-x-x** です。

7 章 RIPng..... 7-1
7.1 RIPng 設定コマンド..... 7-1
7.1.1 checkzero..... 7-1
7.1.2 default cost..... 7-1
7.1.3 display ripng..... 7-2
7.1.4 display ripng database..... 7-4
7.1.5 display ripng graceful-restart..... 7-5
7.1.6 display ripng interface..... 7-6
7.1.7 display ripng non-stop-routing..... 7-7
7.1.8 display ripng route..... 7-8
7.1.9 filter-policy export..... 7-11
7.1.10 filter-policy import..... 7-12
7.1.11 graceful-restart..... 7-14
7.1.12 import-route..... 7-14
7.1.13 maximum load-balancing..... 7-15
7.1.14 non-stop-routing..... 7-16
7.1.15 preference..... 7-17
7.1.16 reset ripng process..... 7-18
7.1.17 reset ripng statistics..... 7-18
7.1.18 ripng..... 7-19
7.1.19 ripng default-route..... 7-20
7.1.20 ripng enable..... 7-21
7.1.21 ripng metricin..... 7-22
7.1.22 ripng metricout..... 7-23
7.1.23 ripng poison-reverse..... 7-23
7.1.24 ripng split-horizon..... 7-24
7.1.25 ripng summary-address..... 7-25
7.1.26 timers..... 7-26

7章 RIPng

7.1 RIPng設定コマンド

7.1.1 checkzero

Syntax

checkzero

undo checkzero

デフォルト

有効

View

RIPng view

定義済みユーザロール

network-admin

説明

checkzero コマンドは RIPng パケットのゼロフィールドのチェック機能を有効にします。

undo checkzero コマンドはゼロフィールドのチェック機能を無効にします。

RIPng パケットヘッダのあるフィールドは 0 にする必要があります。このフィールドはゼロフィールドと呼ばれます。受信 RIPng パケットのゼロフィールドのチェック機能を有効にすることができます。ゼロフィールドのチェック機能が有効であるとき、ルータはゼロフィールドに 0 でない値が含まれる RIPng パケットを廃棄します。

例

RIPng プロセス 100 の RIPng パケットのゼロフィールドチェック機能を無効にします。

<Switch> system-view

[Switch] ripng 100

[Switch-ripng-100] undo checkzero

7.1.2 default cost

Syntax

default cost *value*

undo default cost

デフォルト

0

View

RIPng view

定義済みユーザロール

network-admin

パラメータ

value: 再配信されたルートのデフォルトメトリックを指定します。設定範囲は 0～16 です。

説明

default cost コマンドは再配信されたルートのデフォルトメトリックを設定します。

undo default cost コマンドはデフォルトに戻します。

メトリックを指定しないで別のルーティングプロトコルからルートを再配信するため、**import-route** コマンドを使用するとき、**default cost** コマンドによって指定されたメトリックが適用されます。

例

再配信されたルートのデフォルトメトリックを 2 に設定します。

<Switch> system-view

[Switch] ripng 100

[Switch-ripng-100] default cost 2

関連コマンド

import-route

7.1.3 display ripng

Syntax

display ripng [*process-id*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

process-id: RIPng プロセスの ID を指定します。設定範囲は 1～65535 です。指定されない場合、すべての RIPng プロセスの情報を表示します。

説明

display ripng コマンドは RIPng プロセスの設定情報を表示します。

例

すべての RIPng プロセスの状態と設定情報を表示します。

<Switch> display ripng

```
  Public VPN-instance name:

RIPng process: 1
      Preference: 100
         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
      Number of periodic updates sent: 256
      Number of trigger updates sent: 1
```

表 7-1 コマンド出力

フィールド	説明
Public VPN-instance name/Private VPN-instance name	ぷブリックVPNインスタンスまたは指定したVPNインスタンスで動作するRIPngプロセスです。
RIPng process	RIPngプロセスIDです。
Preference	RIPngの優先順位です。
Checkzero	RIPngパケットのゼロフィールドチェック機能が有効かどうかを示します。
Default Cost	再配信されたルートのデフォルトメトリックです。
Maximum number of balanced paths	ロードバランスが行われるルートの最大数です。

フィールド	説明
Update time	RIPngアップデートの間隔です。単位は秒です。
Timeout time	RIPngタイムアウト時間です。単位は秒です。
Suppress time	RIPngルートが到達不能状態にとどまる時間です。単位は秒です。
Garbage-Collect time	RIPngガーベッジコレクト時間です。単位は秒です。

7.1.4 display ripng database

Syntax

display ripng *process-id* **database** [*ipv6-address prefix-length*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

process-id: RIPng プロセスの ID を指定します。設定範囲は 1～65535 です。

ipv6-address prefix-length: IPv6 アドレスを指定します。*ipv6-address* は IPv6 アドレスを指定します。*prefix-length* はプレフィックス長を指定します。*prefix-length* の設定範囲は 0～128 です。

説明

display ripng database コマンドは RIPng プロセスのアクティブルートを表示します。RIPng は RIPng ルーティングアップデートのアクティブルートを配信します。

例

RIPng プロセス 100 のアクティブルートを表示します。

<Switch> display ripng 100 database

```
1::/64,
    cost 0, RIPng-interface
10::/32,
    cost 0, imported
2::2/128,
   via FE80::20C:29FF:FE7A:E3E4, cost 1
```

表 7-2 コマンド出力

フィールド	説明
cost	ルートのメトリックです。
imported	別のルーティングプロトコルから再配信されたかどうかを示します。
RIPng-interface	インタフェースから学習したルートです。
via	ネクストIPv6アドレスです。

7.1.5 display ripng graceful-restart

Syntax

display ripng [*process-id*] **graceful-restart**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

process-id: RIPng プロセスの ID を指定します。設定範囲は 1～65535 です。

説明

display ripng graceful-restart コマンドは GR 情報を表示します。

例

RIPng プロセス 1 の GR 情報を表示します。

<Switch> display ripng 1 graceful-restart

```
RIPng process: 1
 Graceful Restart capability    : Enabled
 Current GR state             : Normal
 Graceful Restart period       : 60  seconds
 Graceful Restart remaining time: 0   seconds
```

表 7-3 コマンド出力

フィールド	説明
Graceful Restart capability	GRが使用可能かどうかを示します。: **Enabled**または**Disabled**です。
Current GR state	GR状態です。: ● **Under GR**—GRは処理中です。 ● **Normal**—GRは進行中ではないか、完了しています。

7.1.6 display ripng interface

Syntax

display ripng *process-id* **interface** [*interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

process-id: RIPng プロセスの ID を指定します。設定範囲は 1～65535 です。

interface-type interface-number: インタフェースのタイプと番号を指定します。指定しない場合、RIPng プロセスのすべてのインタフェースの情報を表示します。

説明

display ripng interface コマンドは RIPng プロセスのインタフェースの情報を表示します。

例

RIPng プロセス 1 のインタフェースの情報を表示します。

<Switch> display ripng 1 interface

```
Interface: Vlan-interface2
       Link-local address: FE80::20C:29FF:FEC8:B4DD
       Split-horizon: On              Poison-reverse: Off
       MetricIn: 0                   MetricOut: 1
       Default route: Off
       Summary address:
             1::/16
```

表 7-4 コマンド出力

フィールド	説明
Interface	RIPngが動作しているインタフェース名です。
Link Local Address	RIPngが動作しているインタフェースのリンクローカルアドレスです。
Split-horizon	スプリットホライズンが有効かどうかを示します。 ● **on**—有効です。 ● **off**—無効です。
Poison-reverse	ポイズンリバースが有効かどうかを示します。 ● **on**—有効です。 ● **off**—無効です。
MetricIn/MetricOut	送受信ルートに加えられた追加メトリックです
Default route	● **Only**—インタフェースはデフォルトルートのみを配信します。 ● **Originate**—インタフェースは他のRIPngルートと一緒にデフォルトルートを配信します。 ● **Off**—この状態ではインタフェースはデフォルトルートを配信しません。 ● **In garbage-collection status**—この状態ではインタフェースはメトリックが16のデフォルトルートを配信します。
Default route cost	デフォルトルートのメトリックです。

7.1.7 display ripng non-stop-routing

Syntax

display ripng [*process-id*] **non-stop-routing**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

process-id: RIPng プロセスの ID を指定します。設定範囲は 1～65535 です。

説明

display ripng non-stop-routing コマンドは RIPng NSR 情報を表示します。

例

RIPng プロセス 1 の NSR 情報を表示します。

<Switch> display ripng 1 non-stop-routing

```
RIPng process: 1
 Nonstop Routing capability: Enabled
 Current NSR state        : Finish
```

表 7-5 コマンド出力

フィールド	説明
Nonstop Routing capability	NSRが有効かどうかを示します。: **Enabled**または**Disabled**です。
Current NSR state	NSR状態です。: ● **Initialization**—初期化状態です。 ● **Smooth**—データをアップグレードします。 ● **Advertising**—配信ルートです。 ● **Redistribution**—ルートを再配信します。 ● **Finish**—終了です。

7.1.8 display ripng route

Syntax

display ripng *process-id* **route** [*ipv6-address prefix-length* [**verbose**] | **peer** *ipv6-address* | **statistics**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

process-id: RIPng プロセスの ID を指定します。設定範囲は 1～65535 です。

ipv6-address prefix-length: IPv6 アドレスを指定します。*ipv6-address* は IPv6 アドレスを指定します。*prefix-length* はプレフィックス長を指定します。*prefix-length* の設定範囲は 0～128 です。

verbose: 指定された宛先 IPv6 アドレスのすべてのルーティング情報を表示します。指定しない場合、指定された宛先 IPv6 アドレスの最適な IPv6 ルートのみを表示します。

peer *ipv6-address*: IPv6 アドレスで指定したネイバから学習したルート情報を表示します。

statistics: ルートの総数、各ネイバからのルート数を含むルートの統計情報を表示します。

説明

display ripng route コマンドは RIPng プロセスのすべての RIPng ルートの情報を表示します。

例

RIPng プロセス 1 のルーティング情報を表示します。

<Switch> display ripng 1 route

```
  Route Flags: A - Aging, S - Suppressed, G - Garbage-collect
               O - Optimal, F - Flush to RIB
----------------------------------------------------------------

Peer FE80::20C:29FF:FE7A:E3E4 on Ethernet1/2
Destination 1::/64,
    via FE80::20C:29FF:FE7A:E3E4, cost 1, tag 0, AOF, 7 secs
Destination 2::2/128,
    via FE80::20C:29FF:FE7A:E3E4, cost 1, tag 0, AOF, 7 secs
```

RIPng プロセス 1 の指定されたプレフィックスのルート情報を表示します。

<Switch> display ripng 1 route 1:: 64 verbose

```
  Route Flags: A - Aging, S - Suppressed, G - Garbage-collect
               O - Optimal, F - Flush to RIB
----------------------------------------------------------------

Peer FE80::20C:29FF:FE7A:E3E4 on Ethernet1/2
Destination 1::/64,
    via FE80::20C:29FF:FE7A:E3E4, cost 1, tag 0, AOF, 7 secs
Peer FE80::20C:29FF:FE7A:E3E5 on Ethernet1/3
Destination 1::/64,
    via FE80::20C:29FF:FE7A:E3E8, cost 2, tag 0, A, 7 secs
```

表 7-6 コマンド出力

フィールド	説明
A–Aging	ルートがエージアウトしている状態です。

フィールド	説明
S–Suppressed	ルートが集約されている状態です。
G–Garbage-collect	ルートがガーベッジコレクト状態です。
O - Optimal	ルートが最適ルートです。
F - Flush to RIB	ルートがRIBに送られています。
Peer	インタフェースに接続されたネイバです。
Destination	IPv6宛先アドレスです。
via	ネクストホップIPv6アドレスです。
cost	ルーティングメトリックの値です。
tag	ルートタグです。
secs	現在の状態で維持しているルートエントリの時間です。

RIPng プロセス 1 のルーティングの統計情報を表示します。

<Switch> display ripng 1 route statistics

```
 Peer                    Optimal/Aging      Garbage
 FE80::20C:29FF:FE7A:E3E4  2/3                0
Total                    2/3              0
```

表 7-7 コマンド出力

フィールド	説明
Peer	ネイバのIPv6アドレスです。
Optimal	最適ルートの数です。
Aging	エージアウトしているルートの数です。
Garbage	ガーベッジコレクト状態のルートの数です。
Total	すべてのRIPngネイバから学習されたルートの総数です。

7.1.9 filter-policy export

Syntax

filter-policy { *acl6-number* | **prefix-list** *prefix-list-name* } **export** [*protocol* [*process-id*]]

undo filter-policy export [*protocol* [*process-id*]]

デフォルト

設定なし

View

RIPng view

定義済みユーザロール

network-admin

パラメータ

acl6-number: 再配信されたルートをフィルタするため、IPv6 ACL 番号を指定します。設定範囲は 2000～3999 です。

prefix-list *prefix-list-name*: 再配信されたルートをフィルタするため、IPv6 プレフィックスリストの名前を指定します。設定範囲は 1～63 文字です。

protocol: 指定されたルーティングプロトコルから再配信されたルートをフィルタします。再配信されたルートはダイレクト、OSPFv3、RIPng、スタティックがあります。

process-id: ルーティングプロトコルのプロセス ID を指定します。設定範囲は 1～65535 です。ルーティングプロトコルが RIPng または OSPFv3 のときのプロセス ID を指定します。デフォルトは 1 です。

説明

filter-policy export コマンドは再配信されたルートをフィルタするために RIPng を設定します。フィルタされなかったルートのみアップデートメッセージで配信することができます。

undo filter-policy export コマンドは設定を削除します。

プロトコルが指定されている場合、RIPng は指定されたプロトコルからの再配信されたルートのみフィルタします。指定されていない場合、RIPng はすべての再配信されたルートをフィルタします。

拡張 IPv6 ACL（設定範囲は 3000～3999 です）を参照するため、以下の方法の 1 つを使用して IPv6 ACL を設定します。

- 指定された宛先のルートの許可/拒否を行う場合、**rule** [*rule-id*] { **deny** | **permit** } **ipv6 source** *sour sour-prefix* コマンドを使用します。
- 指定された宛先とプレフィックスのルートの許可/拒否を行う場合、**rule** [*rule-id*] { **deny** | **permit** } **ipv6 source** *sour sour-prefix* **destination** *dest dest-prefix* コマンドを使用します。

source はルートの宛先アドレスを指定します。**destination** はルートのプレフィックスを指定します。指定されたプレフィックスは隣接している必要があります。隣接していない場合、プレフィックスの設定は適用されません。

例

再配信された RIPng アップデートをフィルタするため、IPv6 プレフィックスリストを使用します。

<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

再配信されたルートをフィルタするため、IPv6 ACL3000 を設定し、ルート 2001::1/128 のみ許可できるようにします。

<Switch> system-view

[Switch] acl ipv6 number 3000

[Switch-acl6-adv-3000] rule 10 permit ipv6 source 2001::1 128 destination ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff 128

[Switch-acl6-adv-3000] rule 100 deny ipv6

[Switch-acl6-adv-3000] quit

[Switch] ripng 100

[Switch-ripng-100] filter-policy 3000 export

7.1.10 filter-policy import

Syntax

filter-policy { *acl6-number* | **prefix-list** *prefix-list-name* } **import**

undo filter-policy import

デフォルト

設定なし

View

RIPng view

定義済みユーザロール

network-admin

パラメータ

acl6-number: 受信するルートをフィルタするため、IPv6 ACL 番号を指定します。設定範囲は 2000～3999 です。

prefix-list *prefix-list-name*: 受信するルートをフィルタするため、IPv6 プレフィックスリストの名前を指定します。設定範囲は 1～63 文字です。

説明

filter-policy import コマンドは受信するルートをフィルタするために RIPng を設定します。フィルタされなかったルートのみ受信することができます。

undo filter-policy import コマンドは設定を削除します。

拡張 IPv6 ACL（設定範囲は 3000～3999 です）を参照するため、以下の方法の 1 つを使用して IPv6 ACL を設定します。

- 指定された宛先のルートの許可/拒否を行う場合、**rule** [*rule-id*] { **deny** | **permit** } **ipv6 source** *sour sour-prefix* コマンドを使用します。
- 指定された宛先とプレフィックスのルートの許可/拒否を行う場合、**rule** [*rule-id*] { **deny** | **permit** } **ipv6 source** *sour sour-prefix* **destination** *dest dest-prefix* コマンドを使用します。

source はルートの宛先アドレスを指定します。**destination** はルートのプレフィックスを指定します。指定されたプレフィックスは隣接している必要があります。隣接していない場合、プレフィックスの設定は適用されません。

例

受信する RIPng アップデートをフィルタするため、IPv6 プレフィックスリストを使用します。

<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

受信するルートをフィルタするため、IPv6 ACL3000 を設定し、ルート 2001::1/128 のみ許可できるようにします。

<Switch> system-view

[Switch] acl ipv6 number 3000

[Switch-acl6-adv-3000] rule 10 permit ipv6 source 2001::1 128 destination ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff 128

[Switch-acl6-adv-3000] rule 100 deny ipv6

[Switch-acl6-adv-3000] quit

[Switch] ripng 100

[Switch-ripng-100] filter-policy 3000 import

7.1.11 graceful-restart

Syntax

graceful-restart

undo graceful-restart

デフォルト

無効

View

RIPng view

定義済みユーザロール

network-admin

説明

graceful-restart コマンドは、RIPng にグレースフルリスタート(GR)を有効にします。

undo graceful-restart コマンドは、RIPng の GR を無効にします。

RIPng GR と RIPng NSR は互いに排他的です。**graceful-restart** コマンドと **non-stop-routing** コマンドは同時に設定しないでください。

例

RIPng プロセス 1 に GR を有効にします。

<Switch> system-view

[Switch] ripng 1

[Switch-ripng-1] graceful-restart

7.1.12 import-route

Syntax

import-route *protocol* [*process-id*] [**cost** *cost* | **route-policy** *route-policy-name*]*

undo import-route *protocol* [*process-id*]

デフォルト

無効

View

RIPng view

定義済みユーザロール

network-admin

パラメータ

protocol: 指定されたルーティングプロトコルから再配信された RIPng ルートをフィルタします。再配信されたルートはダイレクト、OSPFv3、RIPng、スタティックがあります。

process-id: RIPng プロセスの ID を指定します。設定範囲は 1～65535 です。デフォルトは 1 です。*process-id* はプロトコルが OSPFv3 または RIPng であるときのみ有効です。

cost *cost*: 再配信されるルートのメトリックを指定します。設定範囲は 0～16 です。デフォルトは 0 です。

route-policy *route-policy-name*: ルーティングポリシーの名前を指定します。設定範囲は 1～63 です。大文字、小文字を区別します。

説明

import-route コマンドは別のルーティングプロトコルからのルートを再配信することを有効にします。

undo import-route コマンドはルートの再配信を無効にします。

例

RIPng にスタティックルートを再配信し、再配信されたルートのメトリックを 7 に設定します。

<Switch> system-view

[Switch] ripng 100

[Switch-ripng-100] import-route static cost 7

7.1.13 maximum load-balancing

Syntax

maximum load-balancing *number*

undo maximum load-balancing

デフォルト

8

View

RIPng view

定義済みユーザロール

network-admin

パラメータ

number: ECMP ルートの最大数を指定します。1 を指定した場合、RIPng はロードバランスの動作をしません。

説明

maximum load-balancing コマンドは、ロードバランスをとるために ECMP（イコールコストマルチパス）ルートの最大数を指定します。

undo maximum load-balancing コマンドは、設定をデフォルトに戻します。

例

ECMP)ルートの最大数を 2 と設定します。

<Switch> system-view

[Switch] ripng 100

[Switch-ripng-100] maximum load-balancing 2

関連コマンド

max-ecmp-num

7.1.14 non-stop-routing

Syntax

non-stop-routing

undo non-stop-routing

デフォルト

無効

View

RIPng view

定義済みユーザロール

network-admin

説明

non-stop-routing コマンドは RIPng NSR を有効にします。

undo non-stop-routing コマンドは RIPng NSR を無効にします。

RIPng プロセスに対して有効な RIPng NSR は、そのプロセスに対してのみ有効になります。複数の RIPng プロセスが存在する場合は、各プロセスの RIPng NSR を有効にします。

RIPng NSR と RIPng GR は互いに排他的です。**non-stop-routing** コマンドと **graceful-restart** コマンドは同時に設定しないでください。

例

RIPng プロセス 1 の NSR を有効にします。

<Switch> system-view

[Switch] ripng 1

[Switch-ripng-1] non-stop-routing

7.1.15 preference

Syntax

preference { *preference* | **route-policy** *route-policy-name* } *

undo preference

デフォルト

100

View

RIPng view

定義済みユーザロール

network-admin

パラメータ

preference: RIPng ルートの優先順位を指定します。設定範囲は 1～255 です。値が小さいほど優先順位は高くなります。

route-policy *route-policy-name*: ルーティングポリシーを指定します。設定範囲は 1～63 です。

説明

preference コマンドは RIPng ルートの優先順位を指定します。

undo preference コマンドはデフォルトに戻します。

route-policy を使用してルーティングポリシーを設定すると、そのルーティングポリシーに一致する RIPng ルートに、指定した優先順位を設定することができます。

- ルーティングポリシーによる優先順位が、すべての一致する RIPng ルートへ適用されます。その他のルートの優先順位は、**preference** コマンドで設定されます。
- ルーティングポリシーによって優先順位が設定されていない場合、**preference** コマンドですべての RIPng ルートの優先順位が設定されます。

例

RIPng ルートの優先順位を 120 に設定します。

<Switch> system-view

[Switch] ripng 100

[Switch-ripng-100] preference 120

7.1.16 reset ripng process

Syntax

reset ripng *process-id* **process**

View

User view

定義済みユーザロール

network-admin

パラメータ

process-id: RIPng プロセスの ID を指定します。設定範囲は 1～65535 です。

説明

reset ripng process コマンドは RIPng プロセスをリセットします。

このコマンドを実行したのち、動作を確認するために、確認画面が表示されます。

例

RIPng プロセス 100 をリセットします。

<Switch> reset ripng 100 process

```
Reset RIPng process? [Y/N]:y
```

7.1.17 reset ripng statistics

Syntax

reset ripng *process-id* **statistics**

View

User view

定義済みユーザロール

network-admin

network-operator

パラメータ

process-id: RIPng プロセスの ID を指定します。設定範囲は 1～65535 です。

説明

reset ripng statistics コマンドは RIPng プロセスの統計情報を削除します。

例

RIPng プロセス 100 の統計情報を削除します。

<Switch> reset ripng 100 statistics

7.1.18 ripng

Syntax

ripng [*process-id*] [**vpn-instance** *vpn-instance-name*]

undo ripng [*process-id*]

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

パラメータ

process-id: RIPng プロセスの ID を指定します。設定範囲は 1～65535 です。デフォルトは 1 です。

vpn-instance *vpn-instance-name*: VPN インスタンスを名前で指定します。大文字小文字を区別し、設定範囲は 1～31 文字です。このオプションを指定しない場合、RIPng プロセスはパブリックネットワークで動作します。

説明

ripng コマンドは RIPng を有効にし、RIPng view に移行します。

undo ripng コマンドは RIPng を無効にします。

グローバルの RIPng パラメータを設定する前に、必ず RIPng プロセスを有効にしてください。この制限は、インタフェースの RIPng パラメータの設定には適用しません

RIPng プロセスを無効にすると設定されたインタフェースの RIPng パラメータは、無効になります

例

RIPng プロセス 100 を作成し、RIP view に移行します。

<Switch> system-view

[Switch] ripng 100

[Switch-ripng-100]

7.1.19 ripng default-route

Syntax

ripng default-route { **only** | **originate** } [**cost** *cost*]

undo ripng default-route

デフォルト

RIPng プロセスはデフォルトルートを配信しません。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

only: デフォルト IPv6 ルート（::/0）のみ配信します。

originate: デフォルト IPv6 ルート（::/0）と他のルートを配信します。

cost: デフォルトルートのコストを指定します。設定範囲は 1～15 です。デフォルトは 1 です。

説明

ripng default-route コマンドは指定したメトリックのデフォルトルートを配信する RIPng インタフェースを設定します。

undo ripng default-route コマンドはデフォルトルートを送信する RIPng インタフェースを無効にします。

このコマンドはローカル IPv6 ルーティングテーブルにデフォルトルートが存在するにも関わらず、ルートアップデートの RIPng デフォルトルートを配信するインタフェースを有効にします。

デフォルトルートを配信するように設定されたインタフェースは、RIPng ネイバからデフォルトルートを受信しません。

例

VLAN インタフェース 100 にデフォルトルートのみを配信するように RIPng を設定します。

<Switch> system-view

[Switch] interface vlan-interface 100

[Switch-Vlan-interface100] ripng default-route only

VLAN インタフェース 101 にデフォルトルートと他のルートを配信するように RIPng を設定します。

<Switch> system-view

[Switch] interface vlan-interface 101

[Switch-Vlan-interface101] ripng default-route originate

7.1.20 ripng enable

Syntax

ripng *process-id* **enable**

undo ripng enable

デフォルト

無効

View

Interface view

定義済みユーザロール

network-admin

パラメータ

process-id: RIPng プロセスの ID を指定します。設定範囲は 1～65535 です。

説明

ripng enable コマンドはインタフェースで RIPng を有効にします。

undo ripng enable コマンドはインタフェースで RIPng を無効にします。

例

VLAN インタフェース 100 で RIPng を有効にします。

<Switch> system-view

[Switch] interface vlan-interface 100

[Switch-Vlan-interface100] ripng 100 enable

7.1.21 ripng metricin

Syntax

ripng metricin *value*

undo ripng metricin

デフォルト

0

View

Interface view

定義済みユーザロール

network-admin

パラメータ

value: 受信ルートに加える追加メトリックを指定します。設定範囲は 0～16 です。

説明

ripng metricin コマンドは受信 RIPng ルートにメトリックを追加するようにインタフェースを設定します。

undo ripng metricin コマンドはデフォルトに戻します。

例

VLAN インタフェース 100 で、受信 RIPng ルートにメトリック 12 を追加します。

<Switch> system-view

[Switch] interface vlan-interface 100

[Switch-Vlan-interface100] ripng metricin 12

7.1.22 ripng metricout

Syntax

ripng metricout *value*

undo ripng metricout

デフォルト

1

View

Interface view

定義済みユーザロール

network-admin

パラメータ

value: 送信ルートに加える追加メトリックを指定します。設定範囲は 1～16 です。

説明

ripng metricout コマンドは送信 RIPng ルートにメトリックを追加するようにインタフェースを設定します。

undo ripng metricout コマンドはデフォルトに戻します。

例

VLAN インタフェース 100 で、送信 RIPng ルートにメトリック 12 を追加します。

<Switch> system-view

[Switch] interface vlan-interface 100

[Switch-Vlan-interface100] ripng metricout 12

7.1.23 ripng poison-reverse

Syntax

ripng poison-reverse

undo ripng poison-reverse

デフォルト

無効

View

Interface view

定義済みユーザロール

network-admin

説明

ripng poison-reverse コマンドはポイズンリバースを有効にします。

undo ripng poison-reverse コマンドはポイズンリバースを無効にします。

例

VLAN インタフェース 100 で RIPng アップデートメッセージのポイズンリバースを有効にします。

<Switch> system-view

[Switch] interface vlan-interface 100

[Switch-Vlan-interface100] ripng poison-reverse

7.1.24 ripng split-horizon

Syntax

ripng split-horizon

undo ripng split-horizon

デフォルト

有効

View

Interface view

定義済みユーザロール

network-admin

説明

ripng split-horizon コマンドはスプリットホライズンを有効にします。

undo ripng split-horizon コマンドはスプリットホライズンを無効にします。

スプリットホライズンはルーティングループを防ぎます。この機能を無効にする場合、必要不可欠であるかどうかを確認してください。

スプリットホライズンとポイズンリバースの両方が有効である場合、ポイズンリバースのみが適用されます。

例

VLAN インタフェース 100 でスプリットホライズンを有効にします。

<Switch> system-view

[Switch] interface vlan-interface 100

[Switch-Vlan-interface100] ripng split-horizon

7.1.25 ripng summary-address

Syntax

ripng summary-address *ipv6-address prefix-length*

undo ripng summary-address *ipv6-address prefix-length*

デフォルト

インタフェースを通して配信される集約ネットワークは設定されません。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

ipv6-address: 集約ルートの宛先 IPv6 アドレスを指定します。

prefix-length: 集約ルートの宛先 IPv6 アドレスのプレフィックス長を指定します。設定範囲は 0～128 です。プレフィックスが連続した 1 の個数を示します。ネットワーク ID を定義します。

説明

ripng summary-address コマンドはインタフェースで集約ルートを配信するように設定します。

undo ripng summary-address コマンドは集約ルートを削除します。

集約ネットワーク上のネットワークは配信されません。集約ルートのコストは集約ルートの中でもっとも低いコストです。

例

VLAN インタフェース 100 にプレフィックス長が 64 ビットの IPv6 アドレスを割り当てます。そして 35 ビットのプレフィックスを集約するように設定します。

<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

7.1.26 timers

Syntax

timers { **garbage-collect** *garbage-collect-value* | **suppress** *suppress-value* | **timeout** *timeout-value* | **update** *update-value* } *

undo timers { **garbage-collect** | **suppress** | **timeout** | **update** } *

デフォルト

ガーベッジコレクトタイマが 120 秒、サプレスタイマが 120 秒、タイムアウトタイマが 180 秒、アップデートタイマが 30 秒です。

View

RIPng view

定義済みユーザロール

network-admin

パラメータ

garbage-collect-value: ガーベッジコレクト時間を指定します。設定範囲は 1～86400 秒です。

suppress-value: サプレス状態（到達不能状態）にとどまる時間のサプレスタイマを指定します。設定範囲は 0～86400 秒です。

timeout-value: エージングタイムを指定します。設定範囲は 1～86400 秒です。

update-value: アップデートタイマを指定します。設定範囲は 1～86400 秒です。

説明

timers コマンドは RIPng タイマを設定します。

undo timers コマンドはデフォルトに戻します。

RIPng は以下のタイマを使用します。

- **アップデートタイマ**－ルーティングテーブルのアップデート間隔を指定します。
- **タイムアウトタイマ**－ルートエージングタイムを指定します。もしエージング時間内にルートのアップデートを受信しない場合、RIPng はルートのメトリックを 16 に設定します。
- **サプレスタイマ**－RIPng ルートがサプレス状態(到達不能状態)にとどまる時間を指定します。ルートのメトリックが 16 のとき、ルータはサプレス状態になります。RIPng は停止した到達不能ルートをアップデートされたルートに置き換えます。このアップデートされたルートはサプレスタイマが満了する前に同一の隣接装置から受信したルートで、メトリックは 16 より小さい値を持ちます。

- **ガーベッジコレクトタイマ**—ルートのメトリックが 16 になる時点から、そのルートがルーティングテーブルから削除されるまでの間隔を指定します。RIPng はメトリックが 16 のルートを配信します。タイマの時間が過ぎた後も、そのルートへのルーティングアップデートが行われない場合、RIPng はルーティグテーブルからルートを削除します。

これらのタイマの値は特に必要がない限りデフォルトから変更しないことを推奨します。

タイマの値はネットワークのすべてのルータで統一する必要があります。

例

アップデートタイマを 5 秒、タイムアウトタイマを 15 秒、サプレスタイマを 15 秒、ガーベッジコレクトタイマを 30 秒に設定します。

<Switch> system-view

[Switch] ripng 1

[Switch-ripng-1] timers update 5 timeout 15 suppress 15 garbage-collect 30

目次

このセクションのページは **5-x-x** です。

8 章 OSPFv3 8-1
8.1 OSPFv3 設定コマンド 8-1
8.1.1 abr-summary (OSPFv3 area view) 8-1
8.1.2 area 8-2
8.1.3 bandwidth-reference 8-3
8.1.4 default-cost (OSPFv3 area view) 8-4
8.1.5 default-route-advertise (OSPFv3 view) 8-5
8.1.6 display ospfv3 8-6
8.1.7 display ospfv3 abr-asbr 8-13
8.1.8 display ospfv3 abr-summary 8-14
8.1.9 display ospfv3 asbr-summary 8-16
8.1.10 display ospfv3 graceful-restart 8-19
8.1.11 display ospfv3 interface 8-24
8.1.12 display ospfv3 lsdb 8-27
8.1.13 display ospfv3 nexthop 8-32
8.1.14 display ospfv3 non-stop-routing 8-33
8.1.15 display ospfv3 peer 8-34
8.1.16 display ospfv3 request-queue 8-38
8.1.17 display ospfv3 retrans-queue 8-40
8.1.18 display ospfv3 routing 8-42
8.1.19 display ospfv3 statistics 8-44
8.1.20 display ospfv3 vlink 8-46
8.1.21 filter (OSPFv3 area view) 8-47
8.1.22 filter-policy export (OSPFv3 view) 8-48
8.1.23 filter-policy import (OSPFv3 view) 8-50
8.1.24 graceful-restart enable 8-52
8.1.25 graceful-restart helper enable 8-53
8.1.26 graceful-restart helper strict-lsa-checking 8-54
8.1.27 graceful-restart interval 8-54
8.1.28 import-route (OSPFv3 view) 8-55
8.1.29 log-peer-change 8-57
8.1.30 lsa-generation-interval 8-58
8.1.31 maximum load-balancing (OSPFv3 view) 8-59
8.1.32 non-stop-routing 8-60
8.1.33 ospfv3 8-60
8.1.34 ospfv3 area 8-61

8.1.35 ospfv3 bfd enable 8-62
8.1.36 ospfv3 cost....8-63
8.1.37 ospfv3 dr-priority....8-64
8.1.38 ospfv3 mtu-ignore....8-65
8.1.39 ospfv3 network-type....8-66
8.1.40 ospfv3 peer....8-67
8.1.41 ospfv3 timer dead....8-68
8.1.42 ospfv3 timer hello....8-69
8.1.43 ospfv3 timer poll....8-70
8.1.44 ospfv3 timer retransmit....8-71
8.1.45 ospfv3 trans-delay....8-72
8.1.46 preference....8-72
8.1.47 reset ospfv3 process....8-73
8.1.48 reset ospfv3 redistribution....8-74
8.1.49 reset ospfv3 statistics....8-75
8.1.50 router-id....8-75
8.1.51 silent-interface(OSPFv3 view)....8-76
8.1.52 snmp-agent trap enable ospfv3....8-77
8.1.53 spf-schedule-interval....8-78
8.1.54 stub (OSPFv3 area view)....8-80
8.1.55 vlink-peer (OSPFv3 area view)....8-81

8章 OSPFv3

8.1 OSPFv3設定コマンド

8.1.1 abr-summary (OSPFv3 area view)

Syntax

abr-summary *ipv6-address prefix-length* [**not-advertise**] [**cost** *value*]

undo abr-summary *ipv6-address prefix-length*

デフォルト

設定なし

View

OSPFv3 area view

定義済みユーザロール

network-admin

パラメータ

ipv6-address: ルート集約の宛先 IPv6 アドレスを指定します。

prefix-length: 宛先 IPv6 アドレスのプレフィックス長を指定します。設定範囲は 0～128 です。プレフィックスが連続する 1 の数を指定し、ネットワーク ID を定義します。

not-advertise: 集約 IPv6 ルートを配信しません。指定しない場合、IPv6 集約ルートを配信します。

cost *value*: 集約ルートのコストを指定します。設定範囲は 1～16777215 です。デフォルトは集約されたルートの中で一番大きい値を持つコストです。

説明

abr-summary コマンドは ABR（area border router）のルート集約を設定します。

undo abr-summary コマンドは設定を削除します。

このコマンドは複数の連続するネットワークを 1 つのネットワークに集約するため、ABR でのみ有効です。

指定したルートを配信する ABR を有効にする場合、**undo abr-summary** コマンドを使用します。

例

エリア 1 のネットワーク 2000:1:1:1::/64、2000:1:1:2::/64 を 2000:1:1::/48 に集約します。

<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

8.1.2 area

Syntax

area *area-id*

undo area *area-id*

デフォルト

設定なし

View

OSPFv3 view

定義済みユーザロール

network-admin

パラメータ

area-id: エリアを IPv4 アドレスあるいは 10 進数の整数のエリア ID で指定します。10 進数の整数の設定範囲は 0～4294967295 です。この 10 進数の整数はシステムで IPv4 アドレスの形式に変換されます。

説明

area コマンドは OSPFv3 エリアを作成し、OSPFv3 area view に移行します。

undo area コマンドは OSPFv3 エリアを削除します。

例

OSPFv3 エリア 0 を作成し、OSPFv3 area view に移行します。

<Switch> system-view

[Switch] ospfv3 1

[Switch-ospfv3-1] area 0

[Switch-ospfv3-1-area-0.0.0.0]

8.1.3 bandwidth-reference

Syntax

bandwidth-reference *value*

undo bandwidth-reference

デフォルト

100 Mbps

View

OSPFv3 view

定義済みユーザロール

network-admin

パラメータ

value: リンクコストの計算に必要な帯域幅の基準値を指定します。設定範囲は 1～4294967 Mbps です。

説明

bandwidth-reference コマンドはリンクコストの計算に必要な帯域幅の基準値を設定します。

undo bandwidth-reference コマンドはデフォルトに戻します。

インタフェースの OSPFv3 のコストを以下の方法の 1 つで設定します。

- interface view でコストを設定します。
- 帯域幅の基準値を設定します。OSPFv3 は以下の計算式を使用して自動でコストを計算します。

  OSPFv3 のコスト＝帯域幅の基準値（100Mbps）／インタフェースの帯域幅（Mbps）

  - 計算した値が 65535 よりも大きい場合、コストは 65535 となります。
  - 計算した値が 1 よりも小さい場合、コストは 1 となります。

インタフェースでコストが設定されていない場合、OSPFv3 は自動でインタフェースのコストを計算します。

例

帯域幅の基準値を 1000 Mbps に設定します。

<Switch> system-view

[Switch] ospfv3 1

[Switch-ospfv3-1] bandwidth-reference 1000

8.1.4 default-cost (OSPFv3 area view)

Syntax

default-cost *cost*

undo default-cost

デフォルト

1

View

OSPFv3 area view

定義済みユーザロール

network-admin

パラメータ

cost: スタブあるいは NSSA エリアに配信されるデフォルトルートのコストを指定します。設定範囲は 0～16777214 です。

説明

default-cost コマンドはスタブあるいは NSSA エリアに配信されるデフォルトルートのコストを設定します。

undo default-cost コマンドはデフォルトに戻します。

このコマンドはスタブエリアの ABR、あるいは NSSA エリアの ABR/ASBR でのみ適用します。

例

スタブエリアとしてエリア 1 を設定し、スタブエリアに配信されるデフォルトルートのコストを 60 に設定します。

<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

関連コマンド

- **nssa (OSPFv3 area view)**
- **stub (OSPFv3 area view)**

8.1.5 default-route-advertise (OSPFv3 view)

Syntax

default-route-advertise [[**always** | **permit-calculate-other**] | **cost** *cost* | **route-policy** *route-policy-name* | **type** *type*] *

undo default-route-advertise

デフォルト

設定なし

View

OSPFv3 view

定義済みユーザロール

network-admin

パラメータ

always: ルーティングテーブルにデフォルトルートが存在するかどうかにかかわらず、AS 外部 LSA（Type-5 LSA）のデフォルトルートを OSPFv3 ルーティングドメインに作成します。指定しない場合、現在の IP ルーティングテーブルに存在するときのみ、AS 外部 LSA（Type-5 LSA）のデフォルトルートを OSPFv3 ルーティングドメインに作成します。

permit-calculate-other: ほかのルータから受信したデフォルトルートを計算するために OSPFv3 を有効にします。指定しない場合、OSPFvv3 はほかのルータからデフォルトルートを計算しません。ルータが AS 外部 LSA のデフォルトルートを OSPFv3 ルーティングドメインに作成しない場合、ルータはほかのルータからデフォルトルートを計算します。OSPFv3 は **permit-calculate-other** パラメータが指定されているかどうかにかかわらず、ルートを計算します。

cost *cost*: デフォルトルートのコストを指定します。設定範囲は 0～16777214 です。デフォルトは 1 です。

route-policy *route-policy-name*: ルーティングポリシーの名前を指定します。設定範囲は 1～63 です。大文字、小文字を区別します。ルーティングテーブルにデフォルトルートが存在し、指定したルーティングポリシーが一致する場合、AS 外部 LSA のデフォルトルートを OSPFv3 ルーティングドメインに配信します。ルーティングポリシーは AS 外部 LSA の値を変更します。**route-policy** パラメータと同時に **always** パラメータが指定された場合、指定したルーティングポリシーが一致するとき、AS 外部 LSA のデフォルトルートを OSPFv3 ルーティングドメインに配信します。このコマンドはルーティングテーブルにデフォルトルートが存在するかどうかにかかわらず、ルートを作成します。ルーティングポリシーは AS 外部 LSA の値を変更します。

type *type*: AS 外部 LSA のタイプを指定します。設定範囲は 1 あるいは 2 です。デフォルトは 2 です。

説明

default-route-advertise コマンドはデフォルトルートを OSPFv3 ルーティングドメインに再配信します。

undo default-route-advertise コマンドはデフォルトに戻します。

このコマンドは AS 外部 LSA のデフォルトルートを再配信します。**import-route** コマンドでデフォルトルートを再配信することはできません。ローカルのルーティングテーブルにデフォルトルートがない場合、**always** パラメータを適用する必要があります。

例

#デフォルトルートを OSPFv3 ルーティングドメインに作成します。（ローカルのルーティングテーブルにデフォルトルートがあるかどうかにかかわりなく作成します）

<Switch> system-view

[Switch] ospfv3 1

[Switch-ospfv3-1] default-route-advertise always

関連コマンド

import-route (OSPFv3 view)

8.1.6 display ospfv3

Syntax

display ospfv3 [*process-id*] [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

process-id: OSPFv3 プロセスを指定します。設定範囲は 1～65535 です。指定しない場合、すべての OSPFv3 プロセスの情報を表示します。

verbose: OSPFv3 プロセスの詳細情報を表示します。指定しない場合、OSPFv3 プロセスの概要情報を表示します。

説明

display ospfv3 コマンドは OSPFv3 プロセスの情報を表示します。

例

すべての OSPFv3 プロセスの詳細情報を表示します。

<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 while BGP is converging 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
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
IPsec profile name: Profile000
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
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
```

表 8-1 コマンド出力

フィールド	説明
OSPFv3 Process 1 with Router ID 1.1.1.1	OSPFv3プロセスが1で、ルータIDが1.1.1.1です。
Router type	ルータタイプです。 ● **ABR**－ABRタイプです。 ● **ASBR**－ASBRタイプです。 ● **NSSA**－NSSAタイプです。 ● **Null**－ルータタイプがありません。
Route tag	OSPFv3プロセスに再配信されたルートのタグです。
Route tag check	OSPFv3プロセスのOSPFv3 LSAのルーティングタグが有効かどうかを示します。
Multi-VPN-Instance	OSPFv3プロセスがPEあるいはマルチVPNインスタンスをサポートしているかどうかを示します。 ● **Multi-VPN-Instance: Disabled**－プロセスはマルチVPNインスタンスをサポートしていません。 ● **Multi-VPN-Instance: Enabled**－プロセスはマルチVPNインスタンスをサポートしています。 ● **PE Router, Multi-VPN-Instance: Enabled**－ローカル装置がPEです。
DN-bit check	OSPFv3プロセスのOSPFv3 LSAのDNビットが有効かどうかを示します。
DN-bit set	OSPFv3プロセスのOSPFv3 LSAのDNビットが設定されているかどうかを示します。

フィールド	説明
Condition	ルータがスタブルータとして動作している時間です。 ● Alway状態です。 ● *xxx*秒間、起動します。*xxx*はユーザによって指定されます。
State	スタブルータの状態です。 ● **Active**－アクティブです。 ● **Inactive**－アクティブではありません。
SPF-schedule-interval	SPFを計算する間隔です。
Transmit pacing	LSUの転送レートです。 ● **Interval**–インタフェースのLSU転送間隔を指定します。 ● **Count**–毎回、LSUパケットを送信する最大数を指定します。
Default ASE parameters	デフォルトASEパラメータです。**Tag**は再配信されたルートのルーティングタグを示します。
Route preference	内部ルートの優先順位です。
ASE route preference	外部ルートの優先順位です。
LSA originated count	最初のLSAの数です。
LSA received count	受信したLSAの数です。
Area count	エリアの総数です。
Stub area Count	スタブエリアの数です。
NSSA area Count	NSSAエリアの数です。
ExChange/Loading neighbors	ExChange/Loading状態の隣接です。
Calculation trigger type	ルート計算の起動タイプです。 ● **Full**–すべてのルートの計算が開始します。 ● **Area topology change**－エリアのトポロジが変更します。 ● **Intra router change**－incremental内部エリアのルートが変更します。 ● **ASBR change**－incrementalのASBRルートが変更します。 ● **Full IP prefix**－すべてのIPプレフィックスの計算が開始します。 ● **Nexthop calculation**–ネクストホップの計算が開始します。 ● **N/A**–ルートの計算が開始しません。

フィールド	説明
Current calculation type	現在のルート計算のタイプです。 ● SPFの計算です。 ● **Intra router calculation**－エリア内のルート計算です。 ● **ASBR calculation**–エリア間のASBRルート計算です。 ● **Inc intra router**－Incrementalエリア内のルート計算です。 ● **Inc ASBR calculation**－Incrementalエリア間のASBRルート計算です。 ● **N/A**–ルート計算が開始しません。
Current calculation phase	現在のルート計算のフェーズです。 ● **Calculation area topology**–エリアトポロジを計算しています。 ● **Calculation router**–ルータのルートを計算しています。 ● **Calculation ASBR**–ASBRのルートを計算しています。 ● **Calculation end**–計算の終了フェーズです。 ● **N/A**–ルート計算が開始していません。
Redistribute timer	ルートの再配信タイマの状態です。onあるいはoffがあります。
Redistribute schedule type	ルートの再配信のスケジュールタイプです。 ● **RIB**–RIBテーブルを通してルートを再配信します。 ● **Self**–ルーティングテーブルを通してルートを再配信します。 ● **N/A**–ルートの再配信が開始していません。
Redistribute route count	再配信されたルートの数です。
Process reset state	プロセスのリセット状態です。 ● **N/A**－プロセスがリセットしていません。 ● **Under reset**－プロセスがリセットしています。 ● **Under RIB smooth**－プロセスがRIBの同期化を行っています。
Current reset type	現在のプロセスリセットタイプです。 ● **N/A**－プロセスがリセットしていません。 ● **GR quit**－GRが異常終了したとき、通常リセットを行います。 ● **Delete**－OSPFv3プロセスを削除します。 ● **VPN delete**－VPNを削除します。 ● **Undo router-id**–ルータIDを削除します。 ● **Set router-id**–ルータIDを設定します。

フィールド	説明
Next reset type	次回のプロセスリセットタイプです。 • **N/A**－プロセスがリセットしていません。 • **GR quit**－GRが異常終了したとき、通常リセットを行います。 • **Delete**－OSPFv3プロセスを削除します。 • **Undo router-id**–ルータIDを削除します。 • **Set router-id**–ルータIDを設定します。
Reset prepare message replied	リセット準備のメッセージを応答するモジュールです。 • **P**－隣接メンテナンスモジュールです。 • **L**－LSDB同期モジュールです。 • **C**－ルート計算モジュールです。 • **R**－ルート再配信モジュールです。
Reset process message replied	リセットプロセスメッセージを応答するモジュールです。 • **P**－隣接メンテナンスモジュールです。 • **L**－LSDB同期モジュールです。 • **C**－ルート計算モジュールです。 • **R**－ルート再配信モジュールです。

Reset phase of module	各モジュールのリセットフェーズです。
	• LSDB 同期(S) モジュールです。
	  • **N/A**－リセットしません。
	  • **Delete ASE**–すべてのASE LSAを削除します。
	  • **Delete area LSA**–エリアからのLSAを削除します。
	  • **Delete area IF**–エリアからのインタフェースを削除します。
	• ルート計算(C) モジュールです。
	  • **N/A**－リセットしません。
	  • **Delete topology**－エリアトポロジを削除します。
	  • **Delete router**－ルータのルートを削除します。
	  • **Delete ASBR**–ASBRルートを削除します。
	• ルート再配信(R) モジュールです。
	  • **N/A**－リセットしません。
	  • **Delete import**－再配信されたルートを削除します。

IPsec profile name	インタフェースに適用されたIPsecプロファイルです。
Created by Vlink	仮想リンクを通して作成されたエリアです。

フィールド	説明
7/5 translator state	Type-7 LSAからType-5 LSAに変換する状態です。状態は以下の1つになることができます ● **Enabled**ー変換はコマンドによって指定されます。 ● **Elected**ー変換は選択によって定義されます。 ● **Disabled**–装置は変換しません。
7/5 translate stability timer interval	Type-7 LSAからType-5 LSAに変換する安定間隔です。単位は秒です。

8.1.7 display ospfv3 abr-asbr

Syntax

display ospfv3 [*process-id*] **abr-asbr**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

process-id: OSPFv3 プロセスを指定します。設定範囲は 1～65535 です。指定しない場合、すべての OSPFv3 プロセスの ABR、ASBR へのルート情報を表示します。

説明

display ospfv3 abr-asbr コマンドは OSPFv3 ABR あるいは ASBR へのルートを表示します。

例

OSPFv3 ABR あるいは ASBR へのルートを表示します。

<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
 NextHop     :FE80:1:1::1                      Cost     : 1

 Destination :1.1.1.3                          Rtr Type : ASBR
```

```
Area        :0.0.0.0                          Path Type: Intra
NextHop     :FE80:2:1::1                       Cost     : 1
```

表 8-2 コマンド出力

フィールド	説明
OSPFv3 Process 1 with Router ID 1.1.1.1	OSPFv3プロセスが1で、ルータIDが1.1.1.1です。
Destination	ABRあるいはASBRのルータIDです。
Rtr Type	ルータタイプです。ABRあるいはASBRがあります。
Area	ネクストホップのエリアIDです。
Path Type	ABRあるいはASBRへのルートタイプです。 ● **Intra**–内部エリアルートです。 ● **Inter**–外部エリアルートです。
NextHop	ネクストホップアドレスです。
Cost	ルータからABRあるいはASBRへのコストです。

8.1.8 display ospfv3 abr-summary

Syntax

display ospfv3 [*process-id*] [**area** *area-id*] **abr-summary** [*ipv6-address prefix-length*] [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

process-id: OSPFv3 プロセスを指定します。設定範囲は 1～65535 です。指定しない場合、すべての OSPFv3 プロセスの ABR の集約ルート情報を表示します。

area *area-id*: OSPFv3 エリアを IP アドレスあるいは 10 進数の整数のエリア ID で指定します。10 進数の整数の設定範囲は 0～4294967295 です。この 10 進数の整数はシステムで IP アドレスの形式に変換されます。指定しない場合、すべての OSPFv3 エリアの ABR の集約ルート情報を表示します。

ipv6-address prefix-length: IPv6 アドレスを指定します。*ipv6-address* は IPv6 プレフィックスを指定します。*prefix-length* はプレフィックス長を指定します。設定範囲は 0～128 です。指定しない場合、ABR のすべての集約ルートの情報を表示します。

verbose: ABR の集約ルートの詳細情報を表示します。指定しない場合、ABR の集約ルートの概要情報を表示します。

説明

display ospfv3 abr-summary コマンドは OSPFv3 ABR の集約ルートの情報を表示します。

例

OSPFv3 プロセス 1 の ABR の集約ルートの集約ルートの概要情報を表示します。

<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
```

表 8-3 コマンド出力

フィールド	説明
Total summary addresses	集約ルートの総数です。
Area	集約ルートが所属しているエリアです。
Prefix	集約ルートのプリフィックスです。
Status	集約ルートの配信状態です。
NULL0	Null 0へのルートです。
Cost	集約ネットワークへのコストです。
Routes count	集約されたルート数です。

OSPFv3 プロセス 1 の ABR の集約ルータの詳細情報を表示します。

<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
```

表 8-4 コマンド出力

フィールド	説明
Destination	集約されたルートの宛先アドレスです。
Metric	集約されたルートのメトリックです。

8.1.9 display ospfv3 asbr-summary

Syntax

display ospfv3 [*process-id*] **asbr-summary** [*ipv6-address prefix-length*] [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

process-id: OSPFv3 プロセスを指定します。設定範囲は 1～65535 です。指定しない場合、すべての OSPFv3 プロセスの ASBR の集約ルート情報を表示します。

ipv6-address prefix-length: IPv6 アドレスを指定します。*ipv6-address* は IPv6 プレフィックスを指定します。*prefix-length* はプレフィックス長を指定します。設定範囲は 0～128 です。指定しない場合、ASBR のすべての集約ルートの情報を表示します。

verbose: ASBR の集約ルートの詳細情報を表示します。指定しない場合、ABR の集約ルートの概要情報を表示します。

説明

display ospfv3 asbr-summary コマンドは ASBR の集約ルート情報を表示します。

例

OSPFv3 プロセス 1 の ASBR の集約ルートの概要情報を表示します。

<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
```

表 8-5 コマンド出力

フィールド	説明
Total summary addresses	集約ルートの総数です。
Prefix	集約ルートのプレフィックスとプレフィックス長です。
Status	集約ルートの配信状態です。 ● **Advertise**–集約ルートが配信されました。 ● **Not-advertise**–集約ルートが配信されていません。
NULL0	Null 0へのルートの状態です。 ● **Active**－アクティブ状態です。 ● **Inactive**－アクティブ状態ではありません。
Cost	集約ルートのコストです。 ● **Configured**－設定されています。 ● **Not configured**－設定されていません。
Tag	集約ルートのタグです。 ● **Configured**－設定されています。 ● **Not configured**－設定されていません。

フィールド	説明
Nssa-only	NSSA-ONLY属性が設定されているかどうかを示します。 ● **Configured**－設定されています。 ● **Not configured**－設定されていません。
Routes count	集約されたルートの数です。

OSPFv3 プロセス 1 の ASBR 集約ルートの詳細情報を表示します。

<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
```

表 8-6 コマンド出力

フィールド	説明
Destination	集約されたルートのプレフィックスとプレフィックス長です。
Protocol	ルートを再配信するルーティングプロトコルです。
Process	ルートを再配信するルーティングプロトコルのプロセスです。
Type	集約されたルートのタイプです。
Metric	集約されたルートのメトリックです。

8.1.10 display ospfv3 graceful-restart

Syntax

display ospfv3 [*process-id*] **graceful-restart** [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

process-id: OSPFv3 プロセスを指定します。設定範囲は 1～65535 です。指定しない場合、すべての OSPFv3 プロセスの GR 情報を表示します。

verbose: GR の詳細情報を表示します。指定しない場合、GR の概要情報を表示します。

説明

display ospfv3 graceful-restart コマンドは GR 情報を表示します。

例

すべての OSPFv3 プロセス（GR リスタータ）の GR 情報を表示します。

<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
```

表 8-7 コマンド出力

フィールド	説明
OSPFv3 Process 1 with Router ID 3.3.3.3	ルータID 3.3.3.3のOSPFv3プロセス1のGRの状態が表示されます。
Graceful-restart capability	OSPFv3 GRが有効かどうかを示します。 ● **Enabled**－有効です。 ● **Disabled**－無効です。
Graceful-restart support	プロセスがサポートしているGRモードです。（GRが有効である場合のみ表示されます）。 ● **Planned and un-planned**– planned GR、unplanned GRの両方をサポートします。 ● **Planned only**– planned GRをサポートします。 ● **Partial**– partial GRをサポートします。 ● **Global**–すべてのGRをサポートします。
Helper capability	OSPFv3 GRヘルパーが有効かどうかを示します。 ● **Enabled**－有効です。 ● **Disabled**－無効です。
Helper support	GRヘルパーがサポートするポリシーとGRモードです（GRヘルパーが有効である場合のみ表示されます）。 ● **Strict LSA check**–GRヘルパーはstrict LSA確認をサポートします。 ● **Planned and un-planned**–GRヘルパーはplanned GRとunplanned GRの両方をサポートします。 ● **Planned only**– GRヘルパーはplanned GRのみサポートします。
Current GR state	GRの状態です。 ● **Normal**–GRが処理中でない、あるいは完了しました。 ● **Under GR**–GRが処理中です。 ● **Under Helper**–プロセスがGRヘルパーとして動作しています。
Graceful-restart period	GRを再起動する間隔です。
Number of neighbors under helper	GRヘルパー状態の隣接の数です。
Number of restarting neighbors	GRリスタータ状態の隣接の数です。

フィールド	説明

Last exit reason	最後に終了した理由です。
	• **Restarter**–リスタータが最後に終了した理由です。
	  • 終了していません。
	  • **Completed**–GRが終了しました。
	  • **Interval timer is fired**–GRタイマが終了しました。
	  • **Interface state change**–インタフェースの状態の変更が発生しました。
	  • **Received 1-way hello**–装置は隣接から1方向のHelloパケットを受信しました。
	  • **Reset neighbor**–隣接がリセットしました。
	  • **DR or BDR change**–DRあるいはBDRが変更しました。
	• **Helper**–ヘルパーが最後に終了した理由です。
	  • 終了していません。
	  • **Completed**– GRが終了しました。
	  • **Received 1-way hello**–装置は隣接から1方向のHelloパケットを受信しました。
	  • **Grace Period timer is fired**–GRタイマが終了しました。
	  • **Lsa check failed**–GRヘルパーのLSAの変更を検出しました。
	  • **Reset neighbor**–隣接がリセットしました。
	  • **Received MAXAGE gracelsa but neighbor is not full**–装置は最大エージング時間に到達したgrace LSAを受信しましたが、隣接はFULL状態になっていません。

すべての OSPFv3 プロセス GR の詳細情報を表示します。(GR リスタータ)

<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

Sham-link Neighbor-ID: 100.1.1.1, Neighbor-state: Full
Restarter state: Normal   State: P-2-P    Type: Sham
Interface-ID: 2147483649, Instance-ID: 0
Source      : 8000:88::FFFF
Destination : 7000:77::FFFF
Last exit reason:
  Restarter: None
  Helper   : None
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
```

表 8-8 コマンド出力

フィールド	説明
Area	エリアIDです。
Area flag	エリアのタイプです。 ● **Normal**－正常エリアです。 ● **Transit**－通過するエリアです。 ● **Stub**－スタブエリアです ● **StubNoSummary**–完全スタブエリアです。 ● **NSSA**－NSSAエリアです ● **NSSANoSummary**–完全NSSAエリアです。 ● **NSSANoSummaryNoImportRoute**– **no-import-route**が設定された完全NSSAエリアです。
7/5 translator state	Type-7 LSAからType-5 LSAに変換する状態です。状態は以下の1つになることができます ● **Enabled**－変換はコマンドによって指定されます。 ● **Elected**－変換は選択によって定義されます。 ● **Disabled**–装置は変換しません。
7/5 translate stability timer interval	Type-7 LSAからType-5 LSAに変換する安定状態です。単位は秒です。
Area up interface count	エリアでup状態のインタフェースの数です。

フィールド	説明
Interface	エリアのインタフェース、仮想リンクの出力インタフェースです。
Restarter state	インタフェースのリスタータ状態です。
State	インタフェース状態です。
Type	インタフェースのネットワークタイプです。
Neighbor count of this interface	インタフェースの隣接数です。
Neighbor	隣接のルータIDです。
GR state	隣接のGR状態です。 ● **Normal**–GRが処理中でない、あるいは完了しました。 ● **Under GR**–GRが処理中です。 ● **Under Helper**–プロセスがGRヘルパーとして動作しています。
Last helper exit reason	ヘルパーがもっとも最後に終了した理由です。
Virtual-link Neighbor-ID	仮想リンクの隣接のルータIDです。
Neighbor-State	隣接状態です。Down、Init、2-Way、ExStart、Exchange、Loading、Fullがあります。
Local IPv6 address	隣接関係のローカルIPv6アドレスです。
Remote IPv6 address	隣接関係のピアのIPv6アドレスです。
Transit area	通過するエリアIDです。
Sham-link Neighbor-ID	shamリンクの隣接のルータIDです。
Source	shamリンクの送信元アドレスです。
Destination	shamリンクの宛先アドレスです。

8.1.11 display ospfv3 interface

Syntax

display ospfv3 [*process-id*] **interface** [*interface-type interface-number* | **verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

process-id: OSPFv3 プロセスを指定します。設定範囲は 1～65535 です。

interface-type interface-number: インタフェースのタイプと番号を指定します。

verbose: すべてのインタフェースの OSPFv3 の詳細情報を表示します。

説明

display ospfv3 interface コマンドは OSPFv3 インタフェースの情報を表示します。

process-id を指定しない場合、すべての OSPFv3 プロセスの OSPFv3 インタフェースの概要情報を表示します。

interface-type interface-number あるいは **verbose** を指定しない場合、すべての OSPFv3 インタフェースの概要情報を表示します。

例

VLAN インタフェース 1 の OSPFv3 の情報を表示します。

<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
  Neighbor count is 1, Adjacent neighbor count is 1
  IPsec profile name: profile001
  Exchanging/Loading neighbors: 0
  Wait timer: Off,  LsAck timer: Off
  Prefix-suppression is enabled
```

表 8-9 コマンド出力

フィールド	説明
Area	インタフェースが所属しているエリアIDです。
Interface ID	インタフェースIDです。
Instance ID	インスタンスのIDです。
IPv6 prefixes	IPv6プレフィックスです。
Cost	インタフェースのコストです。
State	インタフェースの状態です。 ● **DOWN**–インタフェース上で送受信できるプロトコルトラフィックはありません。 ● **Waiting**–インタフェースはHello パケットの送受信を開始します。ルータはネットワークの代表ルータ（バックアップ代表ルータ）を決定します。 ● **P-2-P**–インタフェースは、Hello Interval の間隔でHelloパケットを送信し、隣接との隣接関係を確立しようと試みます。 ● **DR**–ルータ自身が接続されたネットワークのDRルータになります。 ● **BDR**–ルータ自身が接続されたネットワークのバックアップDRルータになります。 ● **DROther**–DR otherルータがネットワーク上にいます。
Type	インタフェースのネットワークタイプです。PTP (P2P)、PTMP (P2MP)、Broadcast、NBMA.があります。
MTU	インタフェースのMTUです。
Priority	インタフェースのDRの優先順位です。
Designated router	リンクのDRです。
Backup designated router	リンクのBDRです。
Timer interval configured	インタフェースで設定された時間間隔です。 ● **Hello**–Hello間隔です。 ● **Dead**–Dead間隔です。 ● **Poll**–NBMAネットワークのポーリング間隔です。 ● **Retransmit**–LSAの再配信間隔です。 ● **Transmit delay**–インタフェースの転送遅延です。

フィールド	説明
Neighbor count	インタフェースの隣接の数です。
Adjacent neighbor count	インタフェースの境界数です。
IPsec profile name	インタフェースに適用されたIPsecプロファイルです。

8.1.12 display ospfv3 lsdb

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**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

process-id: OSPFv3 プロセスを指定します。設定範囲は 1～65535 です。指定しない場合、すべての OSPFv3 プロセスの LSDB の情報を表示します。

external: AS 外部 LSA（Type-5 LSA）を表示します。

grace: grace LSA（Type-11 LSA）を表示します。

inter-prefix: 外部エリアプレフィックス LSA（Type-3 LSA）を表示します。

inter-router: 外部エリアルータ LSA（Type-4 LSA）を表示します。

intra-prefix: 内部エリアプレフィックス LSA（Type-9 LSA）を表示します。

link: リンク LSA（Type-8 LSA）を表示します。

network: ネットワーク LSA（Type-2 LSA）を表示します。

router: ルータ LSA（Type-1 LSA）を表示します。

unknown: 不明な LSA を表示します。

type: LSA タイプを指定します。16 進数の文字列です。設定範囲は 0～FFFF です。指定しない場合すべての不明な LSA を表示します。

link-state-id: IPv4 アドレス形式のリンクステート ID を指定します。

originate-router *router-id*: 配信するルータの ID を指定します。

self-originate: ローカルに作成された LSA の情報を表示します。

statistics: LSA の統計情報を表示します。

total: LSDB の LSA の総数を表示します。

verbose: 詳細情報を表示します。指定しない場合、概要情報を表示します。

説明

display ospfv3 lsdb コマンドは OSPFv3 LSDB を表示します。

例

OSPFv3 LSDB 情報を表示します。

<Switch> display ospfv3 lsdb

```
            OSPFv3 Process 1 with Router ID 1.1.1.1

              Link-LSA (Interface Vlan-interface1)
------------------------------------------------------------------------
 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
```

表 8-10 コマンド出力

フィールド	説明
Origin Router	最初のルータです。

フィールド	説明
Age	LSAのエージング時間です。
SeqNum	LSAのシーケンス番号です。
CkSum	LSAチェックサムです。
Prefix	プレフィックス数です。
Link	リンク数です。
Intra-Area-Prefix-LSA	Type-9 LSAです。
Reference	参照LSAのタイプです。

LSDB のリンク LSA の情報を表示します。

<Switch> display ospfv3 lsdb link

```
            OSPFv3 Process 1 with Router ID 1.1.1.1
              Link-LSA (Interface Vlan-interface1)
------------------------------------------------------------------------
  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|-|-|E|V6)
  Link-Local Address: fe80::200:5eff:fe00:100
  Number of Prefixes: 1
      Prefix      : 1001::/64
      Prefix Options: 0 (-|-|-|-)
```

表 8-11 コマンド出力

フィールド	説明
LS age	LSAのエージング時間です。
LS Type	LSAのタイプです。
Link State ID	リンクステートのIDです。

フィールド	説明
Originating Router	最初のルータです。
LS Seq Number	LSAシーケンス番号です。
Checksum	LSAチェックサムです。
Length	LSA長です。
Priority	ルータの優先順位です。
Options	オプションです。
Link-Local Address	リンクローカルアドレスです。
Number of Prefixes	プレフィックスの数です。
Prefix	アドレスのプレフィックスです。
Prefix Options	プレフィックスのオプションです。

LSA の統計情報を表示します。

<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          2      0       0        0       3        1
-------------------------------------------------------------------------
              Link   Grace   ASE
 Total          4      0       0
```

表 8-12 コマンド出力

フィールド	説明
Area ID	エリアIDです。
Router	Type-1 LSAの数です。
Network	Type-2 LSAの数です。
IntePre	Type-3 LSAの数です。

フィールド	説明
InteRou	Type-4 LSAの数です。
IntraPre	Type-9 LSAの数です。
NSSA	Type-7 LSAの数です。
Link	Type-8 LSAの数です。
Grace	Type-11 LSAの数です。
ASE	Type-5 LSAの総数です。

OSPFv3 LSDB の詳細情報を表示します。

<Switch> display ospfv3 lsdb verbose

```
            OSPFv3 Process 1 with Router ID 1.1.1.1

              Link-LSA (Interface Vlan-interface1)
-------------------------------------------------------------------------
 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
```

表 8-13 コマンド出力

フィールド	説明
SendCnt	LSAを送信したインタフェースの数です。
RxmtCnt	リンクステート状態の再配信リストのLSAの数です。
Status	LSA状態です。 ● **Normal**－正常状態です。 ● **Delayed**－遅延しています。 ● **Maxage routed**–LSAが最大エージング時間に到達しました。 ● **Self originated**－ローカル状態です。 ● **Stale**–GRプロセスの間にローカルで作成されたLSAを受信しました。

8.1.13 display ospfv3 nexthop

Syntax

display ospfv3 [*process-id*] **nexthop**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

process-id: OSPFv3 プロセスを指定します。設定範囲は 1～65535 です。指定しない場合、すべての OSPFv3 プロセスのネクストホップの情報を表示します。

説明

display ospfv3 nexthop コマンドは OSPFv3 のネクストホップの情報を表示します。

例

OSPFv3 プロセス 1 のネクストホップの情報を表示します。

<Switch> display ospfv3 1 nexthop

```
            OSPFv3 Process 1 with Router ID 1.1.1.1

 Nexthop : FE80::20C:29FF:FED7:F308            Interface: Vlan2
 RefCount: 4                                  Status   : Valid
 NbrID   : 1.1.1.1                            NbrIntID : 21

 Nexthop : FE80::20C:29FF:FED7:F312            Interface: Vlan12
 RefCount: 3                                  Status   : Valid
 NbrID   : 1.1.1.1                            NbrIntID : 38
```

表 8-14 コマンド出力

フィールド	説明
Nexthop	ネクストホップアドレスです。
Interface	出力インタフェースです。
RefCount	参照回数です（ネクストホップを参照するルートです）。
Status	ネクストホップの状態です。有効、無効があります。
NbrId	隣接ルータのIDです。
NbrIntID	隣接インタフェースのIDです。

8.1.14 display ospfv3 non-stop-routing

Syntax

display ospfv3 [*process-id*] **non-stop-routing**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

process-id: OSPFv3 プロセスを 1～65535 までの ID で指定します。指定しないと、すべての OSPFv3 プロセスの OSPFv3 NSR 情報が表示されます。

説明

display ospfv3 non-stop-routing コマンドは、OSPFv3 の NSR 情報を表示します。

例

OSPFv3 NSR 情報を表示します。

<Switch> display ospfv3 non-stop-routing

```
OSPFv3 Process 1 with Router ID 3.3.3.3

Nonstop Routing capability: Enabled
Upgrade phase           : Normal
```

表 8-15 コマンド出力

フィールド	説明
Nonstop Routing capability	NSR状態–enabledまたはdisabledです。
Upgrade phase	NSRフェーズです。 ● **Normal**–標準状態です。 ● **Preparation**–アップグレード準備フェーズです。 ● **Smooth**–アップグレードフェーズです。 ● **Precalculation**–ルートの事前計算フェーズです。 ● **Calculation**–ルート計算フェーズです。 ● **Redistribution** –ルート再配信フェーズです。

8.1.15 display ospfv3 peer

Syntax

display ospfv3 [*process-id*] [**area** *area-id*] **peer** [[*interface-type interface-number*] [**verbose**] | *peer-router-id* | **statistics**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

process-id: OSPFv3 プロセスを指定します。設定範囲は 1～65535 です。

area *area-id*: エリアの ID を指定します。IPv4 アドレスあるいは 10 進数の整数で指定します。10 進数の整数の設定範囲は 0～4294967295 で、システムで自動に IPv4 アドレスに変換されます。

interface-type interface-number: インタフェースのタイプと番号を指定します。

verbose: 隣接の詳細情報を表示します。

peer-router-id: 隣接を指定します。

statistics: OSPFv3 の隣接の統計情報を表示します。

説明

display ospfv3 peer コマンドは OSPFv3 の隣接の情報を表示します。

process-id を指定しない場合、すべての OSPFv3 プロセスの隣接情報を表示します。

area *area-id* を指定しない場合、すべてのエリアの隣接情報を表示します。

interface-type interface-number あるいは *peer-router-id* を指定しない場合、すべてのインタフェースの隣接情報を表示します。

例

インタフェースの OSPFv3 プロセス 1 の隣接情報を表示します。

<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
```

表 8-16 コマンド出力

フィールド	説明
Router ID	隣接のルータIDです。
Pri	隣接ルータの優先順位です。
State	隣接状態です。
Dead-Time	deadタイマの残り時間です。

フィールド	説明
Inst ID	インスタンスのIDです。
Interface	隣接に接続されたインタフェースです。

インタフェースの OSPFv3 プロセス 1 の隣接の詳細情報を表示します。

<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 0x000013 (-|R|-|-|E|V6)
  Dead timer due in 00:00:33
  Neighbor is up for 00:24:19
  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
```

表 8-17 コマンド出力

フィールド	説明
Router ID	隣接のルータIDです。
Address	インタフェースのリンクローカルアドレスです。
State	隣接状態です。
Mode	LSDBの同期を行うための隣接モードです。
Priority	隣接ルータの優先順位です。
DR	インタフェースのネットワークセグメントのDRです。
BDR	インタフェースのネットワークセグメントのBDRです。

フィールド	説明
MTU	インタフェースのMTUです。
Options	LSAオプションです。 ● **DC**－最初のルータはオンデマンドリンクを越えてOSPFv3をサポートします ● **R**－最初のルータがアクティブルータかどうかを示します。 ● **N**－最初のルータはNSSALSAをサポートします。 ● **x**–予約されています。 ● **E**－最初のルータがAS外部LSAを受信できます。 ● **V6**–最初のルータがIPv6ルーティングの計算を行うかどうかを示します。
Dead timer due in 33 sec	deadタイマが33秒後に終了します。
Neighbor is up for 00:24:19	隣接が00:24:19の間、up状態です。
Neighbor state change count	隣接状態が変更した回数です。
Database Summary List	LSAがDDパケットを送信した数です。
Link State Request List	リンク状態のLSAがリストを要求した数です。
Link State Retransmission List	リンク状態のLSAがリストを再送信した数です。
GR state	GRの状態です。 ● **Normal**－正常状態です。 ● **Doing GR**–GRリスタータとして動作しています。 ● **Complete GR**－GRを終了しました。 ● **Helper**–GRヘルパーとして動作しています。
Grace period	grace LSAの送信間隔です。
Grace period timer	grace LSAを送信する間隔のタイマです。
DD Rxmt timer	DDパケットを再配信するタイマです。
LS Rxmt timer	LSAを再配信するタイマです。

OSPFv3 の隣接の統計情報を表示します。

<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
```

表 8-18 コマンド出力

フィールド	説明
Area ID	エリアIDです。
Down	この状態の隣接は初期状態です。一定期間、隣接するルータから情報を受信していません。
Attempt	NBMAネットワークでのみ有効です。この状態ではOSPFv3ルータは一定の期間、隣接から情報を受信しません。ルータは隣接との関係を保持するためにhelloパケットを長い間隔で送信することができます。
Init	この状態ではルータは隣接からHelloパケットを受信しましたが、パケットに隣接のルータIDがありません。 ルータは隣接と双方向の接続を確立していません。
2-Way	ルータと隣接間の双方向の通信が有効です。この状態以降でDRとBDRの選択は完了しています。
ExStart	この状態ではルータは初期のDDシーケンス番号、相互のアクティブ/スタンバイの関係を決定します。
Exchange	この状態ではルータは隣接のDDパケットを交換します。
Loading	この状態ではルータは必要なLSAのために隣接に要求するためLSRを送信します。
Full	LSDBの同期化が隣接間で完了しています。
Total	同一状態の隣接の総数です。

8.1.16 display ospfv3 request-queue

Syntax

display ospfv3 [*process-id*] [**area** *area-id*] **request-queue** [*interface-type interface-number*] [*neighbor-id*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

process-id: OSPFv3 プロセスを指定します。設定範囲は 1～65535 です。

area *area-id*: エリアの ID を指定します。IPv4 アドレスあるいは 10 進数の整数で指定します。10 進数の整数の設定範囲は 0～4294967295 で、システムで自動に IPv4 アドレスに変換されます。

interface-type interface-number: インタフェースのタイプと番号を指定します。

neighbor-id: 隣接のルータ ID を指定します。

説明

display ospfv3 request-queue コマンドは OSPFv3 の要求リストの情報を表示します。

process-id を指定しない場合、すべての OSPFv3 プロセスの OSPFv3 要求リストの情報を表示します。

area *area-id* を指定しない場合、すべてのエリアの OSPFv3 要求リストの情報を表示します。

interface-type interface-number を指定しない場合、すべてのインタフェースの OSPFv3 要求リストの情報を表示します。

neighbor-id を指定しない場合、すべての隣接の OSPFv3 要求リストの情報を表示します。

例

OSPFv3 の要求リストの情報を表示します。

<Switch> display ospfv3 request-queue

```
            OSPFv3 Process 1 with Router ID 1.1.1.1

                Area: 0.0.0.0
                Interface Vlan-interface1
--------------------------------------------------------------------------
                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
```

表 8-19 コマンド出力

フィールド	説明
Area	エリアIDです。

フィールド	説明
Interface	インタフェースのタイプとシーケンス番号です。
Nbr-ID	隣接のIDです。
Request list	要求リスト情報です。
Type	LSAタイプです。
AdvRouter	配信するルータです。
SeqNum	LSAのシーケンス番号です。
Age	LSAのエージング時間です。
CkSum	チェックサムです。

8.1.17 display ospfv3 retrans-queue

Syntax

display ospfv3 [*process-id*] [**area** *area-id*] **retrans-queue** [*interface-type interface-number*] [*neighbor-id*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

process-id: OSPFv3 プロセスを指定します。設定範囲は 1～65535 です。

area *area-id*: エリアの ID を指定します。IPv4 アドレスあるいは 10 進数の整数で指定します。10 進数の整数の設定範囲は 0～4294967295 で、システムで自動に IPv4 アドレスに変換されます。

interface-type interface-number: インタフェースのタイプと番号を指定します。

neighbor-id: 隣接のルータ ID を指定します。

説明

display ospfv3 retrans-queue コマンドは OSPFv3 再送リストの情報を表示します。

process-id を指定しない場合、すべての OSPFv3 プロセスの OSPFv3 再送リストの情報を表示します。

area *area-id* を指定しない場合、すべてのエリアの OSPFv3 再送リストの情報を表示します。

interface-type interface-number を指定しない場合、すべてのインタフェースの OSPFv3 再送リストの情報を表示します。

neighbor-id を指定しない場合、すべての隣接の OSPFv3 再送リストの情報を表示します。

例

OSPFv3 再送リストの情報を表示します。

<Switch> display ospfv3 retrans-queue

```
            OSPFv3 Process 1 with Router ID 1.1.1.1

                Area: 0.0.0.0
                Interface Vlan-interface1
--------------------------------------------------------------------------
                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
```

表 8-20 コマンド出力

フィールド	説明
Area	エリアIDです。
Interface	インタフェースのタイプとシーケンス番号です。
Nbr-ID	隣接のIDです。
Retransmit List	再配信リストの情報です。
Type	LSAタイプです。
AdvRouter	配信するルータです。
SeqNum	LSAのシーケンス番号です。
Age	LSAのエージング時間です。
CkSum	チェックサムです。

8.1.18 display ospfv3 routing

Syntax

display ospfv3 [*process-id*] r**outing** [*ipv6-address prefix-length*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

process-id: OSPFv3 プロセスを指定します。設定範囲は 1～65535 です。指定しない場合、すべての OSPFv3 プロセスのルーティング情報を表示します。

ipv6-address prefix-length: IPv6 アドレスを指定します。*ipv6-address* は IPv6 プレフィックスを指定します。*prefix-length* はプレフィックス長を指定します。設定範囲は 0～128 です。

説明

display ospfv3 routing コマンドは OSPFv3 のルーティング情報を表示します。

例

OSPFv3 のルーティング情報を表示します。

<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                                  Cost     : 0
  Nexthop   : ::                                  Interface: Loop1
  AdvRouter : 9.9.9.9                             Area     : 0.0.0.0
  Preference : 10

 *Destination: 4::4/128
  Type      : I                                  Cost     : 1
  Nexthop   : FE80::20C:29FF:FED4:7171              Interface: Vlan2
  AdvRouter : 8.8.8.8                             Area     : 0.0.0.0
```

```
 Preference : 10

*Destination: 6::/64
 Type       : I                                  Cost     : 1
 Nexthop    : ::                                 Interface: Vlan2
 AdvRouter  : 9.9.9.9                            Area     : 0.0.0.0
 Preference : 10

Total: 3
Intra area: 3       Inter area: 0       ASE: 0       NSSA: 0
```

表 8-21 コマンド出力

フィールド	説明
Destination	宛先ネットワークのセグメントです。
Type	ルートタイプです。
Cost	ルートのコストです。
Nexthop	ネクストホップのアドレスです。
Interface	出力インタフェースです。
AdvRouter	配信するルータです。
Area	エリアIDです。
Tag	外部ルートのタグです。
Preference	ルートの優先順位です。
Total	ルートの総数です。
Intra area	内部エリアルートの数です。
Inter area	外部エリアルートの数です。
ASE	Type-5外部ルートの数です。
NSSA	Type-7外部ルートの数です。

8.1.19 display ospfv3 statistics

Syntax

display ospfv3 [*process-id*] **statistics**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

process-id: OSPFv3 プロセスを指定します。設定範囲は 1～65535 です。指定しない場合、すべての OSPFv3 プロセスの OSPFv3 の統計情報を表示します。

説明

display ospfv3 statistics コマンドは OSPFv3 の統計情報を表示します。

例

OSPFv3 の統計情報を表示します。

<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
```

表 8-22 コマンド出力

フィールド	説明
Packet Statistics	送受信パケットの統計情報です。
Hello	Helloパケットです。
DB Description	DB宛先パケットです。
Ls Req	リンクステート要求パケットです。
Ls Upd	リンクステートアップデートパケットです。
Ls Ack	リンクステートacknowledgmentパケットです。
Local Originated LSAs Statistics	作成されたLSAの統計情報です。
Router-LSA	Type-1 LSAの数です。
Network-LSA	Type-2 LSAの数です。
Inter-Area-Prefix-LSA	Type-3 LSAの数です。
Inter-Area-Router-LSA	Type-4 LSAの数です。
AS-external-LSA	Type-5 LSAの数です。
NSSA-LSA	Type-7 LSAの数です。
Link-LSA	Type-8 LSAの数です。
Intra-Area-Prefix-LSA	Type-9 LSAの数です。

フィールド	説明
Grace-LSA	Type-11 LSAの数です。
Unknown-LSA	不明なLSAの数です。
Total	総数です。
Routes Statistics	ルートの数です
Intra Area	内部エリアルートです。
Inter Area	外部エリアルートです。
ASE	Type-5 外部ルートです。
NSSA	Type-7外部ルートです。

8.1.20 display ospfv3 vlink

Syntax

display ospfv3 [*process-id*] **vlink**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

process-id: OSPFv3 プロセスを指定します。設定範囲は 1～65535 です。指定しない場合、すべての OSPFv3 プロセスの OSPFv3 仮想リンクの情報を表示します。

説明

display ospfv3 vlink コマンドは OSPFv3 仮想リンクの情報を表示します。

例

OSPFv3 仮想リンクの情報を表示します。

<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
```

表 8-23 コマンド出力

フィールド	説明
Virtual-link Neighbor-ID	仮想リンクの隣接のIDです。
Neighbor-State	隣接状態です。Down、Init、2-Way、ExStart、Exchange、Loading、Fullがあります。
Interface	仮想リンクのローカルインタフェースの番号と名前です。
Cost	インタフェースのルートのコストです。
State	インタフェースの状態です。
Type	仮想リンクです。
Transit Area	通過するエリアIDです。（このフィールドはインタフェースで仮想リンクが存在しているとき表示します。）
Timers	OSPFv3タイマの値です。単位は秒です。hello、dead、retransmit、interface transmission delayがあります。
IPsec profile name	仮想リンクに適用したIPsecプロファイルです

8.1.21 filter (OSPFv3 area view)

Syntax

filter { *acl6-number* | **prefix-list** *prefix-list-name* | **route-policy** *route-policy-name* } { **export** | **import** }

undo filter { **export** | **import** }

デフォルト

設定なし

View

OSPFv3 area view

定義済みユーザロール

network-admin

パラメータ

acl6-number: 送信/受信の外部エリアプレフィックス LSA をフィルタするため IPv6 ACL の番号を指定します。設定範囲は 2000～3999 です。

prefix-list-name: 送信/受信の外部エリアプレフィックス LSA をフィルタするため IPv6 プレフィックスリストを指定します。設定範囲は 1～63 文字です。大文字、小文字を区別します。

route-policy-name: 送信/受信の外部エリアプレフィックス LSA をフィルタするためルーティングポリシーの名前を指定します。設定範囲は 1～63 文字です。大文字、小文字を区別します。

export: ほかのエリアに配信する外部エリアプレフィックス LSA をフィルタします。

import: ローカルエリアに配信する外部エリアプレフィックス LSA をフィルタします。

説明

filter コマンドは ABR で送信/受信の外部エリアプレフィックス LSA をフィルタするために OSPFv3 を設定します。

undo filter コマンドは設定を削除します。

このコマンドは ABR でのみ有効です。

例

OSPFv3 エリア 1 で、受信の外部エリアプレフィックス LSA をフィルタするため IP プレフィックスリスト my-prefix-list を設定し、送信の外部エリアプレフィックス LSA をフィルタするため ACL 2000 を設定します。

```
<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
```

8.1.22 filter-policy export (OSPFv3 view)

Syntax

filter-policy { *acl6-number* | **prefix-list** *prefix-list-name* } **export** [*protocol* [*process-id*]]

undo filter-policy export [*protocol* [*process-id*]]

デフォルト

設定なし

View

OSPFv3 view

定義済みユーザロール

network-admin

パラメータ

acl6-number: 再配信されるルートを宛先アドレスでフィルタするため IPv6 ACL の番号を指定します。設定範囲は 2000～3999 です。

prefix-list-name: 再配信されるルートを宛先アドレスでフィルタするため IPv6 プレフィックスリストの名前を指定します。設定範囲は 1～63 文字です。大文字、小文字を区別します。

protocol: 指定したルーティングプロトコルから再配信されるルートをフィルタします。ルーティングプロトコルは **direct**、**ospfv3**、**ripng**、**static** を指定できます。指定しない場合、すべての再配信されるルートをフィルタします。

process-id: プロセス ID を指定します。設定範囲は 1～65535 です。*process-id* は *protocol* パラメータが **ripng**、**ospfv3** であるときのみ有効です。

説明

filter-policy export コマンドは再配信されるルートをフィルタするため OSPFv3 を設定します。

undo filter-policy export コマンドは設定を削除します。

コマンドで拡張 ACL（ACL 番号が 3000～3999）を参照する場合、以下の方法の 1 つを使用して ACL を設定します。

- 指定した宛先でルートを拒否/許可する場合、**rule** [*rule-id*] { **deny** | **permit** } **ipv6 source** *sour sour-prefix*.コマンドを使用します。
- 指定した宛先とプリフィックスでルートを拒否/許可する場合、**rule** [*rule-id*] { **deny** | **permit** } **ipv6 source** *sour sour-prefix* **destination** *dest dest-prefix*.コマンドを使用します。

source はルートの宛先アドレスを指定し、**destination** はルートのプレフィックスを指定します。指定したプレフィックスは連続している必要があります。連続していない場合、設定は適用しません。

filter-policy export コマンドは **import-route** コマンドで再配信されたルートのみフィルタします。**import-route** コマンドがほかのプロトコル、ほかの OSPFv3 プロセスから再配信されたルートに設定されていない場合、**filter-policy export** コマンドは適用しません。

例

再配信されるルートをフィルタするため IPv6 プレフィックスリスト abc を設定します。

<Switch> system-view

[Switch] ipv6 prefix-list abc permit 2002:1:: 64

[Switch] ospfv3

[Switch-ospfv3-1] filter-policy prefix-list abc export

ルート 2001::1/128 のみ許可するように IPv6 ACL 3000 を設定します。再配信されるルートをフィルタするため ACL 3000 を設定します。

<Switch> system-view

[Switch] acl ipv6 number 3000

[Switch-acl6-adv-3000] rule 10 permit ipv6 source 2001::1 128 destination ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff 128

[Switch-acl6-adv-3000] rule 100 deny ipv6

[Switch-acl6-adv-3000] quit

[Switch] ospfv3

[Switch-ospfv3-1] filter-policy 3000 export

8.1.23 filter-policy import (OSPFv3 view)

Syntax

filter-policy { *acl6-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

デフォルト

設定なし

View

OSPFv3 view

定義済みユーザロール

network-admin

パラメータ

acl6-number: 受信したルートを宛先アドレスでフィルタするため IPv6 ACL の番号を指定します。設定範囲は 2000～3999 です。

gateway *prefix-list-name*: ネクストホップで受信したルートをフィルタするため IPv6 プレフィックスリストを指定します。設定範囲は 1～63 文字です。大文字、小文字を区別します。指定しない、ネクストホップでルートをフィルタしません。

prefix-list *prefix-list-name*: 受信したルートを宛先アドレスでフィルタするため IPv6 プレフィックスリストの名前を指定します。設定範囲は 1～63 文字です。大文字、小文字を区別します。

route-policy *route-policy-name*: 受信したルートをフィルタするためルーティングポリシーを指定します。設定範囲は 1～63 文字です。大文字、小文字を区別します。

説明

filter-policy import コマンドは受信した LSA を使用して計算したルートをフィルタするため OSPFv3 を設定します。

undo filter-policy import コマンドはデフォルトに戻します。

filter-policy import コマンドあるいは指定したルーティングポリシーで拡張 ACL（ACL 番号が 3000～3999）を参照する場合、以下の方法の 1 つを使用して ACL を設定します。

- 指定した宛先でルートを拒否/許可する場合、**rule** [*rule-id*] { **deny** | **permit** } **ipv6 source** *sour sour-prefix* コマンドを使用します。
- 指定した宛先とプリフィックスでルートを拒否/許可する場合、**rule** [*rule-id*] { **deny** | **permit** } **ipv6 source** *sour sour-prefix* **destination** *dest dest-prefix* コマンドを使用します。

source はルートの宛先アドレスを指定し、**destination** はルートのプレフィックスを指定します。指定したプレフィックスは連続している必要があります。連続していない場合、設定は適用しません。

filter-policy export コマンドは OSPFv3 で計算されたルートのみフィルタします。フィルタのパスに失敗したルートはルーティングテーブルに追加されません。

例

受信したルートをフィルタするため IPv6 プレフィックスリスト abc を設定します。

<Switch> system-view

[Switch] ipv6 prefix-list abc permit 2002:1:: 64

[Switch] ospfv3

[Switch-ospfv3-1] filter-policy prefix-list abc import

ルート 2001::1/128 のみ許可するように IPv6 ACL 3000 を設定します。受信されるルートをフィルタするため ACL 3000 を設定します。

<Switch> system-view

[Switch] acl ipv6 number 3000

[Switch-acl6-adv-3000] rule 10 permit ipv6 source 2001::1 128 destination ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff 128

[Switch-acl6-adv-3000] rule 100 deny ipv6

[Switch-acl6-adv-3000] quit

[Switch] ospfv3

[Switch-ospfv3-1] filter-policy 3000 import

8.1.24 graceful-restart enable

Syntax

graceful-restart enable

undo graceful-restart enable

デフォルト

無効

View

OSPFv3 view

定義済みユーザロール

network-admin

説明

graceful-restart enable コマンドは OSPFv3 GR を有効にします。

undo graceful-restart enable コマンドは OSPFv3 GR を無効にします。

GR は planned GR と unplanned GR があります。

- **Planned GR**–手動で OSPFv3 を再起動する、あるいはアクティブ/スタンバイの切り替えを実行します。OSPFv3 の再起動、あるいはアクティブ/スタンバイの切り替えを行う前に、GR リスタータは grace LSA を GR ヘルパーに送信します。
- **Unplanned GR**–装置が故障したため、OSPFv3 は、OSPFv3 の再起動、あるいはアクティブ/スタンバイの切り替えを行います。OSPFv3 の再起動、あるいはアクティブ/スタンバイの切り替えを行う前、GR リスタータは grace LSA を GR ヘルパーに送信しません。

OSPFv 3 GR と OSPFv 3 NSR は相互に排他的です。**graceful-restart enable** コマンドと **non-stop-routing** コマンドを同時に設定しないでください。

アクティブ/スタンバイの切り替えを実行したのち、サービスの中断を防ぐため、OSPFv3 が動作している GR リスタータは以下の作業を完了している必要があります。

- 再起動中に GR リスタータの転送エントリを安定に保ってください。
- 再起動後、すべての隣接関係を確立し、完全なトポロジ情報を取得してください。

例

OSPFv3 プロセス 1 の GR を有効にします。

<Switch> system-view

[Switch] ospfv3 1

[Switch-ospfv3-1] graceful-restart enable

関連コマンド

graceful-restart helper enable

8.1.25 graceful-restart helper enable

Syntax

graceful-restart helper enable

undo graceful-restart helper enable

デフォルト

有効

View

OSPFv3 view

定義済みユーザロール

network-admin

説明

graceful-restart helper enable コマンドは OSPFv3 GR ヘルパーを有効にします。

undo graceful-restart helper enable コマンドは OSPFv3 GR ヘルパーを無効にします。

Grace LSA を受信した後、GR ヘルパー機能のある隣接ルータはヘルパーモード（このため、GR ヘルパーと呼ばれます）となります。その後、GR リスタータが GR ヘルパーの支援で隣接関係と LSDB を回復します。

例

OSPFv3 プロセス 1 の GR ヘルパーを有効にします。

<Switch> system-view

[Switch] ospfv3 1

[Switch-ospfv3-1] graceful-restart helper enable

関連コマンド

graceful-restart enable

8.1.26 graceful-restart helper strict-lsa-checking

Syntax

graceful-restart helper strict-lsa-checking

undo graceful-restart helper strict-lsa-checking

デフォルト

無効

View

OSPFv3 view

定義済みユーザロール

network-admin

説明

graceful-restart helper strict-lsa-checking コマンドは GR ヘルパーの strict LSA checking を有効にします。

undo graceful-restart helper strict-lsa-checking コマンドは GR ヘルパーの strict LSA checking を無効にします。

GR ヘルパーで LSA の変更が検出されたとき、GR ヘルパーは GR ヘルパーモードを終了します。

例

OSPFv3 プロセス 1 の GR ヘルパーの strict LSA 確認を有効にします。

<Switch> system-view

[Switch] ospfv3 1

[Switch-ospfv3-1] graceful-restart helper strict-lsa-checking

関連コマンド

graceful-restart helper enable

8.1.27 graceful-restart interval

Syntax

graceful-restart interval *interval-value*

undo graceful-restart interval

デフォルト

120 秒

View

OSPFv3 view

定義済みユーザロール

network-admin

パラメータ

interval-value: GR 間隔を指定します。設定範囲は 40～1800 秒です。

説明

graceful-restart interval コマンドは GR 間隔を設定します。

undo graceful-restart interval コマンドはデフォルトに戻します。

GR を再起動する間隔の値は、すべての OSPFv3 インタフェースの OSPFv3 隣接の dead タイマの最大値よりも小さくすることはできません。小さい場合、GR の再起動は失敗します。

例

OSPFv3 プロセス 1 の GR 間隔を 100 秒に設定します。

<Switch> system-view

[Switch] ospfv3 1

[Switch-ospfv3-1] graceful-restart interval 100

関連コマンド

ospfv3 timer dead

8.1.28 import-route (OSPFv3 view)

Syntax

import-route *protocol* [*process-id* | **all-processes**] [**cost** *cost* | **route-policy** *route-policy-name* | **type** *type*] *

undo import-route *protocol* [*process-id* | **all-processes**]

import-route { ospfv3 | ripng } [*process-id* | all-processes]

undo import-route { ospfv3 | ripng } [*process-id* | all-processes]

デフォルト

無効

View

OSPFv3 view

定義済みユーザロール

network-admin

パラメータ

protocol: 指定したプロトコルからルートを再配信します。**direct、ospfv3、ripng、static** が指定できます。

process-id: プロセスの ID を指定します。設定範囲は 1～65535 です。デフォルトは 1 です。*process-id* は *protocol* が **ripng、ospfv3** であるときのみ有効です。

all-processes: 指定されたルーティングプロトコルのすべてのプロセスからルートを再配信します。**all-processes** は *protocol* が **ripng、ospfv3** であるときのみ有効です。

cost *cost*: ルートコストを指定します。設定範囲は 1～16777214 です。デフォルトは 1 です。

nssa-only: Type-7 LSA の P ビットを 0 に設定して、NSSA エリアへのルートアドバタイズメントを制限します。 このキーワードを指定しない場合、Type-7 LSA の P ビットは 1 に設定されます。 ルータが ASBR として動作し、バックボーンエリアに ABR および FULL ステートネイバーが存在する場合、ルータによって発信される Type-7 LSA の P ビットは 0 に設定されます。 このキーワードは、NSSA ルータに適用されます。

route-policy *route-policy-name*: 再配信するルートをフィルタするためルーティングポリシーを指定します。設定範囲は 1～63 文字です。大文字、小文字を区別します。

tag *tag*: 外部 LSA のタグを 0~4294967295 の範囲で指定します。 このオプションを指定しない場合、デフォルトの tag コマンドで指定されたタグが適用されます。

type *type*: 再配信ルートのコストタイプを指定します。設定範囲は 1 あるいは 2 です。デフォルトは 2 です。

説明

import-route コマンドは別のルーティングプロトコルから AS 外部ルートを再配信することを有効にします。

undo import-route コマンドは別のルーティングプロトコルから AS 外部ルートを再配信することを無効にします。

外部ルートは OSPFv3 AS の外部にある宛先のルートです。外部ルートは以下のタイプがあります。

- Type-1 外部ルートは高い信頼性を持ちます。Type-1 外部ルートのコストは OSPFv3 内部ルートのコストと同等です。OSPFv3 ルータから Type-1 外部ルータの宛先へのコストは、ルータから ASBR までのコストと ASBR から外部ルートの宛先までのコストを加えたものと等しくなります。
- Type-1 外部ルートは低い信頼性を持ちます。OSPFv3 では、ASBR から Type-2 外部ルートまでのコストは ASBR から OSPFv3 内部ルータまでのコストよりもはるかに大きいと認識します。このため、内部ルータから Type-2 の外部ルート宛先までのコストは、ASBR から Type-2 の外部ルートの宛先までのコストと等しくなります。

import-route コマンドは、デフォルトルートを再配布することはできません。

例

RIPng からルートを再配信する OSPFv3 プロセス 1 を設定します。再配信するルートのタイプを 2、コストを 50 に設定します。

<Switch> system-view

[Switch] ospfv3

[Switch-ospfv3-1] import-route ripng 10 type 2 cost 50

OSPFv3 プロセス 160 から検出されたルートを再配信するように OSPFv3 プロセス 100 を設定します。

<Switch> system-view

[Switch] ospfv3 100

[Switch-ospfv3-100] import-route ospfv3 160

関連コマンド

default-route-advertise (OSPFv3 view)

8.1.29 log-peer-change

Syntax

log-peer-change

undo log-peer-change

デフォルト

有効

View

OSPFv3 view

定義済みユーザロール

network-admin

説明

log-peer-change コマンドは隣接状態の変更に伴うログの作成を有効にします。

undo log-peer-change コマンドは隣接状態の変更に伴うログの作成を無効にします。

このコマンドは隣接状態の変更のログを information center に送信します。

information center はユーザが定義した出力ルール（ログを出力するか、どこにログを出力するか）に従ってログを処理します。information center の詳細は、オペレーションマニュアルのセクション 11 *システム管理* "*Information Center*"を参照してください。

例

OSPFv3 プロセス 100 の隣接状態の変更に伴うログの作成を無効にします。

<Switch> system-view

[Switch] ospfv3 100

[Switch-ospfv3-100] undo log-peer-change

8.1.30 lsa-generation-interval

Syntax

lsa-generation-interval *maximum-interval* [*minimum-interval* [*incremental-interval*]]

undo lsa-generation-interval

デフォルト

最大間隔は 5 秒、最小間隔は 0 ミリ秒、増加する間隔は 0 ミリ秒です。

View

OSPFv3 view

定義済みユーザロール

network-admin

パラメータ

maximum-interval: OSPFv3 LSA の生成する最大間隔を指定します。設定範囲は 1～60 秒です。

minimum-interval: OSPFv3 LSA の生成する最小間隔を指定します。設定範囲は 10～60000 ミリ秒です。デフォルトは 0 です。0 に設定した場合、最小間隔がどのような値にでもなるかもしれないことを示します。

incremental-interval: OSPFv3 LSA の生成する間隔が増加する間隔を指定します。設定範囲は 10～60000 ミリ秒です。

説明

lsa-generation-interval コマンドは OSPFv3 LSA を生成する間隔を設定します。

undo lsa-generation-interval コマンドはデフォルトに戻します。

ネットワークが頻繁に変わらないとき、LSA は *minimum-interval* の間隔で生成されます。ネットワークの変更がしばしば起こると、計算の間隔は計算のたびに *incremental-interval* × 2^{n-2} ずつ増え、最後は *maximum-interval* になります。n は生成回数です。

最小間隔と増加する間隔は最大間隔よりも大きくすることができません。

例

LSA の生成する最大間隔を 2 秒、最小間隔を 100 ミリ秒、増加する間隔を 100 ミリ秒に設定します。

<Switch> system-view

[Switch] ospfv3 100

[Switch-ospfv3-100] lsa-generation-interval 2 100 100

関連コマンド

lsa-arrival-interval

8.1.31 maximum load-balancing (OSPFv3 view)

Syntax

maximum load-balancing *maximum*

undo maximum load-balancing

View

OSPFv3 view

定義済みユーザロール

network-admin

パラメータ

maximum: ECMP（equal-cost multi-path）ルートの最大数を指定します。1 に指定した場合、OSPFv3 は負荷分散を実行しません。

説明

maximum load-balancing コマンドは負荷分散を行うため ECMP（equal-cost multi-path）の最大数を指定します。

undo maximum load-balancing コマンドはデフォルトに戻します。

OSPFv3 ECMP ルートの最大数のデフォルトはシステムでサポートする ECMP ルートの最大数と同じ、8 です。

例

負荷分散を行うため ECMP の最大数を 2 に設定します。

<Switch> system-view

[Switch] ospfv3 100

[Switch-ospfv3-100] maximum load-balancing 2

関連コマンド

max-ecmp-num

8.1.32 non-stop-routing

Syntax

non-stop-routing

undo non-stop-routing

デフォルト

無効

View

OSPFv3 view

定義済みユーザロール

network-admin

説明

non-stop-routing コマンドは、OSPFv3NSR を有効にします。

undo non-stop-routing コマンドは、OSPFv3 NSR を無効にします。

このコマンドは、現在のプロセスに対してのみ有効です。複数の OSPFv3 プロセスが存在する場合、プロセスごとに OSPFv3 NSR を有効にします。

OSPFv3 NSR と OSPFv3 GR は相互に排他的です。**non-stop-routing** コマンドと **graceful-restart enable** コマンドを同時に設定しないでください。

例

OSPFv3 プロセスの NSR100 を有効にします。

<Switch> system-view

[Switch] ospfv3 100

[Switch-ospfv3-100] non-stop-routing

8.1.33 ospfv3

Syntax

ospfv3 [*process-id* | **vpn-instance** *vpn-instance-name*] *

undo ospfv3 [*process-id*]

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

パラメータ

process-id: OSPFv3 プロセスを指定します。設定範囲は 1～65535 です。デフォルトは 1 です。

vpn-instance *vpn-instance-name*: VPN インスタンスを指定します。設定範囲は 1～31 文字です。大文字、小文字を区別します。指定しない場合、パブリックネットワークで OSPFv3 プロセスが動作します。

説明

ospfv3 コマンドは OSPFv3 プロセスを有効にし、OSPFv3 view に移行します。

undo ospfv3 コマンドは OSPFv3 プロセスを有効にします。

OSPFv3 プロセスでルータ ID を指定してください。指定しない場合、OSPFv3 プロセスは LSA を作成できません。

例

OSPFv3 プロセス 120 を有効にし、ルータ ID を 1.1.1.1 に指定します。

<Switch> system-view

[Switch] ospfv3 120

[Switch-ospfv3-120] router-id 1.1.1.1

8.1.34 ospfv3 area

Syntax

ospfv3 *process-id* **area** *area-id* [**instance** *instance-id*]

undo ospfv3 *process-id* **area** *area-id* [**instance** *instance-id*]

デフォルト

無効

View

Interface view

定義済みユーザロール

network-admin

パラメータ

process-id: OSPFv3 プロセスを指定します。設定範囲は 1～65535 です。

area-id: OSPFv3 エリアを IP アドレスあるいは 10 進数の整数のエリア ID で指定します。10 進数の整数の設定範囲は 0～4294967295 です。この 10 進数の整数はシステムで IP アドレスの形式に変換されます。

instance-id: インスタンスの ID を指定します。設定範囲は 0～255 です。デフォルトは 0 です。

説明

ospfv3 area コマンドは OSPFv3 プロセスを有効にし、インタフェースのエリアを設定します。

undo ospfv3 area コマンドは OSPFv3 プロセスを無効にします。

例

エリア 1 の OSPFv3 プロセスのインスタンス 1 を有効にし、VLAN インタフェース 10 を設定します。

<Switch> system-view

[Switch] interface vlan-interface 10

[Switch-Vlan-interface10] ospfv3 1 area 1 instance 1

8.1.35 ospfv3 bfd enable

Syntax

ospfv3 bfd enable [**instance** *instance-id*]

undo ospfv3 bfd enable [**instance** *instance-id*]

デフォルト

無効

View

Interface view

定義済みユーザロール

network-admin

パラメータ

instance-id: インスタンスの ID を指定します。設定範囲は 0～255 です。デフォルトは 0 です。

説明

ospfv3 bfd enable コマンドは OSPFv3 インタフェースで BFD を有効にします。

undo ospfv3 bfd enable コマンドは OSPFv3 インタフェースで BFD を無効にします。

BFD は、ネットワークの収束時間を改善し、OSPFv3 隣接装置間のリンクの接続を早急に検出するメカニズムを提供します。

OSPFv3 は双方向コントロール検出を実装するため BFD を使用します。

例

インスタンス 1 の VLAN インタフェース 11 で BFD を有効にします。

<Switch> system-view

[Switch] interface vlan-interface 11

[Switch-Vlan-interface11] ospfv3 bfd enable instance 1

8.1.36 ospfv3 cost

Syntax

ospfv3 cost *value* [**instance** *instance-id*]

undo ospfv3 cost [**instance** *instance-id*]

デフォルト

VLAN インタフェースのコストは 1 です。loopback インタフェースのコストは 0 です。ほかのインタフェースはインタフェースの帯域幅に従い、コストを計算します。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

value: OSPFv3 のコストを指定します。ループバックインタフェースの設定範囲は 0～65535 です。ほかのインタフェースの設定範囲は 1～65535 です。

instance-id: インスタンスの ID を指定します。設定範囲は 0～255 です。デフォルトは 0 です。

説明

ospfv3 cost コマンドはインスタンスのインタフェースの OSPFv3 のコストを設定します。

undo ospfv3 cost コマンドはデフォルトに戻します。

例

インスタンス 1 の VLAN インタフェース 10 の OSPFv3 のコストを 33 に設定します。

<Switch> system-view

[Switch] interface vlan-interface 10

[Switch-Vlan-interface10] ospfv3 cost 33 instance 1

8.1.37 ospfv3 dr-priority

Syntax

ospfv3 dr-priority *priority* [**instance** *instance-id*]

undo ospfv3 dr-priority [**instance** *instance-id*]

デフォルト

1

View

Interface view

定義済みユーザロール

network-admin

パラメータ

priority: ルータの優先順位を指定します。設定範囲は 0～255 です。

instance-id: インスタンスの ID を指定します。設定範囲は 0～255 です。デフォルトは 0 です。

説明

ospfv3 dr-priority コマンドはインスタンスのルータの優先順位を設定します。

undo ospfv3 dr-priority コマンドはデフォルトに戻します。

インタフェースのルータは DR/BDR の選出を行うために優先順位を決定します。

例

インスタンス 1 の VLAN インタフェース 10 のルータの優先順位を 8 に設定します。

<Switch> system-view

[Switch] interface vlan-interface 10

[Switch-Vlan-interface10] ospfv3 dr-priority 8 instance 1

8.1.38 ospfv3 mtu-ignore

Syntax

ospfv3 mtu-ignore [**instance** *instance-id*]

undo ospfv3 mtu-ignore [**instance** *instance-id*]

デフォルト

有効

View

Interface view

定義済みユーザロール

network-admin

パラメータ

instance-id: インスタンスの ID を指定します。設定範囲は 0～255 です。デフォルトは 0 です。

説明

ospfv3 mtu-ignore コマンドは DD パケットの交換を行う間に MTU チェックをインタフェースで無効にします。

undo ospfv3 mtu-ignore コマンドはデフォルトに戻します。

インタフェースの MTU がピアと同一である場合、隣接関係を確立することができます。

例

DD パケットの交換を行う間に MTU チェックを無効にするため、インスタンス 1 に属している VLAN インタフェース 10 を設定します。

<Switch> system-view

[Switch] interface vlan-interface 10

[Switch-Vlan-interface10] ospfv3 mtu-ignore instance 1

8.1.39 ospfv3 network-type

Syntax

ospfv3 network-type { **broadcast** | **nbma** | **p2mp** [**unicast**] | **p2p** } [**instance** *instance-id*]

undo ospfv3 network-type [**instance** *instance-id*]

デフォルト

デフォルトで OSPFv3 インタフェースのネットワークタイプは、リンクレイヤプロトコルに依存します。

- Ethernet、FDDI のネットワークタイプは broadcast です。
- ATM、FR、X.25 のネットワークタイプは NBMA です。
- PPP、LAPB、HDLC、POS のネットワークタイプは P2P です。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

broadcast: ネットワークタイプを broadcast に指定します。

nbma: ネットワークタイプを NBMA に指定します。

p2mp: ネットワークタイプを P2MP に指定します。

unicast: OSPFv3 パケットをユニキャストするため、P2MP インタフェースを指定します。デフォルトで P2MP インタフェースは OSPFv3 パケットをマルチキャストします。

p2p: ネットワークタイプを P2P に指定します。

instance-id: インスタンスの ID を指定します。設定範囲は 0～255 です。デフォルトは 0 です。

説明

ospfv3 network-type コマンドは OSPFv3 インタフェースのネットワークタイプを設定します。

undo ospfv3 network-type コマンドはデフォルトに戻します。

ブロードキャストネットワークのルータがマルチキャストをサポートしない場合、インタフェースに接続するネットワークタイプは NBMA に設定します。

NBMA ネットワークの 2 つのルータが仮想リンクを通して直接接続している場合、ネットワークはフルメッシュ構成となります。インタフェースに接続するネットワークタイプを NBMA に設定することができます。2 つのルータが直接接続されていない場合、2

つのルータが別のルータを通してルーティング情報を交換できるように P2MP ネットワークタイプを設定します。

インタフェースのネットワークタイプが NBMA あるいは P2MP ユニキャストであるとき、隣接を指定するため、**peer** コマンドを使用する必要があります。

インタフェースのネットワークタイプが P2MP ユニキャストである場合、すべての OSPFv3 パケットはインタフェースでユニキャストされます。

例

VLAN インタフェース 20 の OSPFv3 ネットワークタイプを NBMA に設定します。

<Switch> system-view

[Switch] interface vlan-interface 20

[Switch-Vlan-interface20] ospfv3 network-type nbma

関連コマンド

ospfv3 dr-priority

8.1.40 ospfv3 peer

Syntax

ospfv3 peer *ipv6-address* [**cost** *value* | **dr-priority** *dr-priority*] [**instance** *instance-id*]

undo ospfv3 peer *ipv6-address* [**instance** *instance-id*]

デフォルト

設定なし

View

Interface view

定義済みユーザロール

network-admin

パラメータ

ipv6-address: 隣接のリンクローカル IPv6 アドレスを指定します。

cost *value*: 隣接のコストを指定します。設定範囲は 1～65535 です。

dr-priority *dr-priority*: 隣接の DR 優先度を指定します。設定範囲は 0～255 です。デフォルトは 1 です。

instance *instance-id*: インスタンスの ID を指定します。設定範囲は 0～255 です。デフォルトは 0 です。

説明

ospfv3 peer コマンドは隣接を設定し、隣接の DR 優先度を設定します。

undo ospfv3 peer コマンドは設定を削除します。

NBMA、P2MP インタフェース（ユニキャストモードのみ）において、インタフェースは hello パケットをブロードキャストして隣接を検出することができないため、隣接のリンクローカル IPv6 アドレスを指定する必要があります。NBMA インタフェースでは隣接の DR 優先度も設定する必要があります。

例

VLAN インタフェース 10 で隣接のリンクローカルアドレスを FE80::1111 に設定します。

<Switch> system-view

[Switch] interface vlan-interface 10

[Switch-Vlan-interface10] ospfv3 peer fe80::1111

8.1.41 ospfv3 timer dead

Syntax

ospfv3 timer dead *seconds* [**instance** *instance-id*]

undo ospfv3 timer dead [**instance** *instance-id*]

デフォルト

ブロードキャスト、P2P インタフェースのデフォルト値は 40 秒です。P2MP および NBMA インタフェースのデフォルト値は 120 秒です。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

seconds: dead タイマを指定します。設定範囲は 1～65535 秒です。

説明

ospfv3 timer dead コマンドは OSPFv3 の隣接 dead タイマを設定します。

undo ospfv3 timer dead コマンドはデフォルトに戻します。

インタフェースが隣接から Hello パケットを dead タイマ以内に受信しない場合、インタフェースは隣接がダウンしたと認識します。

インタフェースの dead タイマは少なくとも hello タイマの 4 倍以上にする必要があります。同一セグメントに接続されているルータは同一の dead タイマにする必要があります。

例

VLAN インタフェース 10 の OSPFv3 隣接 dead タイマを 60 秒に設定します。

<Switch> system-view

[Switch] interface vlan-interface 10

[Switch-Vlan-interface10] ospfv3 timer dead 60

関連コマンド

ospfv3 timer hello

8.1.42 ospfv3 timer hello

Syntax

ospfv3 timer hello *seconds* [**instance** *instance-id*]

undo ospfv3 timer hello [**instance** *instance-id*]

デフォルト

ブロードキャスト、P2P インタフェースのデフォルト値は 10 秒です。P2MP および NBMA インタフェースのデフォルト値は 30 秒です。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

seconds: Hello タイマを指定します。設定範囲は 1～65535 秒です。

instance-id: インスタンスの ID を指定します。設定範囲は 0～255 です。デフォルトは 0 です。

説明

ospfv3 timer hello コマンドはインタフェースの Hello タイマを設定します。

undo ospfv3 timer hello コマンドはデフォルトに戻します。

Hello タイマを小さくするとトポロジの収束は早くなりますが、多くのリソースが消費されます。2 つの隣接するインタフェースの Hello タイマは同一にしてください。

例

VLAN インタフェースの Hello タイマを 20 秒に設定します。

<Switch> system-view

[Switch] interface vlan-interface 10

[Switch-Vlan-interface10] ospfv3 timer hello 20

関連コマンド

ospfv3 timer dead

8.1.43 ospfv3 timer poll

Syntax

ospfv3 timer poll *seconds* [**instance** *instance-id*]

undo ospfv3 timer poll [**instance** *instance-id*]

デフォルト

120 秒

View

Interface view

定義済みユーザロール

network-admin

パラメータ

seconds: poll タイマを指定します。設定範囲は 1～65535 秒です。

instance-id: インスタンスの ID を指定します。設定範囲は 0～255 です。デフォルトは 0 です。

説明

ospfv3 timer poll コマンドは NBMA インタフェースの poll タイマを設定します。

undo ospfv3 timer poll コマンドはデフォルトに戻します。

NBMA インタフェースで隣接がダウンしたことを検出するとき、poll タイマの間隔で Hello パケットを送信します。

poll タイマは少なくとも hello タイマの 4 倍以上にする必要があります。

例

VLAN インタフェース 10 の poll タイマを 120 秒に設定します。

<Switch> system-view

[Switch] interface vlan-interface 10

[Switch-Vlan-interface10] ospfv3 timer poll 120

関連コマンド

ospfv3 timer hello

8.1.44 ospfv3 timer retransmit

Syntax

ospfv3 timer retransmit *seconds* [**instance** *instance-id*]

undo ospfv3 timer retransmit [**instance** *instance-id*]

デフォルト

5 秒

View

Interface view

定義済みユーザロール

network-admin

パラメータ

seconds: LSA の再送間隔を指定します。設定範囲は 1～3600 秒です。

instance-id: インスタンスの ID を指定します。設定範囲は 0～255 です。デフォルトは 0 です。

説明

ospfv3 timer retransmit コマンドはインタフェースで LSA を再送する間隔を設定します。

undo ospfv3 timer retransmit コマンドはデフォルトに戻します。

LSA を送信したのち、インタフェースは acknowledgment パケットを待ちます。インタフェースが再送間隔以内に acknowledgment パケットを受信しない場合、LSA を再送します。

LSA パケットの不必要な再送を防ぐため、適切な再送間隔を設定してください。たとえば低速リンクの再送間隔は大きくします。

例

インスタンス 1 の VLAN インタフェース 10 の LSA 再送間隔を 12 秒に設定します。

<Switch> system-view

[Switch] interface vlan-interface 10

[Switch-Vlan-interface10] ospfv3 timer retransmit 12 instance 1

8.1.45 ospfv3 trans-delay

Syntax

ospfv3 trans-delay *seconds* [**instance** *instance-id*]

undo ospfv3 trans-delay [**instance** *instance-id*]

デフォルト

1 秒

View

Interface view

定義済みユーザロール

network-admin

パラメータ

seconds: LSA の伝送遅延を指定します。設定範囲は 1～3600 秒です。

instance-id: インスタンスの ID を指定します。設定範囲は 0～255 です。デフォルトは 0 です。

説明

ospfv3 trans-delay コマンドはインタフェースの LSA の伝送遅延を設定します。

undo ospfv3 trans-delay コマンドはデフォルトに戻します。

LSDB の各 LSA のエージングタイマは 1 秒ごとに増加しますが、送信する間、エージングタイマは変更しません。低速ネットワークではエージング時間に伝送遅延を追加することが必要となります。

例

インスタンス 1 の VLAN インタフェース 10 の LSA 伝送遅延を 3 秒に設定します。

<Switch> system-view

[Switch] interface vlan-interface 10

[Switch-Vlan-interface10] ospfv3 trans-delay 3 instance 1

8.1.46 preference

Syntax

preference [**ase**] [**route-policy** *route-policy-name*] *preference*

undo preference [**ase**]

デフォルト

OSPFv3 内部ルートの優先順位は 10 です。OSPFv3 外部ルートの優先順位は 150 です。

View

OSPFv3 view

定義済みユーザロール

network-admin

パラメータ

ase: OSPFv3 外部ルートの優先順位を指定します。指定しない場合、OSPFv3 内部ルートの優先順位を設定します。

route-policy *route-policy-name*: 指定したルートの優先順位を設定するためにルーティングポリシーを指定します。設定範囲は 1～63 文字です。大文字、小文字を区別します。

preference: OSPFv3 の優先順位を指定します。設定範囲は 1～255 です。値が小さければ、優先順位は高くなります。

説明

preference コマンドは OSPFv3 の優先順位を設定します。

undo preference コマンドはデフォルトに戻します。

複数のルーティングプロトコルが同一宛先への複数のルートを検出した場合、ルータはもっとも高い優先順位のプロトコルのルートを使用します。

例

OSPFv3 ルートの優先順位を 150 に設定します。

<Switch> system-view

[Switch] OSPFv3

[Switch-OSPFv3-1] preference 150

8.1.47 reset ospfv3 process

Syntax

reset ospfv3 [*process-id*] **process** [**graceful-restart**]

View

User view

定義済みユーザロール

network-admin

パラメータ

process-id: OSPFv3 プロセスを指定します。設定範囲は 1～65535 です。指定しない場合、すべての OSPFv3 プロセスを再起動します。

graceful-restart: GR を使用して OSPFv3 プロセスを再起動します。

説明

reset ospfv3 process コマンドは OSPFv3 プロセスを再起動します。

reset ospfv3 process コマンドは以下のアクションを実行します。

- タイマのタイムアウトを待つことなく、すべての異常な LSA を削除します。
- 新しく設定されたルータ ID を適用します。
- 新しい DR、BDR の選定を開始します。
- 以前の OSPFv3 の設定を保持します。

システムは OSPFv3 プロセスの実行を開始するかどうかの選択メッセージを表示します。

例

OSPFv3 プロセスを再起動します。

<Switch> reset ospfv3 process

```
Reset OSPFv3 process? [Y/N]:y
```

8.1.48 reset ospfv3 redistribution

Syntax

reset ospfv3 [*process-id*] **redistribution**

View

User view

定義済みユーザロール

network-admin

パラメータ

process-id: OSPFv3 プロセスを指定します。設定範囲は 1～65535 です。指定しない場合、すべての OSPFv3 プロセスのルートの再配信を再スタートします。

説明

reset ospfv3 redistribution コマンドはルートの再配信を再スタートします。

例

ルートの再配信を再スタートします。

<Switch> reset ospfv3 redistribution

8.1.49 reset ospfv3 statistics

Syntax

reset ospfv3 [*process-id*] **statistics**

View

User view

定義済みユーザロール

network-admin

パラメータ

process-id: OSPFv3 プロセスを指定します。設定範囲は 1～65535 です。指定しない場合、すべての OSPFv3 プロセスの統計情報を削除します。

説明

reset ospfv3 statistics コマンドは OSPFv3 の統計情報を削除します。

例

すべての OSPFv3 プロセスの統計情報を削除します。

<Switch> reset ospfv3 statistics

8.1.50 router-id

Syntax

router-id *router-id*

undo router-id

デフォルト

設定なし

View

OSPFv3 view

定義済みユーザロール

network-admin

パラメータ

router-id: IPv4 アドレス形式でルータ ID を指定します。

説明

router-id コマンドはグローバルのルータ ID を設定します。

undo router-id コマンドはグローバルのルータ ID を削除します。

ルータ ID は AS で OSPFv3 が動作する装置を識別するために使用します。OSPFv3 プロセスはルータ ID なしで実行することができません。

異なるプロセスは異なるルータ ID にする必要があります。

例

OSPFv3 プロセス 1 のルータ ID を 10.1.1.3 に設定します。

<Switch> system-view

[Switch] ospfv3 1

[Switch-ospfv3-1] router-id 10.1.1.3

関連コマンド

ospfv3

8.1.51 silent-interface(OSPFv3 view)

Syntax

silent-interface { *interface-type interface-number* | **all** }

undo silent-interface { *interface-type interface-number* | **all** }

デフォルト

設定なし

View

OSPFv3 view

定義済みユーザロール

network-admin

パラメータ

interface-type interface-number: インタフェースのタイプと番号を指定します。

all: すべてのインタフェースを指定します。

説明

silent-interface コマンドは指定したインタフェースあるいはすべてのインタフェースで OSPFv3 パケットの送受信を無効にします。

undo silent-interface コマンドはデフォルトに戻します。

複数のプロセスは OSPFv3 パケットの送受信を行う同一のインタフェースを無効にすることができます。しかし **silent-interface** コマンドは現在のプロセスで有効なインタフェースのみ適用します。

例

OSPFv3 プロセス 100、200 で OSPFv3 パケットの送受信を行う VLAN インタフェース 10 を無効にします。

```
<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
```

8.1.52 snmp-agent trap enable 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] *

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

パラメータ

grrestarter-status-change: GR リスタータの変更の通知を指定します。

grhelper-status-change: GR ヘルパーの変更の通知を指定します。

if-state-change: インタフェースの状態の変更の通知を指定します。

if-cfg-error: インタフェースのエラー設定の通知を指定します。

if-bad-pkt: インタフェースで受信したエラーメッセージの通知を指定します。

neighbor-state-change: 隣接状態の変更の通知を指定します。

nssatranslator-status-change: NSSA 転送状態の変更の通知を指定します。

virtif-bad-pkt: 仮想インタフェースで受信したエラーメッセージの通知を指定します。

virtif-cfg-error: 仮想インタフェースのエラー設定の通知を指定します。

virtif-state-change: 仮想インタフェースの状態の変更の通知を指定します。

virtgrhelper-status-change: 仮想インタフェースの GR ヘルパーの状態の変更の通知を指定します。

virtneighbor-state-change: 仮想インタフェースの隣接状態の変更の通知を指定します。

説明

snmp-agent trap enable ospfv3 コマンドは OSPFv3 の SNMP 通知を有効にします。

undo snmp-agent trap enable ospfv3 コマンドは OSPFv3 の SNMP 通知を無効にします。

例

OSPFv3 の SNMP 通知を無効にします。

<Switch> system-view

[Switch] undo snmp-agent trap enable ospfv3

8.1.53 spf-schedule-interval

Syntax

spf-schedule-interval *maximum-interval* [*minimum-interval* [*incremental-interval*]]

undo spf-schedule-interval

デフォルト

ルート計算の最大間隔は 5 秒、最小間隔は 50 ミリ秒、増加する間隔は 200 ミリ秒です。

View

OSPFv3 view

定義済みユーザロール

network-admin

パラメータ

maximum-interval: OSPFv3 ルート計算の最大間隔を指定します。設定範囲は 1～60 秒です。

minimum-interval: OSPFv3 ルート計算の最小間隔を指定します。設定範囲は 10～60000 ミリ秒です。

incremental-interval: OSPFv3 ルート計算の増加する間隔を指定します。設定範囲は 10～60000 ミリ秒です。

説明

spf-schedule-interval コマンドは OSPFv3 SPF 計算の間隔を設定します。

undo spf-schedule-interval コマンドはデフォルトに戻します。

LSDB にもとづいて、OSPFv3 ルータはルートとして OSPFv3 ルータの最小パスツリーを計算するため、SPF を使用します。OSPFv3 は宛先へのネクストホップを決定するため、最小のパスツリーを使用します。SPF 計算間隔を調整することによって、頻繁にトポロジが変更することにより、帯域幅とルータのリソースの過剰な消費を防止することができます。

安定したネットワークでは最小間隔が使用されます。頻繁にネットワークが変更する場合、SPF を計算する間隔は最大間隔に到達するまで、各計算を行う際に増加する間隔を追加していきます。

最小間隔と増加する間隔は、最大間隔よりも小さくする必要があります。

例

SPF 計算の最大間隔を 10 秒、最小間隔を 500 ミリ秒、増加する間隔を 300 ミリ秒に設定します。

<Switch> system-view

[Switch] ospfv3 100

[Switch-ospfv3-100] spf-schedule-interval 10 500 300

8.1.54 stub (OSPFv3 area view)

Syntax

stub [**default-route-advertise-always** | **no-summary**] *

undo stub

デフォルト

設定なし

View

OSPFv3 area view

定義済みユーザロール

network-admin

パラメータ

default-route-advertise-always: ABR は常にデフォルトルートをスタブエリアに配信するように ABR を有効にします。

no-summary: 外部エリアプレフィックス LSA のデフォルトルートのみ、スタブエリアに配信するようにスタブ ABR の ABR を有効にします。エリアの AS 外部 LSA、内部エリアプレフィックス LSA やほかの外部エリアルータ LSA は配信されません。この種類のスタブエリアは完全スタブエリアとして知られています。

説明

stub コマンドはスタブエリアとしてエリアを設定します。

undo stub コマンドはデフォルトに戻します。

ABR で **no-summary** の設定を削除する場合、設定を上書きするため、再度 **stub** コマンドを設定します。

スタブエリアとしてエリアを設定する場合、エリアに接続しているすべてのルータで **stub** コマンドを設定します。

例

スタブエリアとして OSPFv3 エリア 1 を設定します。

<Switch> system-view

[Switch] ospfv3 1

[Switch-ospfv3-1] area 1

[Switch-ospfv3-1-area-0.0.0.1] stub

関連コマンド

default-cost (OSPFv3 area view)

8.1.55 vlink-peer (OSPFv3 area view)

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**] *

デフォルト

設定なし

View

OSPFv3 area view

定義済みユーザロール

network-admin

パラメータ

router-id: 仮想リンクの隣接のルータ ID を指定します。

dead *seconds*: dead タイマを指定します。設定範囲は 1～32768 秒です。デフォルトは 40 秒です。dead タイマは仮想リンクの隣接間で同一にする必要があります。少なくとも Hello タイマの 4 倍にする必要があります。

hello *seconds*: hello 間隔を指定します。設定範囲は 1～8192 秒です。デフォルトは 10 秒です。仮想リンクの隣接間で同一にする必要があります。

instance *instance-id*: 仮想リンクのインスタンス ID を指定します。設定範囲は 0～255 です。デフォルトは 0 です。

retransmit *seconds*: 再配信する間隔を指定します。設定範囲は 1～3600 秒です。デフォルトは 5 です。

trans-delay *seconds*: 伝送遅延を指定します。設定範囲は 1～3600 秒です。デフォルトは 1 秒です。

説明

vlink-peer コマンドは仮想リンクを設定します。

undo vlink-peer コマンドは仮想リンクを削除します。

非バックボーンエリアとバックボーン間の接続を維持する、あるいはバックボーン内の接続を維持するため、仮想リンクを設定することができます。仮想リンクは OSPFv3 が有効なインタフェースとみなすことができます。仮想リンクで **hello**、**dead**、**retransmit**、**trans-delay** のようなパラメータを設定することができます。

仮想リンクの両端は **vlink-peer** コマンドが設定された ABR にする必要があります。

パラメータを適用するため、以下のガイドラインに従ってください。

- Hello 間隔が短くなると、ネットワークの収束が早くなりますが、ネットワークのリソースの消費が大きくなります。
- 再配信する間隔が小さすぎる場合、不必要な再配信が発生する可能性があります。低速のリンクの場合、大きい値にしてください。
- **trans-delay** パラメータで適切に伝送遅延を設定してください。

例

仮想リンクを 10.10.0.3 に設定します。

<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

関連コマンド

display ospfv3 vlink

目次

このセクションのページは **5-x-x** です。

9 章 IPv6 ポリシーベースルーティング 9-1
9.1 IPv6 ポリシーベースルーティング設定コマンド 9-1
9.1.1 apply next-hop 9-1
9.1.2 description 9-2
9.1.3 display ipv6 policy-based-route 9-2
9.1.4 display ipv6 policy-based-route interface 9-4
9.1.5 display ipv6 policy-based-route setup 9-6
9.1.6 if-match acl 9-7
9.1.7 ipv6 local policy-based-route 9-8
9.1.8 ipv6 policy-based-route (interface view) 9-9
9.1.9 ipv6 policy-based-route (system view) 9-10
9.1.10 reset ipv6 policy-based-route statistics 9-11

9章 IPv6 ポリシーベースルーティング

9.1 IPv6 ポリシーベースルーティング設定コマンド

9.1.1 apply next-hop

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>]

デフォルト

設定なし

View

IPv6 policy node view

定義済みユーザロール

network-admin

パラメータ

vpn-instance *vpn-instance-name*：VPN インスタンスを名前で指定します。大文字小文字を区別し、設定範囲は 1～31 文字です。指定の VPN インスタンスはすでに存在していなくてはなりません。

Ipv6-address: ネクストホップの IPv6 アドレスを指定します。

direct: 直接接続されているネクストホップを指定します。

track *track-entry-number*: Track エントリを指定します。設定範囲は 1～1024 です。

&<1-2>: 引数を最大 2 回まで設定できることを示します。

説明

apply next-hop コマンドはネクストホップを設定します。

undo apply next-hop コマンドは設定を削除します。

バックアップあるいはロードシェアリングのために、このコマンドを繰り返し設定することで、ネクストホップを複数指定することができます。

ネクストホップを指定して **undo apply next-hop** コマンドを使用すると、ネクストホップを削除します。

ネクストホップを指定せずにこのコマンドを使用すると、すべてのデフォルトのネクストホップを削除します。

例

直接接続された 1.1.1.1 をネクストホップに設定します。

<Switch> system-view

[Switch] ipv6 policy-based-route aa permit node 11

[Switch-pbr6-aa-11] apply next-hop 1::1

9.1.2 description

Syntax

description *text*

undo description

デフォルト

設定なし

View

IPv6 policy node view

定義済みユーザロール

network-admin

パラメータ

text: 説明を指定します。設定範囲は 1～127 文字です。大文字、小文字を区別します。

説明

description コマンドはポリシーノードの説明を設定します。

undo description コマンドはデフォルトに戻します。

例

ポリシーノード 1 の **Officeuse** という記述を設定検索します。

<Switch> system-view

[Switch] policy-based-route 1 permit node 1

[Switch-pbr-1-1] description Officeuse

9.1.3 display ipv6 policy-based-route

Syntax

display ipv6 policy-based-route [**policy** *policy-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

policy *policy-name*: ポリシーの名前を指定します。設定範囲は 1～19 です。大文字、小文字を区別します。ポリシーを指定しない場合、このコマンドはすべての IPv6 PBR ポリシーの情報を表示します。

説明

display ipv6 policy-based-route コマンドは PBR ポリシー情報を表示します。

例

すべてのポリシーの情報を表示します。

<Switch> display ipv6 policy-based-route

```
Policy name: aaa
  node 1 permit:
    if-match acl 2000
    apply next-hop 1000::1
```

表 9-1 コマンド出力

フィールド	説明
node 1 permit	ノード1にマッチするモードが許可されています。
if-match acl	パケットをACLと比較します。
apply next-hop	許可されたパケットのネクストホップを指定します。

関連コマンド

Ipv6 policy-based-route (system view)

9.1.4 display ipv6 policy-based-route interface

Syntax

display ipv6 policy-based-route interface *interface-type interface-number* [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface-type interface-number: インタフェースタイプと番号を指定します。

slot *slot-number*: メンバ ID によって IRF スタックメンバ装置を指定します。メンバ装置を指定しない場合、このコマンドはマスタ装置の情報を表示します。

説明

display ipv6 policy-based-route interface コマンドはインタフェースの PBR 設定情報と統計情報を表示します。

例

VLAN インタフェース 2 の IPv6 PBR 設定情報と統計情報を表示します。

<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
```

表 9-2 コマンド出力

フィールド	説明
Policy based routing information for interface XXXX(failed)	統計情報のIPv6 PBR設定とインタフェースです。 ポリシー内のどのノードもドライバに正常に発行されなかった場合、このフィールドには 「**failed**」が括弧内に表示されます。 グローバルインタフェース (VLAN-interface 10などの一次元インタフェース番号のみ)の場合、**failed**と表示されるのは、コマンドにスロット情報を指定している場合だけです。
node 0 deny node 2 permit	ノードのマッチモードで、**permit**あるいは**deny**があります。 ノードをドライバに発行できない場合は、次のような原因が角かっこで囲まれて表示されます。 ● **not support**—ノードで設定されたマッチ基準を装置がサポートしていないことを示します。 ● **no resource**—ACLリソースが不十分で、ノードにACLリソースを割り当てることができないことを示します。 グローバルインタフェース（VLAN-interface 10などの1次元インタフェース番号のみ）の場合、サポートなし、およびリソースなしは、コマンドのスロット情報を指定した場合のみ表示されます。
if-match acl	IPv6パケットをIPv6 ACLと比較します。
apply next-hop	許可されたIPv6パケットのネクストホップを指定します。

フィールド	説明
Matched: 0	ノードでマッチした数です。（統計リソースがない場合は、統計リソースが不十分であることを示します）。 グローバルインタフェース（VLAN-interface 10などの1次元インタフェース番号のみ）の場合、コマンドのスロット情報を指定する場合のみ、統計情報リソースを表示できません。
Total matched	すべてのノードでマッチした総数です。

関連コマンド

reset ipv6 policy-based-route statistics

9.1.5 display ipv6 policy-based-route setup

Syntax

display ipv6 policy-based-route setup

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display ipv6 policy-based-route setup コマンドは PBR 設定を表示します。

例

IPv6 PBR 設定を表示します。

<Switch> display ipv6 policy-based-route setup

```
Policy name            Type     Interface
pr01                  Forward  Vlan-interface2
pr02                   Local    N/A
```

表 9-3 コマンド出力

フィールド	説明
Policy name	ポリシー名です。
Type	PBRのタイプです。 ● **Forward**—インタフェースPBRです。 ● **Local**—ローカルPBRです。
Interface	ポリシーが適用されるインタフェースです。

関連コマンド

Ipv6 policy-based-route (interface view)

9.1.6 if-match acl

Syntax

if-match acl { *ipv6-acl-number* | **name** *ipv6-acl-name* }

undo if-match acl

デフォルト

設定なし

View

IPv6 policy node view

定義済みユーザロール

network-admin

パラメータ

ipv6-acl-number: ACL の番号を指定します。標準 IPv6 ACL の設定範囲は 2000～2999 です。拡張 IPv6 ACL の設定範囲は 3000～3999 です。

name *ipv6-acl-name*: IPv6 ACL の名前を指定します。設定範囲は 1～63 です。大文字、小文字を区別しません。IPv6 ACL の名前の先頭は *a*～*z*、*A*～*Z* の英字です。コマンドを有効にするには、指定した IPv6 ACL が標準 ACL または拡張 ACL であることを確認してください。

説明

if-match acl コマンドは IPv6 ACL マッチ基準を設定します。

undo if-match acl コマンドはデフォルトに戻します。

例

#ACL 2011 にマッチするパケットを許可するポリシー**aa** のノード 11 を設定します。

<Switch> system-view

[Switch] ipv6 policy-based-route aa permit node 11

[Switch-pbr-aa-11] if-match acl 2011

#ACL 名 **aaa** の ACL にマッチするパケットを許可するポリシー**aa** のノード 11 を設定します。

<Switch> system-view

[Switch] ipv6 policy-based-route aa permit node 11

[Switch-pbr-aa-11] if-match acl name aaa

9.1.7 ipv6 local policy-based-route

Syntax

Ipv6 local policy-based-route *policy-name*

undo ipv6 local policy-based-route

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

policy-name: ポリシー名を指定します。設定範囲は 1～19 です。大文字、小文字を区別します。ポリシーは既に作成されている必要があります。

説明

ipv6 local policy-based-route コマンドはローカル IPv6 PBR のポリシーを指定します。

undo ipv6 local policy-based-route コマンドはデフォルトに戻します。

ローカル IPv6 PBR は、**ping** コマンドを使用して生成された ICMP パケットなど、ローカルに生成されたパケットの転送をガイドします。

ローカル IPv6 PBR は、ping や Telnet などのローカルサービスに影響を与える可能性があります。ローカル IPv6 PBR を使用する場合は、装置のローカルサービスへの影響を十分に理解してください。

ローカル IPv6 PBR に指定できるポリシーは 1 つだけで、指定したポリシーがすでに存在することを確認する必要があります。

新しいポリシーを適用する前に、現在のポリシーを削除する必要があります。

例

ポリシー**aaa** にもとづいてローカル PBR を設定します。

<Switch> system-view

[Switch] ipv6 local policy-based-route aaa

関連コマンド

- **display ipv6 policy-based-route setup**
- **ipv6 policy-based-route (system view)**

9.1.8 ipv6 policy-based-route (interface view)

Syntax

ipv6 policy-based-route *policy-name*

undo ipv6 policy-based-route

デフォルト

設定なし

View

Interface view

定義済みユーザロール

network-admin

パラメータ

policy-name: ポリシー名を指定します。設定範囲は 1～19 です。大文字、小文字を区別します。ポリシーは既に作成されている必要があります。

説明

ipv6 policy-based-route コマンドはインタフェース上のインタフェース PBR のポリシーを指定します。

undo ipv6 policy-based-route コマンドはデフォルトに戻します。

例

VLAN インタフェース 2 にポリシー**aaa** を適用します。

<Switch> system-view

[Switch] interface vlan-interface 2

[Switch-Vlan-interface2] ipv6 policy-based-route aaa

関連コマンド

- **display ipv6 policy-based-route setup**
- **ipv6 policy-based-route (system view)**

9.1.9 ipv6 policy-based-route (system view)

Syntax

ipv6 policy-based-route *policy-name* [**deny** | **permit**] **node** *node-number*

undo ipv6 policy-based-route *policy-name* [**deny** | **node** *node-number* | **permit**]

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

policy-name: ポリシー名を指定します。設定範囲は 1～19 です。大文字、小文字を区別します。

deny: ポリシーのマッチモードを **deny** に指定します。

permit: ポリシーのマッチモードを **permit** に指定します。（デフォルトモード）

node *node-number*: ポリシーノードを指定します。設定範囲は 0～255 です。値を小さくすると優先度が高くなります。

説明

ipv6 policy-based-route コマンドはポリシーノードを作成し、そのビューに移行するか、デフォルトのポリシーノードのビューに移行します。

undo ipv6 policy-based-route コマンドはポリシーノードを削除します。

インタフェースあるいはローカルに適用されたポリシーは削除することができません。削除する場合、最初にインタフェースあるいはローカルからポリシーベースの PBR の適用を削除してください。

- ポリシーノードが指定されている場合、**undo ipv6 policy-based-route** コマンドは指定されたノードのポリシーを削除します。

- マッチモードが指定されている場合、コマンドはマッチモードに設定されたすべてのノードを削除します。
- ポリシーノードあるいはマッチモードが指定されていない場合、コマンドはポリシー全体を削除します

例

ノード 10 の許可モードのポリシー**policy1** を作成し、policy node view に移行します。

<Switch> system-view

[Switch] ipv6 policy-based-route policy1 permit node 10

[Switch-pbr-policy1-10]

関連コマンド

display ipv6 policy-based-route

9.1.10 reset ipv6 policy-based-route statistics

Syntax

reset ipv6 policy-based-route statistics [**policy** *policy-name*]

View

User view

定義済みユーザロール

network-admin

パラメータ

policy *policy-name*: ポリシー名を指定します。設定範囲は 1～19 です。大文字、小文字を区別します。ポリシーを指定しない場合、このコマンドはすべてのポリシーの IPv6 PBR 統計情報を削除します。

説明

reset ipv6 policy-based-route statistics コマンドは PBR の統計情報を削除します。

例

すべての PBR の統計情報を削除します。

<Switch> reset ipv6 policy-based-route statistics

関連コマンド

- **display ip policy-based-route interface**

目次

このセクションのページは **5-x-x** です。

10 章 ルーティングポリシー.....10-1
10.1 共通ルーティングポリシー設定コマンド.....10-1
10.1.1 apply cost.....10-1
10.1.2 apply cost-type.....10-2
10.1.3 apply preference.....10-2
10.1.4 apply tag.....10-3
10.1.5 display route-policy.....10-4
10.1.6 if-match cost.....10-5
10.1.7 if-match interface.....10-6
10.1.8 if-match route-type.....10-7
10.1.9 if-match tag.....10-8
10.1.10 route-policy.....10-8
10.2 IPv4 ルーティングポリシー設定コマンド.....10-10
10.2.1 apply ip-address next-hop.....10-10
10.2.2 display ip prefix-list.....10-11
10.2.3 if-match ip.....10-12
10.2.4 ip prefix-list.....10-13
10.2.5 reset ip prefix-list.....10-15
10.3 IPv6 ルーティングポリシー設定コマンド.....10-15
10.3.1 apply ipv6 next-hop.....10-15
10.3.2 display ipv6 prefix-list.....10-16
10.3.3 if-match ipv6.....10-17
10.3.4 ipv6 prefix-list.....10-18
10.3.5 reset ipv6 prefix-list.....10-20

10章 ルーティングポリシー

10.1 共通ルーティングポリシー設定コマンド

10.1.1 apply cost

Syntax

apply cost [+ | **-**] *value*

undo apply cost

デフォルト

設定なし

View

Routing policy node view

定義済みユーザロール

network-admin

パラメータ

+: コストを増加します。

-: コストを減少させます。

value: コストを指定します。設定範囲は 0～4294967295 です。

説明

apply cost コマンドはルートのコストを設定します。

undo apply cost コマンドはデフォルトに戻します。

例

ルーティングポリシー**policy1** の permit モードのノード 10 で、OSPF 外部ルートのコストを 120 に設定します。

<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

10.1.2 apply cost-type

Syntax

apply cost-type { **type-1** | **type-2** }

undo apply cost-type

デフォルト

設定なし

View

Routing policy node view

定義済みユーザロール

network-admin

パラメータ

type-1: OSPF Type-1 外部ルートにコストタイプを指定します。

type-2: OSPF Type-2 外部ルートにコストタイプを指定します。

説明

apply cost-type コマンドはルートのコストタイプを設定します。

undo apply cost-type コマンドはデフォルトに戻します。

例

ルーティングポリシー**policy1** の permit モードのノード 10 で、タグが 8 のルートを持つ場合、ルートのコストタイプを OSPF Type-1 外部ルートに設定します。

<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

10.1.3 apply preference

Syntax

apply preference *preference*

undo apply preference

デフォルト

設定なし

View

Routing policy node view

定義済みユーザロール

network-admin

パラメータ

preference: プリファレンスを指定します。設定範囲は 1～255 です。

説明

apply preference コマンドはルーティングプロトコルのプリファレンスを設定します。

undo apply preference コマンドはデフォルトに戻します。

preference コマンドを使用してルーティングプロトコルにプリファレンスを設定する場合、**apply preference** コマンドを使用するとマッチするルーティングプロトコルに新しいプリファレンスが設定されます。マッチしないルーティングプロトコルには、既に **preference** コマンドで設定されたプリファレンスが使用されます。

例

ルーティングポリシー**policy1** の permit モードのノード 10 で、OSPF 外部ルートのプリファレンスを 90 に設定します。

<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

10.1.4 apply tag

Syntax

apply tag *value*

undo apply tag

デフォルト

設定なし

View

Routing policy node view

定義済みユーザロール

network-admin

パラメータ

value: タグを指定します。設定範囲は 0～4294967295 です。

説明

apply tag コマンドは IGP ルートの指定されたタグを設定します。

undo apply tag コマンドはデフォルトに戻します。

例

ルーティングポリシー**policy1** の permit モードのノード 10 でタグを 100 に設定します。

<Switch> system-view

[Switch] route-policy policy1 permit node 10

[Switch-route-policy-policy1-10] apply tag 100

10.1.5 display route-policy

Syntax

display route-policy [**name** *route-policy-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

name *route-policy-name*: ルーティングポリシーを指定します。設定範囲は 1～63 文字です。大文字、小文字を区別します。指定しない場合、すべてのルーティングポリシーを表示します。

説明

display route-policy コマンドはルーティングポリシーの情報を表示します。

例

ルーティングポリシー1 の情報を表示します。

<Switch> display route-policy name policy1

```
Route-policy: policy1
  permit : 1
         if-match cost 10
```

```
continue: next node 11
apply comm-list a delete
```

表 10-1 コマンド出力

フィールド	説明
Route-policy	ルーティングポリシーの名前です。
permit	マッチモードです。 ● **permit**ー許可モードです。 ● **deny**ー拒否モードです。
if-match	マッチ条件です。
continue	マッチされるネクストノードを指定します。
apply	アクションです。

10.1.6 if-match cost

Syntax

if-match cost *value*

undo if-match cost

デフォルト

設定なし

View

Routing policy node view

定義済みユーザロール

network-admin

パラメータ

value: コストを指定します。設定範囲は 0～4294967295 です。

説明

if-match cost コマンドは指定されたコストを持つルートにマッチするルートを定義します。

undo if-match cost コマンドはデフォルトに戻します。

例

ルーティングポリシー**policy1** の **permit** モードのノード 10 で、コスト 8 のルートを許可するルートを設定します。

<Switch> system-view

[Switch] route-policy policy1 permit node 10

[Switch-route-policy-policy1-10] if-match cost 8

10.1.7 if-match interface

Syntax

if-match interface { *interface-type interface-number* }&<1-16>

undo if-match interface [*interface-type interface-number*]&<1-16>

デフォルト

設定なし

View

Routing policy node view

定義済みユーザロール

network-admin

パラメータ

interface-type interface-number: インタフェースのタイプと番号を指定します。

&<1-16>: &<1-16>は VLAN インタフェース番号を 16 個まで指定できることを示します。

説明

if-match interface コマンドは指定された出力インタフェースにマッチするルートを定義します。

undo if-match interface コマンドは設定を削除します。

例

ルーティングポリシー**policy1** の **permit** モードのノード 10 で、出力 VLAN インタフェース 1 のルートを許可します。

<Switch> system-view

[Switch] route-policy policy1 permit node 10

[Switch-route-policy-policy1-10] if-match interface vlan-interface 1

10.1.8 if-match route-type

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**] *

デフォルト

設定なし

View

Routing policy node view

定義済みユーザロール

network-admin

パラメータ

external-type1: OSPF Type-1 外部ルートにマッチします。

external-type1or2: OSPF Type-1 外部ルート、Type-2 外部ルートにマッチします。

external-type2: OSPF Type-2 外部ルートにマッチします。

internal: OSPF 内部ルートにマッチします。（OSPF 内部エリアルート、OSPF 外部ルートを含みます）

nssa-external-type1: OSPF NSSA Type-1 外部ルートにマッチします。

nssa-external-type1or2: OSPF NSSA Type-1 外部ルート、NSSA Type-2 外部ルートにマッチします。

nssa-external-type2: OSPF NSSA Type-2 外部ルートにマッチします。

説明

if-match route-type コマンドはルートタイプのマッチ条件を設定します。

undo if-match route-type コマンドは設定を削除します。

例

ルーティングポリシー**policy1** の **permit** モードのノード 10 で、OSPF 内部ルートにマッチするように設定します。

<Switch> system-view

[Switch] route-policy policy1 permit node 10

[Switch-route-policy-policy1-10] if-match route-type internal

10.1.9 if-match tag

Syntax

if-match tag *value*

undo if-match tag

デフォルト

設定なし

View

Routing policy node view

定義済みユーザロール

network-admin

パラメータ

value: タグを指定します。設定範囲は 0～4294967295 です。

説明

if-match tag コマンドは指定されたタグを持つ IGP ルートにマッチするルートを定義します。

undo if-match tag コマンドはデフォルトに戻します。

例

ルーティングポリシー**policy1** の **permit** モードのノード 10 で、タグが 8 の IGP ルートにマッチするルートを設定します。

<Switch> system-view

[Switch] route-policy policy1 permit node 10

[Switch-route-policy-policy1-10] if-match tag 8

10.1.10 route-policy

Syntax

route-policy *route-policy-name* { **deny** | **permit** } **node** *node-number*

undo route-policy *route-policy-name* [**deny** | **permit**] [**node** *node-number*]

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

route-policy-name: ルーティングポリシーを指定します。設定範囲は 1～63 文字です。大文字、小文字を区別します。

deny: ルーティングポリシーノードのマッチモードを拒否します。ルートがノードのすべての **if-match** にマッチする場合、ルートは次のノードに対してマッチさせることなく拒否されます。ルートがノードのすべての **if-match** にマッチしない場合、ルートは次のノードに対してマッチさせます。

permit: ルーティングポリシーノードのマッチモードを許可します。ルートがノードのすべての **if-match** にマッチする場合、ノードの **apply** を処理します。ルートがノードのすべての **if-match** にマッチしない場合、ルートは次のノードに対してマッチさせます。

node *node-number*: ノードの番号を指定します。設定範囲は 0～65535 です。最初にもっとも小さい番号のノードがマッチされます。

説明

route-policy コマンドはルーティングポリシーとノードを作成し、routing policy node view に移行します。

undo route-policy コマンドはルーティングポリシーあるいはルーティングポリシーのノードを削除します。

ルーティング情報をフィルタするためにルーティングポリシーを使用します。ルーティングポリシーは、いくつかのノードがあり、各ノードは **if-match** と **apply** のセットで構成されます。**if-match** はノードのマッチ条件を定義します。**apply** は条件にマッチするパケットのアクションを定義します。

ノードの **if-match** 間の関係は論理積です。ルーティング情報は、すべての **if-match** を満たす必要があります。**if-match** 間の関係は論理和です。ルーティング情報は、すべての **if-match** を満たす必要があります。ノード間の関係は論理和です。ノードをパスしたパケットはルーティンポリシーにパスします。

例

ルーティングポリシー**policy1** の **permit** モードのノード 10 を作成し、routing policy node view に移行します。

<Switch> system-view

[Switch] route-policy policy1 permit node 10

[Switch-route-policy-policy1-10]

関連コマンド

display route-policy

10.2 IPv4ルーティングポリシー設定コマンド

10.2.1 apply ip-address next-hop

Syntax

apply ip-address next-hop *ip-address* [**public** | **vpn-instance** *vpn-instance-name*]

undo apply ip-address next-hop

デフォルト

設定なし

View

Routing policy node view

定義済みユーザロール

network-admin

パラメータ

ip-address: ネクストホップの IP アドレスを指定します。

public: パブリックネットワークを指定します。

vpn-instance *vpn-instance-name*: VPN インスタンスを指定します。設定範囲は 1～31 文字です。大文字、小文字を区別します。

説明

apply ip-address next-hop コマンドは IPv4 ルートのネクストホップを設定します。

undo apply ip-address next-hop コマンドはデフォルトに戻します。

コマンドは再配信されたルートのネクストホップを設定することができません。

public パラメータあるいは **vpn-instance** *vpn-instance-name* パラメータを指定しない場合、ネクストホップはパブリックネットワークに属します。

例

コスト 8にマッチするルートのネクストホップ 193.1.1.8 指定するようにルーティングポリシー**policy1** の **permit** モードのノード 10 を設定します。

```
<Switch> system-view
[Switch] route-policy policy1 permit node 10
[Switch-route-policy-policy1-10] if-match cost 8
[Switch-route-policy-policy1-10] apply ip-address next-hop 193.1.1.8
```

10.2.2 display ip prefix-list

Syntax

display ip prefix-list [**name** *prefix-list-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

name *prefix-list-name*: IP プレフィックスリストを指定します。設定範囲は 1～63 文字です。大文字、小文字を区別します。指定しない場合、すべての IPv4 プレフィックスリストの統計情報を表示します。

説明

display ip prefix-list コマンドは IPv4 プレフィックスリストの統計情報を表示します。

例

IPv4 プレフィックスリスト **abc** の統計情報を表示します。

<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
```

表 10-2 コマンド出力

フィールド	説明
Prefix-list	IPv4プレフィックスリストの名前です。
Permitted	条件にマッチするルートの数です。
Denied	条件にマッチしないルートの数です。
index	アイテムのインデックスです。
deny	アイテムのマッチモードです。 ● **permit**ー許可モードです。 ● **deny**ー拒否モードです。

フィールド	説明
6.6.6.0/24	IPアドレスとマスクです。
ge	下限マスク長以上（≧）を示します。
le	上限マスク長以下（≦）を示します。

関連コマンド

- **ip prefix-list**
- **reset ip prefix-list**

10.2.3 if-match ip

Syntax

if-match ip { **address** | **next-hop** | **route-source** } { **acl** *acl-number* | **prefix-list** *prefix-list-name* }

undo if-match ip { **address** | **next-hop** | **route-source** } [**acl** | **prefix-list**]

デフォルト

設定なし

View

Routing policy node view

定義済みユーザロール

network-admin

パラメータ

address: IPv4 ルートの宛先アドレスにマッチします。

next-hop: IPv4 ルートのネクストホップにマッチします。

route-source: IPv4 ルートの送信元アドレスにマッチします。

acl *acl-number*: ACL を指定します。**address**パラメータの設定範囲は 2000～3999 です。**next-hop** パラメータと **route-source** パラメータの設定範囲は 2000～2999 です。

prefix-list *prefix-list-name*: IP プレフィックスリストを指定します。設定範囲は 1～63 文字です。大文字、小文字を区別します。

説明

if-match ip コマンドは宛先、ネクストホップ、送信元が指定された ACL あるいはプレフィックスリストにマッチするルートを定義します。

undo if-match ip コマンドは設定を削除します。

例

ルーティングポリシー**policy1** のノード 10 で、ネクストホップが IP プレフィックスリスト **p1** にマッチする IPv4 ルートを定義します。

<Switch> system-view

[Switch] route-policy policy1 permit node 10

[Switch-route-policy-policy1-10] if-match ip next-hop prefix-list p1

10.2.4 ip prefix-list

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*]

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

prefix-list-name: IPv4 プレフィックスリストの名前を指定します。設定範囲は 1～63 文字です。大文字、小文字を区別します。

index-number: IPv4 プレフィックスリストのアイテムのインデックス番号を指定します。設定範囲は 1～65535 です。最初に小さい番号のアイテムがマッチされます。

deny: deny モードを指定します。ルートがアイテムにマッチする場合、ルートはネクストアイテムをマッチすることなく、拒否されます。ルートがアイテムにマッチしない場合、ルートはネクストアイテムに対してマッチを行います。(IPv4 プレフィックスリストに複数のアイテムがあると仮定します)

permit: permit モードを指定します。ルートがアイテムにマッチする場合、IPv4 プレフィックスリストをパスします。ルートがアイテムにマッチしない場合、ネクストアイテ

ムに対してマッチを行います。(IPv4 プレフィックスリストに複数のアイテムがあると仮定します)

ip-address mask-length: IPv4 プレフィックスとマスク長を指定します。*mask-length* の設定範囲は 0～32 です。

min-mask-length, *max-mask-length*: プレフィックス長の範囲を指定します。

greater-equal パラメータは以上（≧）を示し、**less-equal** パラメータは以下（≦）を示します。

範囲の関係は 32 ≧ *max-mask-length* ≧ *min-mask-length* ≧ *mask-length* です。

- *min-mask-length* パラメータのみが指定された場合、プレフィックス長の範囲は [*min-mask-length*, 32]です。
- *max-mask-length* パラメータのみが指定された場合、プレフィックス長の範囲は [*mask-length*, *max-mask-length*]です。
- *min-mask-length* パラメータと *max-mask-length* パラメータが指定された場合、プレフィックス長の範囲は[*min-mask-length*, *max-mask-length*]です。

説明

ip prefix-list コマンドはリストの IPv4 プレフィックスリストあるいはアイテムを設定します。

undo ip prefix-list コマンドは IPv4 プレフィックスリストあるいはアイテムを削除します。

IPv4 プレフィックスリストは IPv4 アドレスをフィルタするために使用されます。IP プレフィックスリストは複数のアイテムを指定することができます。各アイテムは IPv4 プレフィックスの範囲を指定できます。アイテム間の関係は論理和です。アイテムがパスした場合、IPv4 プレフィックスリストがパスします。アイテムがパスしない場合、IP プレフィックスリストはパスすることができません。

ip-address パラメータと *mask-length* パラメータの両方が 0.0.0.0 に指定された場合、デフォルトルートがマッチします。

すべてのルートをマッチする場合、0.0.0.0 0 **less-equal** 32 を使用します。

例

ネットワーク 10.0.0.0/8 とマスク長 17 あるいは 18 のルートを許可する IP プレフィックスリスト **p1** を設定します。

<Switch> system-view

[Switch] ip prefix-list p1 permit 10.0.0.0 8 greater-equal 17 less-equal 18

関連コマンド

- **display ip prefix-list**
- **reset ip prefix-list**

10.2.5 reset ip prefix-list

Syntax

reset ip prefix-list [*prefix-list-name*]

View

User view

定義済みユーザロール

network-admin

パラメータ

prefix-list-name: IP プレフィックスリストを指定します。設定範囲は 1～63 文字です。指定しない場合、すべての IPv4 プレフィックスリストの統計情報を削除します。

説明

reset ip prefix-list コマンドは IPv4 プレフィックスリストの統計情報を削除します。

例

IPv4 プレフィックスリスト **abc** の統計情報を削除します。

<Switch> reset ip prefix-list abc

関連コマンド

- **display ip prefix-list**
- **ip prefix-list**

10.3 IPv6ルーティングポリシー設定コマンド

10.3.1 apply ipv6 next-hop

Syntax

apply ipv6 next-hop *ipv6-address*

undo apply ipv6 next-hop

デフォルト

設定なし

View

Routing policy node view

定義済みユーザロール

network-admin

パラメータ

ipv6-address: ネクストホップの IPv6 アドレスを指定します。

説明

apply ipv6 next-hop コマンドは IPv6 ルートのネクストホップを設定します。

undo apply ipv6 next-hop コマンドはデフォルトに戻します。

コマンドは再配信されたルートのネクストホップを設定することができません。

例

ルーティングポリシー**policy1** のノード 10 で、コスト 8 にマッチする IPv6 ルートのネクストホップ 3ffe:506::1 を指定します。

<Switch> system-view

[Switch] route-policy policy1 permit node 10

[Switch-route-policy-policy1-10] if-match cost 8

[Switch-route-policy-policy1-10] apply ipv6 next-hop 3ffe:506::1

10.3.2 display ipv6 prefix-list

Syntax

display ipv6 prefix-list [**name** *prefix-list-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

name *prefix-list-name*: IPv6 プレフィックスリストを指定します。設定範囲は 1～63 文字です。大文字、小文字を区別します。指定しない場合、すべての IPv6 プレフィックスリストの統計情報を表示します。

説明

display ipv6 prefix-list コマンドは IPv6 プレフィックスリストの統計情報を表示します。

例

すべての IPv6 プレフィックスリストの統計情報を表示します。

<Switch> display ipv6 prefix-list

```
Prefix-list6: 666
 Permitted 0
 Denied 0
        index: 10       permit 6::/64               ge  66  le  88
```

表 10-3 コマンド出力

フィールド	説明
Prefix-list6	IPv6プレフィックスリストの名前です。
Permitted	条件にマッチするルートの数です。
Denied	条件にマッチしないルートの数です。
index	アイテムのインデックスです。
permit	アイテムのマッチモードです。 ● **permit**ー許可モードです。 ● **deny**ー拒否モードです。
6::/64	マッチするIPv6アドレスとプレフィックス長です。
ge	下限マスク長以上（≧）を示します。
le	上限マスク長以下（≦）を示します。

関連コマンド

- **ipv6 prefix-list**
- **reset ipv6 prefix-list**

10.3.3 if-match ipv6

Syntax

if-match ipv6 { **address** | **next-hop** | **route-source** } { **acl** *acl6-number* | **prefix-list** *prefix-list-name* }

undo if-match ipv6 { **address** | **next-hop** | **route-source** } [**acl** | **prefix-list**]

デフォルト

設定なし

View

Routing policy node view

定義済みユーザロール

network-admin

パラメータ

address: IPv6 ルートの宛先アドレスにマッチします。

next-hop: IPv6 ルートのネクストホップにマッチします。

route-source: IPv6 ルートの送信元アドレスにマッチします。

acl *acl6-number*: IPv6 ACL を指定します。**address** パラメータの設定範囲は 2000～3999 です。**next-hop** パラメータと **route-source** パラメータの設定範囲は 2000～2999 です。

prefix-list *prefix-list-name*: IPv6 プレフィックスリストを指定します。設定範囲は 1～63 文字です。大文字、小文字を区別します。

説明

if-match ipv6 コマンドは宛先、ネクストホップ、送信元が指定された ACL あるいは IPv6 プレフィックスリストにマッチする IPv6 ルートを定義します。

undo if-match ipv6 コマンドは設定を削除します。

例

ルーティングポリシー **policy1** のノード 10 で、ネクストホップが IPv6 プレフィックスリスト **p1** にマッチする IPv6 ルートを定義します。

<Switch> system-view

[Switch] route-policy policy1 permit node 10

[Switch-route-policy-policy1-10] if-match ipv6 next-hop prefix-list p1

10.3.4 ipv6 prefix-list

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*]

undo ipv6 prefix-list *prefix-list-name* [**index** *index-number*]

デフォルト

No IPv6 prefix list is configured.

View

System view

定義済みユーザロール

network-admin

パラメータ

prefix-list-name: IPv6 プレフィックスリストの名前を指定します。設定範囲は 1～63 文字です。大文字、小文字を区別します。

index-number: IPv6 プレフィックスリストのアイテムのインデックス番号を指定します。設定範囲は 1～65535 です。最初に小さい番号のアイテムがマッチされます。

deny: deny モードを指定します。ルートがアイテムにマッチする場合、ルートはネクストアイテムをマッチすることなく、拒否されます。ルートがアイテムにマッチしない場合、ルートはネクストアイテムに対してマッチを行います。(IPv6 プレフィックスリストに複数のアイテムがあると仮定します)

permit: permit モードを指定します。ルートがアイテムにマッチする場合、IPv4 プレフィックスリストをパスします。ルートがアイテムにマッチしない場合、ネクストアイテムに対してマッチを行います。(IPv6 プレフィックスリストに複数のアイテムがあると仮定します)

ipv6-address prefix-length: IPv6 プレフィックスとマスク長を指定します。*prefix-length* の設定範囲は 0～128 です。::0 が指定された場合、デフォルトルートをマッチします。

greater-equal *min-prefix-length*: 最小プレフィックス長以上を指定します。

less-equal *max-prefix-length*: 最大プレフィックス長以下を指定します。

範囲の関係は 128 ≧ *max-mask-length* ≧ *min-mask-length* ≧ *mask-length* です。

- *min-prefix-length* パラメータのみが指定された場合、プレフィックス長の範囲は [*min-prefix-length*, 128]です。
- *max-prefix-length* パラメータのみが指定された場合、プレフィックス長の範囲は [*prefix-length*, *max-prefix-length*]です。
- *min-prefix-length* パラメータと *max-prefix-length* パラメータが指定された場合、プレフィックス長の範囲は[*min-prefix-length*, *max-prefix-length*]です。

説明

ipv6 prefix-list コマンドは IPv6 プレフィックスリストあるいはアイテムを設定します。

undo ipv6 prefix-list コマンドは IPv6 プレフィックスリストあるいはアイテムを削除します。

IPv6 プレフィックスリストは複数のアイテムを指定することができます。各アイテムは IPv6 プレフィックスの範囲を指定できます。アイテム間の関係は論理和です。アイテムがパスした場合、IPv6 プレフィックスリストがパスします。

ipv6-address パラメータと *prefix-length* パラメータの両方が::0 に指定された場合、デフォルトルートがマッチします。

すべてのルートをマッチする場合、:: 0 **less-equal** 128 を使用します。

例

マスク長が 32 ビット～64 ビットの IPv6 アドレスを許可します。

<Switch> system-view

[Switch] ipv6 prefix-list abc permit :: 0 greater-equal 32 less-equal 64

プレフィックス 3FFE:D00::/32、プレフィックス長が 32 ビット以下の IPv6 アドレスを拒否します。

<Switch> system-view

[Switch] ipv6 prefix-list abc deny 3FFE:D00:: 32 less-equal 128

関連コマンド

- **display ipv6 prefix-list**
- **reset ipv6 prefix-list**

10.3.5 reset ipv6 prefix-list

Syntax

reset ipv6 prefix-list [*prefix-list-name*]

View

User view

定義済みユーザロール

network-admin

パラメータ

prefix-list-name: IPv6 プレフィックスリストの名前を指定します。設定範囲は 1～63 文字です。大文字、小文字を区別します。指定しない場合、すべての IPv6 プレフィックスリストの統計情報を削除します。

説明

reset ipv6 prefix-list コマンドは IPv6 プレフィックスリストの統計情報を削除します。

例

IPv6 プレフィックスリスト **abc** の統計情報を削除します。

<Switch> reset ipv6 prefix-list abc

関連コマンド

- **display ipv6 prefix-list**

- **ipv6 prefix-list**

QX-S5100G シリーズ Ethernet スイッチ

コマンドマニュアル

6. マルチキャスト

本マニュアルは以下に示す章で構成されています。

01-IGMP スヌーピング

02-マルチキャスト VLAN

03-MLD スヌーピング

04-IPv6 マルチキャスト VLAN

目次

このセクションのページは **6-x-x** です。

1 章 IGMP スヌーピング 1-1
1.1 IGMP スヌーピング設定コマンド 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 1-17
1.1.12 dot1p-priority (IGMP-snooping view) 1-18
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) 1-22
1.1.17 host-aging-time (IGMP-snooping view) 1-24
1.1.18 igmp-snooping 1-25
1.1.19 igmp-snooping dot1p-priority 1-26
1.1.20 igmp-snooping drop-unknown 1-27
1.1.21 igmp-snooping enable 1-28
1.1.22 igmp-snooping fast-leave 1-29
1.1.23 igmp-snooping general-query source-ip 1-30
1.1.24 igmp-snooping group-limit 1-31
1.1.25 igmp-snooping group-policy 1-32
1.1.26 igmp-snooping host-aging-time 1-34
1.1.27 igmp-snooping host-join 1-35
1.1.28 igmp-snooping last-member-query-interval 1-36
1.1.29 igmp-snooping leave source-ip 1-37
1.1.30 igmp-snooping max-response-time 1-38
1.1.31 igmp-snooping overflow-replace 1-40
1.1.32 igmp-snooping proxy enable 1-41
1.1.33 igmp-snooping querier 1-42
1.1.34 igmp-snooping query-interval 1-43

1.1.35 igmp-snooping report source-ip 1-44
1.1.36 igmp-snooping router-aging-time 1-45
1.1.37 igmp-snooping source-deny 1-46
1.1.38 igmp-snooping special-query source-ip 1-47
1.1.39 igmp-snooping static-group 1-48
1.1.40 igmp-snooping static-router-port 1-49
1.1.41 igmp-snooping version 1-50
1.1.42 last-member-query-interval (IGMP-snooping view) 1-51
1.1.43 mac-address multicast 1-52
1.1.44 max-response-time (IGMP-snooping view) 1-54
1.1.45 overflow-replace (IGMP-snooping view) 1-55
1.1.46 report-aggregation (IGMP-snooping view) 1-56
1.1.47 reset igmp-snooping group 1-57
1.1.48 reset igmp-snooping router-port 1-57
1.1.49 reset igmp-snooping statistics 1-58
1.1.50 router-aging-time (IGMP-snooping view) 1-59
1.1.51 source-deny (IGMP-snooping view) 1-60

1章 IGMP スヌーピング

1.1 IGMPスヌーピング設定コマンド

1.1.1 display igmp-snooping

Syntax

display igmp-snooping [**global** | **vlan** *vlan-id*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

global: グローバルの IGMP snooping の状態を表示します。

vlan *vlan-id*: VLAN の ID を指定します。設定範囲は 1～4094 です。

説明

display igmp-snooping コマンドは IGMP snooping の状態を表示します。

パラメータを指定しない場合、グローバルとすべての VLAN の IGMP snooping の状態を表示します。

例

🕮 **メモ：**

Global-enable の表示は未サポートです。Global-enable の表示が Disabled であっても、IGMP snooping はグローバルで有効の状態です。なお、グローバルで無効の場合は、IGMP snooping is not configured.と表示されます。

グローバルとすべての VLAN の IGMP snooping の状態を表示します。

<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: Disabled
 Querier-election: Disabled
 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: Disabled
 Querier-election: Disabled
 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
```

表 1-1 コマンド出力

フィールド	説明
IGMP snooping	IGMP snoopingの状態です。 ● **Enabled**－有効です。 ● **Disabled**－無効です。
Drop-unknown	未知のマルチキャストデータの廃棄機能の状態です。 ● **Enabled**－有効です。 ● **Disabled**－無効です。
Version	IGMP snoopingのバージョンです。
Host-aging-time	ダイナミックメンバポートのエージングタイマです。
Router-aging-time	ダイナミックルータポートのエージングタイマです。
Max-response-time	IGMP general クエリの最大応答時間です。
Last-member-query-interval	IGMP group-specific クエリの送信間隔です。
Report-aggregation	IGMP report抑制機能の状態です。 ● **Enabled**－有効です。 ● **Disabled**－無効です。
Dot1p-priority	IGMPメッセージの802.1pプライオリティです。プライオリティが設定されていない場合、ハイフン（--）が表示されます。
Querier	IGMP snoopingクエリアの状態です。 ● **Enabled**－有効です。 ● **Disabled**－無効です。
Query-interval	IGMP general クエリの間隔です。
General-query source IP	IGMP general クエリの送信元IPアドレスです。
Special-query source IP	IGMP group-specific クエリの送信元IPアドレスです。
Report source IP	IGMP reportsの送信元IPアドレスです。
Leave source IP	IGMP leaveメッセージの送信元IPアドレスです。
Host-tracking	host trackingの状態です。 ● **Enabled**－有効です。 ● **Disabled**－無効です。
Proxy Status of IGMP	IGMP snooping proxyingの状態です。 ● **Enabled**－有効です。 ● **Disabled**－無効です。

1.1.2 display igmp-snooping group

Syntax

display igmp-snooping group [*group-address* | *source-address*] * [**vlan** *vlan-id*] [**verbose**] [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

group-address: マルチキャストグループの IP アドレスを指定します。設定範囲は 224.0.1.0～239.255.255.255 です。マルチキャストグループを指定しない場合、すべてのマルチキャストグループのダイナミック IGMP snooping 転送エントリを表示します。

source-address: マルチキャストソースの IP アドレスを指定します。マルチキャストソースを指定しない場合、すべてのマルチキャストソースのダイナミック IGMP snooping 転送エントリを表示します。

vlan *vlan-id*: VLAN の ID を指定します。設定範囲は 1～4094 です。指定しない場合、すべての VLAN のダイナミック IGMP snooping 転送エントリを表示します。

verbose: ダイナミック IGMP snooping 転送エントリの詳細情報を表示します。指定しない場合、概要情報を表示します。

slot *slot-number*: IRF スタックメンバ装置を指定します。*slot-number* は IRF スタックメンバ装置の ID を示します。指定しない場合、IRF スタックユニットのマスタ装置のダイナミック IGMP snooping 転送エントリを表示します。

説明

display igmp-snooping group コマンドはダイナミック IGMP snooping 転送エントリを表示します。

例

VLAN 2 のダイナミック IGMP snooping 転送エントリの詳細情報を表示します。

<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)
```

表 1-2 コマンド出力

フィールド	説明
Total 1 entries	ダイナミックIGMP snooping転送エントリの総数です。
VLAN 2: Total 1 entries	VLAN 2のダイナミックIGMP snooping転送エントリの総数です。
(0.0.0.0, 224.1.1.1)	（S,G）エントリです。Sが**0.0.0.0**の場合、すべてのマルチキャストソースを示します。
Attribute	エントリ属性です。 • **global port**—エントリにグローバルポートがあります。 • **local port**—エントリに指定された装置上のポートがあります。 • **slot**—エントリに指定された装置以外の装置上のポートがあります。
FSM information	エントリの有限状態装置（Finite state machine）情報です。 • **delete**—エントリの属性が削除されています。 • **dummy**—エントリが新規で一時的なエントリです。 • **no info**—エントリが存在しません。
Host slots (0 in total)	メンバIDとメンバ装置が指定されていないとき、指定されたメンバ装置、あるいはマスタ装置を除いたメンバ装置の総数です。
Host ports (1 in total)	メンバポートとメンバポートの総数です。
(00:03:23)	ダイナミックメンバポートの残りのエージング時間です。アグリゲートインタフェースのようなグローバルポートでは常に表示されます。 グローバルポートでない場合、以下のときに表示されます。 • 指定されたメンバ装置のポートです。 • ポートがマスタ装置にあり、メンバ装置が指定されていません。

関連コマンド

reset igmp-snooping group

1.1.3 display igmp-snooping router-port

Syntax

display igmp-snooping router-port [**vlan** *vlan-id*] [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

vlan *vlan-id*: VLAN の ID を指定します。設定範囲は 1～4094 です。指定しない場合、すべての VLAN のダイナミックルータポートの情報を表示します。

slot *slot-number*: IRF スタックメンバ装置を指定します。*slot-number* は IRF スタックメンバ装置の ID を示します。指定しない場合、IRF スタックユニットのマスタ装置のダイナミックルータポートの情報を表示します。

説明

display igmp-snooping router-port コマンドはダイナミックルータポートの情報を表示します。

例

VLAN 2 のダイナミックルータポートの情報を表示します。

<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)
```

表 1-3 コマンド出力

フィールド	説明
VLAN 2	VLAN IDです。
Router slots (0 in total)	メンバIDとメンバ装置が指定されていないとき、指定されたメンバ装置、あるいはマスタ装置を除いたメンバ装置の総数です。
Router ports (2 in total)	ダイナミックルータポートと、ダイナミックルータポートの総数です。

フィールド	説明
(00:01:30)	ダイナミックルータポートの残りのエージング時間です。 グローバルポートでは常に表示されます。 グローバルポートでない場合、以下のときに表示されます。 ● 指定されたメンバ装置のポートです。 ● ポートがマスタ装置にあり、メンバ装置が指定されていません。

関連コマンド

reset igmp-snooping router-port

1.1.4 display igmp-snooping static-group

Syntax

display igmp-snooping static-group [*group-address* | *source-address*] * [**vlan** *vlan-id*] [**verbose**] [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

group-address: マルチキャストグループの IP アドレスを指定します。設定範囲は 224.0.1.0～239.255.255.255 です。マルチキャストグループを指定しない場合、すべてのマルチキャストグループのスタティック IGMP snooping 転送エントリを表示します。

source-address: マルチキャストソースの IP アドレスを指定します。マルチキャストソースを指定しない場合、すべてのマルチキャストソースのスタティック IGMP snooping 転送エントリを表示します。

vlan *vlan-id*: VLAN の ID を指定します。設定範囲は 1～4094 です。指定しない場合、すべての VLAN のスタティック IGMP snooping 転送エントリを表示します。

verbose: 詳細な情報を表示します。指定しない場合、概要情報を表示します。

slot *slot-number*: IRF スタックメンバ装置を指定します。*slot-number* は IRF スタックメンバ装置の ID を示します。指定しない場合、IRF スタックユニットのマスタ装置のスタティック IGMP snooping 転送エントリを表示します。

説明

display igmp-snooping static-group コマンドはスタティック IGMP snooping 転送エントリを表示します。

例

VLAN 2 のスタティック IGMP snooping 転送エントリの詳細情報を表示します。

<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
```

表 1-4 コマンド出力

フィールド	説明
Total 1 entries	スタティックIGMP snooping転送エントリの総数です。
VLAN 2: Total 1 entries	VLAN 2のスタティックIGMP snooping転送エントリの総数です。
(0.0.0.0, 224.1.1.1)	（S,G）エントリです。Sが**0.0.0.0**の場合、すべてのマルチキャストソースを示します。
Attribute	エントリ属性です。 • **global port**—エントリにグローバルポートがあります。 • **local port**—エントリに指定された装置上のポートがあります。 • **slot**—エントリに指定された装置以外の装置上のポートがあります。
FSM information	エントリの有限状態装置（Finite state machine）情報です。 • **delete**—エントリの属性が削除されています。 • **dummy**—エントリが新規で一時的なエントリです。 • **no info**—エントリが存在しません。
Host slots (0 in total)	メンバIDとメンバ装置が指定されていないとき、指定されたメンバ装置、あるいはマスタ装置を除いたメンバ装置の総数です。
Host ports (1 in total)	メンバポートとメンバポートの総数です。

1.1.5 display igmp-snooping static-router-port

Syntax

display igmp-snooping static-router-port [**vlan** *vlan-id*] [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

vlan *vlan-id*: VLAN の ID を指定します。設定範囲は 1～4094 です。

slot *slot-number*: IRF スタックメンバ装置を指定します。*slot-number* は IRF スタックメンバ装置の ID を示します。指定しない場合、IRF スタックユニットのマスタ装置のスタティックルータポートの情報を表示します。

説明

display igmp-snooping static-router-port コマンドはスタティックルータポートの情報を表示します。

例

VLAN 2 のスタティックルータポートの情報を表示します。

<Switch> display igmp-snooping static-router-port vlan 2

```
VLAN 2:
  Router ports (2 in total):
    GE1/0/1
    GE1/0/2
```

表 1-5 コマンド出力

フィールド	説明
VLAN 2	VLAN IDです。
Router slots (0 in total)	メンバIDとメンバ装置が指定されていないとき、指定されたメンバ装置、あるいはマスタ装置を除いたメンバ装置の総数です。
Router ports (2 in total)	スタティックルータポートとスタティックルータポートの総数です。

1.1.6 display igmp-snooping statistics

Syntax

display igmp-snooping statistics

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display igmp-snooping statistics コマンドは IGMP snooping によって学習した IGMP メッセージと PIMv2 hello メッセージの統計情報を表示します。

例

IGMP snooping によって学習した IGMP メッセージと PIMv2 hello メッセージの統計情報を表示します。

<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
```

表 1-6 コマンド出力

フィールド	説明
general queries	IGMP general クエリの数です。
specific queries	IGMP group-specific クエリの数です。

フィールド	説明
reports	IGMP reportの数です。
leaves	IGMP leaveメッセージの数です。
reports with right and wrong records	正常な記録、正常でない記録のIGMP reportの数です。
specific sg queries	IGMP group-and-source-specific クエリの数です。
PIMv2 hello	PIMv2 helloメッセージの数です。
error IGMP messages	エラーがあるIGMPメッセージの数です。

関連コマンド

reset igmp-snooping statistics

1.1.7 display l2-multicast ip

Syntax

display l2-multicast ip [**group** *group-address* | **source** *source-address*] * [**vlan** *vlan-id*] [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

group *group-address*: マルチキャストグループを IP アドレスで指定します。マルチキャストグループを指定しない場合、このコマンドはすべてのレイヤ 2 IP マルチキャストグループの情報を表示します。

source *source-address*: マルチキャスト送信元を IP アドレスで指定します。マルチキャスト送信元アドレスを指定しない場合、このコマンドは、すべてのマルチキャスト送信元のレイヤ 2 IP マルチキャストグループの情報を表示します。

vlan *vlan-id*: VLAN ID で VLAN を 1～4094 の範囲で指定します。VLAN を指定しない場合、このコマンドは、すべての VLAN のレイヤ 2 IP マルチキャストグループの情報を表示します。

slot *slot-number*: メンバ ID によって IRF スタックメンバ装置を指定します。メンバ装置を指定しない場合、このコマンドはマスタ装置のレイヤ 2 IP マルチキャストグループの情報を表示します。

説明

display l2-multicast ip コマンドは、レイヤ 2 IP マルチキャストグループの情報を表示します。

例

VLAN2 のレイヤ 2 IP マルチキャストグループの情報を表示します。

<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)
```

表 1-7 コマンド出力

フィールド	説明
Total 1 entries	レイヤ2 IPマルチキャストグループエントリの総数です。
VLAN 2: Total 1 entries	VLAN 2のレイヤ2 IPマルチキャストグループエントリの総数です。
(0.0.0.0, 224.1.1.1)	（S,G）エントリです。Sが**0.0.0.0**の場合、すべてのマルチキャストソースを示します。
Attribute	エントリ属性です。 • **dynamic**—エントリはダイナミックプロトコルによって作成されます。 • **static**—エントリはスタティックプロトコルによって作成されます。 • **pim**—エントリはPIMによって作成されます。 • **kernel**—エントリはカーネルから取得されます。 • **success**—処理に成功しました。 • **fail**—処理に失敗しました。
Host ports (1 in total)	メンバポートおよびメンバポートの総数です。

フィールド	説明
(S, SUC)	ポート属性です。 • **D**—ダイナミックポートです。 • **S**—スタティックポートです。 • **P**—PIMポートです。 • **K**—カーネルから取得されたポートです。 • **R**—(*, *)エントリから学習したポートです。 • **W**— (*, G)エントリから学習したポートです。 • **SUC**—処理に成功しました。 • **F**—処理に失敗しました。

1.1.8 display l2-multicast ip forwarding

Syntax

display l2-multicast ip forwarding [**group** *group-address* | **source** *source-address*] * [**vlan** *vlan-id*] [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

group *group-address*: マルチキャストグループの IP アドレスを指定します。マルチキャストグループを指定しない場合、すべてのマルチキャストグループのレイヤ 2 マルチキャスト転送エントリを表示します。

source *source-address*: マルチキャストソースの IP アドレスを指定します。マルチキャストソースを指定しない場合、すべてのマルチキャストソースのレイヤ 2 IP マルチキャスト転送エントリを表示します。

vlan *vlan-id*: VLAN の ID を指定します。設定範囲は 1～4094 です。指定しない場合、すべての VLAN のレイヤ 2 IP マルチキャスト転送エントリを表示します。

slot *slot-number*: IRF スタックメンバ装置を指定します。*slot-number* は IRF スタックメンバ装置の ID を示します。指定しない場合、IRF スタックユニットのマスタ装置のレイヤ 2 IP マルチキャスト転送エントリを表示します。

説明

display l2-multicast ip forwarding コマンドはレイヤ 2 IP マルチキャスト転送エントリを表示します。

例

VLAN 2 のレイヤ 2 IP マルチキャスト転送エントリを表示します。

<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
```

表 1-8 コマンド出力

フィールド	説明
Total 1 entries	レイヤ2 IPマルチキャスト転送エントリの総数です。
VLAN 2: Total 1 IP entries	VLAN 2のレイヤ2 IPマルチキャスト転送エントリの総数です。
(0.0.0.0, 224.1.1.1)	（S,G）エントリです。Sが**0.0.0.0**の場合、すべてのマルチキャストソースを示します。
Host ports (3 in total)	メンバポートとメンバポートの総数です。

1.1.9 display l2-multicast mac

Syntax

display l2-multicast mac [*mac-address*] [**vlan** *vlan-id*] [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

mac-address: マルチキャスト MAC アドレスで MAC マルチキャストグループを指定します。MAC マルチキャストグループを指定しない場合、このコマンドはすべてのレイヤ 2 MAC マルチキャストグループの情報を表示します。

vlan *vlan-id*: VLAN ID で VLAN を 1～4094 の範囲で指定します。VLAN を指定しない場合、このコマンドは、すべての VLAN のレイヤ 2 MAC マルチキャストグループの情報を表示します。

slot *slot-number*: メンバ ID によって IRF スタックメンバ装置を指定します。メンバ装置を指定しない場合、このコマンドはマスタ装置のレイヤ 2 MAC マルチキャストグループの情報を表示します。

説明

display l2-multicast mac コマンドは、レイヤ 2 MAC マルチキャストグループの情報を表示します。

例

VLAN2 のレイヤ 2 MAC マルチキャストグループの情報を表示します。

<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
```

表 1-9 コマンド出力

フィールド	説明
Total 1 entries	レイヤ2 MACマルチキャストグループエントリの総数です。
VLAN 2: Total 1 entries	VLAN 2のレイヤ2 MACマルチキャストグループエントリの総数です。
MAC group address	MACマルチキャストグループのアドレスです。
Attribute	エントリ属性です。 ● **success**—処理に成功しました。 ● **fail**—処理に失敗しました。
Host ports (1 in total)	メンバポートとメンバポートの総数です。

1.1.10 display l2-multicast mac forwarding

Syntax

display l2-multicast mac forwarding [*mac-address*] [**vlan** *vlan-id*] [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

mac-address: MAC アドレスで MAC マルチキャストグループを指定します。指定しない場合、すべての MAC マルチキャストグループのレイヤ 2 MAC マルチキャスト転送エントリを表示します。

vlan *vlan-id*: VLAN の ID を指定します。設定範囲は 1～4094 です。指定しない場合、すべての VLAN のレイヤ 2 MAC マルチキャスト転送エントリを表示します。

slot *slot-number*: IRF スタックメンバ装置を指定します。*slot-number* は IRF スタックメンバ装置の ID を示します。指定しない場合、IRF スタックユニットのマスタ装置のレイヤ 2 MAC マルチキャスト転送エントリを表示します。

説明

display l2-multicast mac forwarding コマンドはレイヤ 2 MAC マルチキャスト転送エントリを表示します。

例

VLAN 2 のレイヤ 2 MAC マルチキャスト転送エントリを表示します。

<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
```

表 1-10 コマンド出力

フィールド	説明
Total 1 entries	レイヤ2 MACマルチキャスト転送エントリの総数です。
VLAN 2: Total 1 entries	VLAN 2のレイヤ2 MACマルチキャスト転送エントリの総数です。
MAC group address	MACマルチキャストグループのアドレスです。
Host ports (3 in total)	メンバポートとメンバポートの総数です。

1.1.11 display mac-address multicast

Syntax

display mac-address [*mac-address* [**vlan** *vlan-id*] | [**multicast**] [**vlan** *vlan-id*] [**count**]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

mac-address: マルチキャスト MAC アドレスを指定します。MAC アドレスは正常なマルチキャスト MAC アドレスです。MAC アドレスは 0100-5Exx-xxxx and 3333-xxxx-xxxx（x は 0～F の 16 進数の値）を除いて設定できます。

vlan *vlan-id*: VLAN の ID を指定します。設定範囲は 1～4094 です。指定しない場合、すべての VLAN のスタティックマルチキャスト MAC アドレスエントリを表示します。

multicast: スタティックマルチキャスト MAC アドレスエントリを指定します。

count: スタティックマルチキャスト MAC アドレスエントリの数を表示します。指定した場合、スタティックマルチキャスト MAC アドレスエントリに一致する数を表示します。指定しない場合、エントリの数ではなく一致するエントリの内容を表示します。

説明

display mac-address multicast コマンドはスタティックマルチキャスト MAC アドレスエントリを表示します。

パラメータを指定しない場合、ユニキャスト MAC アドレスエントリ、スタティックマルチキャスト MAC アドレスエントリを含むすべての MAC アドレステーブルエントリを表示します。

例

VLAN 2 のスタティックマルチキャスト MAC アドレスエントリを表示します。

<Switch> display mac-address multicast vlan 2

```
MAC Address      VLAN ID    State          Port/NickName          Aging
0100-0001-0001   2          Multicast      GE1/0/1                N
                                           GE1/0/2
```

スタティックマルチキャスト MAC アドレスエントリの数を表示します。

<Switch> display mac-address multicast count

```
1 mac address(es) found.
```

表 1-11 コマンド出力

フィールド	説明
MAC address	マルチキャストグループのMACアドレスです。
VLAN ID	MACアドレスによって識別されたネットワーク装置が所属するVLAN IDです。
State	MACアドレスの状態です。マルチキャストMACアドレスエントリがスタティックである場合、**Multicast**と表示されます。
Port/NickName	MACアドレスエントリのMACアドレスに送信されるパケットの出力ポートあるいはニックネームです。 ニックネームは現在のソフトウェアバージョンでサポートしていません。
Aging	エージング時間の状態です。エントリがエージアウトしない場合、**N**と表示されます。
1 mac address(es) found	1つのスタティックマルチキャストMACアドレスエントリが見つかりました。

関連コマンド

mac-address multicast

1.1.12 dot1p-priority (IGMP-snooping view)

Syntax

dot1p-priority *priority*

undo dot1p-priority

デフォルト

IGMP メッセージの 802.1p 優先度はデフォルトで設定されていません。

装置によって作成される IGMP メッセージの優先度は 0 です。IGMP メッセージを転送する場合、優先度は変更しません。

View

IGMP-snooping view

定義済みユーザロール

network-admin

パラメータ

priority: IGMP メッセージの 802.1p 優先度を指定します。設定範囲は 0～7 です。値が高いほど優先度が高くなります。

説明

dot1p-priority コマンドはグローバルで IGMP メッセージの 802.1p 優先度を設定します。

undo dot1p-priority コマンドはデフォルトに戻します。

このコマンドは **igmp-snooping dot1p-priority** コマンドと同一機能ですが、適用範囲が異なります。

- IGMP-snooping view の **dot1p-priority** コマンドはすべての VLAN に適用されます。
- **igmp-snooping dot1p-priority** コマンドは現在の VLAN に適用されます。

VLAN では **igmp-snooping dot1p-priority** コマンドは IGMP-snooping view の **dot1p-priority** コマンドより優先されます。

例

IGMP メッセージの 802.1p 優先度を 3 に設定します。

<Switch> system-view

[Switch] igmp-snooping

[Switch-igmp-snooping] dot1p-priority 3

関連コマンド

igmp-snooping dot1p-priority

1.1.13 dscp

Syntax

dscp *dscp-value*

undo dscp

デフォルト

48

View

IGMP-snooping view

定義済みユーザロール

network-admin

パラメータ

dscp-value: 0～63 の範囲で DSCP 値を指定します。

説明

dscp コマンドは、出力 IGMP プロトコルパケットの DSCP 値を設定します。

undo dscp コマンドは、デフォルトに戻します。

DSCP 値は、パケットの送信優先順位を決定するために、IP パケットの ToS フィールドで伝送されます。DSCP 値が大きいほど、優先順位が高くなります。

例

出力 IGMP プロトコルパケットの DSCP 値を 63 に設定します。

<Switch> system-view

[Switch] igmp-snooping

[Switch-igmp-snooping] dscp 63

1.1.14 entry-limit (IGMP-snooping view)

Syntax

entry-limit *limit*

undo entry-limit

デフォルト

4294967295

View

IGMP-snooping view

定義済みユーザロール

network-admin

パラメータ

limit: IGMP snooping 転送エントリの最大数を指定します。設定範囲は 0～4294967295 です。

説明

entry-limit コマンドはグローバルでの IGMP snooping 転送エントリの最大数を設定します。IGMP snooping 転送エントリの最大数はダイナミックエントリとスタティックエントリを含みます。

undo entry-limit コマンドはデフォルトに戻します。

例

IGMP snooping 転送エントリのグローバルの最大数を 512 に設定します。

<Switch> system-view

[Switch] igmp-snooping

[Switch-igmp-snooping] entry-limit 512

1.1.15 fast-leave (IGMP-snooping view)

Syntax

fast-leave [**vlan** *vlan-list*]

undo fast-leave [**vlan** *vlan-list*]

デフォルト

無効

View

IGMP-snooping view

定義済みユーザロール

network-admin

パラメータ

vlan *vlan-list*: VLAN を指定します。半角スペースで区切り、1 行のコマンドで 10 個まで設定することができます。VLAN を範囲で指定する形式は *start-vlan-id* **to** *end-vlan-id* です。設定範囲は 1～4094 です。指定しない場合、すべての VLAN に適用します。

説明

fast-leave コマンドはグローバルに fast-leave 処理機能を有効にします。

undo fast-leave コマンドはグローバルに fast-leave 処理機能を無効にします。

ポートが leave メッセージを受信したとき、装置はマルチキャストグループの転送エントリから迅速にポートを削除します。

このコマンドは **igmp-snooping fast-leave** コマンドと同一機能ですが、適用範囲が異なります。

- IGMP-snooping view の **fast-leave** コマンドはすべてのポートに適用されます。
- **igmp-snooping fast-leave** コマンドは現在のポートに適用されます。

ポートでは **igmp-snooping fast-leave** コマンドは IGMP-snooping view の **fast-leave** コマンドより優先されます。

例

VLAN 2 でグローバルに fast-leave 処理機能を有効にします。

<Switch> system-view

[Switch] igmp-snooping

[Switch-igmp-snooping] fast-leave vlan 2

関連コマンド

igmp-snooping fast-leave

1.1.16 group-policy (IGMP-snooping view)

Syntax

group-policy *ipv4-acl-number* [**vlan** *vlan-list*]

undo group-policy [**vlan** *vlan-list*]

デフォルト

マルチキャストグループポリシーは設定されていません。受信ホストはすべてのマルチキャストグループに加入することができます。

View

IGMP-snooping view

定義済みユーザロール

network-admin

パラメータ

ipv4-acl-number: 標準 IPv4 ACL あるいは拡張 IPv4 ACL を指定します。設定範囲は 2000～3999 です。受信ホストは ACL が許可するマルチキャストグループのみ加入することができます。ACL が存在しない、あるいは ACL に正常なルールがないとき、受信ホストはマルチキャストグループに加入することができません。

vlan *vlan-list*: VLAN を指定します。半角スペースで区切り、10 まで設定することができます。VLAN を範囲で指定する形式は *start-vlan-id* **to** *end-vlan-id* です。設定範囲は 1～4094 です。指定しない場合、すべての VLAN に適用します。

説明

group-policy コマンドは受信ホストが加入するマルチキャストグループを管理するため、グローバルでマルチキャストグループポリシーを設定します。

undo group-policy コマンドはグローバルのマルチキャストグループポリシーを削除します。

マルチキャストグループポリシーはホストが加入するマルチキャストグループを管理する IGMP report をフィルタします。

スタティックメンバポートは IGMP report を送信しないため、**group-policy** コマンドはスタティックメンバポートに適用されません。

IGMP-snooping view のすべてのポートでグローバルにマルチキャストグループポリシーを設定することができます。また interface view のポートでマルチキャストグループポリシーを設定することができます。ポートでは **igmp-snooping group-policy** コマンドは IGMP-snooping view の **group-policy** コマンドより優先されます。

IPv4 ACL でルールを設定するとき、以下の制限とガイドラインに従ってください。

- 標準 IPv4 ACL の **source** *source-address source-wildcard* パラメータはマルチキャストグループアドレスを指定します。
- 拡張 IPv4 ACL の **source** *source-address source-wildcard* パラメータは IGMP report のマルチキャスト送信元アドレスを指定します。**destination** *dest-address dest-wildcard* パラメータはマルチキャストグループアドレスを指定します。

  以下の IGMP report に一致するように、マルチキャスト送信元アドレス **source** *source-address source-wildcard* を 0.0.0.0 に設定します。

  - IGMPv1、IGMPv2 の report
  - マルチキャスト送信元アドレスを送信しない IGMPv3 IS_EX、IGMPv3 TO_EX の report
- ACL ルールの **time-range** *time-range-name* パラメータ、**fragment** パラメータを除く他のオプションパラメータは無視します。

異なる VLAN のポートに異なる ACL のルールを設定することができます。同一 VLAN で複数の ACL を設定した場合、最後に行った ACL のルールが適用されます。

例

VLAN 2 のホストがマルチキャストグループ 225.1.1.1 のみ加入できるように VLAN 2 のマルチキャストグループポリシーをグローバルに設定します。

<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

関連コマンド

igmp-snooping group-policy

1.1.17 host-aging-time (IGMP-snooping view)

Syntax

host-aging-time *seconds*

undo host-aging-time

デフォルト

260 秒

View

IGMP-snooping view

定義済みユーザロール

network-admin

パラメータ

seconds: ダイナミックメンバポートのエージングタイマを設定します。設定範囲は 1～8097894 秒です。

説明

host-aging-time コマンドはグローバルでダイナミックメンバポートのエージングタイマを設定します。

undo host-aging-time コマンドはデフォルトに戻します。

このコマンドは **igmp-snooping host-aging-time** コマンドと同一機能ですが、適用範囲が異なります。

- IGMP-snooping view の **host-aging-time** コマンドはすべての VLAN に適用されます。
- **igmp-snooping host-aging-time** コマンドは現在の VLAN に適用されます。

VLAN では **igmp-snooping host-aging-time** コマンドは IGMP-snooping view の **host-aging-time** コマンドより優先されます。

マルチキャストグループメンバを間違って削除しないようにするため、ダイナミックメンバポートのエージングタイマを、以下の式で計算された値よりも大きい値に設定してください。

[IGMP general クエリの間隔] ＋ [IGMP general クエリの最大応答時間]

ダイナミックメンバポートのエージングタイマを以下の式で計算した値に設定することを推奨します。

[IGMP general クエリの間隔] × 2 ＋ [IGMP general クエリの最大応答時間]

例

グローバルでダイナミックメンバポートのエージングタイマを 300 秒に設定します。

<Switch> system-view

[Switch] igmp-snooping

[Switch-igmp-snooping] host-aging-time 300

関連コマンド

igmp-snooping host-aging-time

1.1.18 igmp-snooping

Syntax

igmp-snooping

undo igmp-snooping

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

igmp-snooping コマンドはグローバルで IGMP snooping を有効にし、IGMP-snooping view に移行します。

undo igmp-snooping コマンドはグローバルで IGMP snooping を無効にします。

グローバルで IGMP snooping を有効にした後、使用する VLAN で IGMP snooping を有効にしてください。IGMP snooping の設定については、セクション 6 *マルチキャスト オペレーションマニュアル*の“*IGMP スヌーピング*”を参照してください。

例

グローバルで IGMP snooping を有効にし、IGMP-snooping view に移行します。

<Switch> system-view

[Switch] igmp-snooping

[Switch-igmp-snooping]

関連コマンド

igmp-snooping enable

1.1.19 igmp-snooping dot1p-priority

Syntax

igmp-snooping dot1p-priority *priority*

undo igmp-snooping dot1p-priority

デフォルト

IGMP メッセージの 802.1p 優先度はデフォルトで設定されていません。

装置によって作成される IGMP メッセージの優先度は 0 です。IGMP メッセージを転送する場合、優先度は変更しません。

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

priority: IGMP メッセージの 802.1p 優先度を指定します。設定範囲は 0～7 です。値が高いほど優先度が高くなります。

説明

igmp-snooping dot1p-priority コマンドは VLAN の IGMP メッセージの 802.1p 優先度を設定します。

undo igmp-snooping dot1p-priority コマンドはデフォルトに戻します。

このコマンドを実行する前に VLAN で IGMP snooping を有効にしてください。

このコマンドは **dot1p-priority** コマンドと同一機能ですが、適用範囲が異なります。

- IGMP-snooping view の **dot1p-priority** コマンドはすべての VLAN に適用されます。
- **igmp-snooping dot1p-priority** コマンドは現在の VLAN に適用されます。

VLAN では **igmp-snooping dot1p-priority** コマンドは IGMP-snooping view の **dot1p-priority** コマンドより優先されます。

例

VLAN 2 で IGMP snooping を有効にし、IGMP メッセージの 802.1p 優先度を 3 に設定します。

<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

関連コマンド

- **dot1p-priority (IGMP-snooping view)**
- **igmp-snooping enable**

1.1.20 igmp-snooping drop-unknown

Syntax

igmp-snooping drop-unknown

undo igmp-snooping drop-unknown

デフォルト

VLAN の未知のマルチキャストデータの廃棄機能は無効です。未知のマルチキャストデータは VLAN にフラッディングされます。

View

VLAN view

定義済みユーザロール

network-admin

説明

igmp-snooping drop-unknown コマンドは VLAN の未知のマルチキャストデータの廃棄機能を有効にします。

undo igmp-snooping drop-unknown コマンドは VLAN の未知のマルチキャストデータの廃棄機能を無効にします。

このコマンドを実行する前に VLAN で IGMP snooping 機能を有効にしてください。

例

IGMP snooping を有効にし、VLAN 2 の未知のマルチキャストデータの廃棄機能を有効にします。

<Switch> system-view

[Switch] igmp-snooping

[Switch-igmp-snooping] quit

[Switch] vlan 2

[Switch-vlan2] igmp-snooping enable

[Switch-vlan2] igmp-snooping drop-unknown

関連コマンド

igmp-snooping enable

1.1.21 igmp-snooping enable

Syntax

igmp-snooping enable

undo igmp-snooping enable

デフォルト

無効

View

VLAN view

定義済みユーザロール

network-admin

説明

igmp-snooping enable コマンドは VLAN の IGMP snooping を有効にします。

undo igmp-snooping enable コマンドは VLAN の IGMP snooping を無効にします。

このコマンドを実行する前にグローバルで IGMP snooping 機能を有効にしてください。IGMP snooping の設定については、セクション 6 *マルチキャスト オペレーションマニュアル*の“*IGMP スヌーピング*”を参照してください。

例

グローバルと VLAN 2 の IGMP snooping を有効にします。

<Switch> system-view

[Switch] igmp-snooping

[Switch-igmp-snooping] quit

[Switch] vlan 2

[Switch-vlan2] igmp-snooping enable

関連コマンド

igmp-snooping

1.1.22 igmp-snooping fast-leave

Syntax

igmp-snooping fast-leave [**vlan** *vlan-list*]

undo igmp-snooping fast-leave [**vlan** *vlan-list*]

デフォルト

無効

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

vlan *vlan-list*: VLAN を指定します。半角スペースで区切り、10 まで設定することができます。VLAN を範囲で指定する形式は *start-vlan-id* **to** *end-vlan-id* です。設定範囲は 1～4094 です。指定しない場合、すべての VLAN に適用します。

説明

igmp-snooping fast-leave コマンドはポートで fast-leave 処理機能を有効にします。

undo igmp-snooping fast-leave コマンドはポートで fast-leave 処理機能を無効にします。

この機能は、ポートが leave メッセージを受信したとき、装置がマルチキャストグループの転送エントリから迅速にポートを削除します。

このコマンドは IGMP-snooping view の **fast-leave** コマンドと同一機能ですが、適用範囲が異なります。

- IGMP-snooping view の **fast-leave** コマンドはすべてのポートに適用されます。

- **igmp-snooping fast-leave** コマンドは現在のポートに適用されます。

ポートでは **igmp-snooping fast-leave** コマンドは IGMP-snooping view の **fast-leave** コマンドより優先されます。

例

GigabitEthernet 1/0/1 の VLAN 2 で fast-leave 処理機能を有効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] igmp-snooping fast-leave vlan 2

関連コマンド

fast-leave (IGMP-snooping view)

1.1.23 igmp-snooping general-query source-ip

Syntax

igmp-snooping general-query source-ip *ip-address*

undo igmp-snooping general-query source-ip

デフォルト

IGMP general クエリの送信元 IP アドレスは現在の VLAN インタフェースの IP アドレスです。現在の VLAN インタフェースに IP アドレスがない場合、送信元 IP アドレスは 0.0.0.0 です。

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

ip-address: IGMP general クエリの送信元 IP アドレスを指定します。

説明

igmp-snooping general-query source-ip コマンドは IGMP general クエリの送信元 IP アドレスを設定します。

undo igmp-snooping general-query source-ip コマンドはデフォルトに戻します。

このコマンドを実行する前に VLAN で IGMP snooping を有効にしてください。

例

VLAN 2 で IGMP snooping を有効にし、IGMP general クエリの送信元 IP アドレス 10.1.1.1 を設定します。

<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

関連コマンド

igmp-snooping enable

1.1.24 igmp-snooping group-limit

Syntax

igmp-snooping group-limit *limit* [**vlan** *vlan-list*]

undo igmp-snooping group-limit [**vlan** *vlan-list*]

デフォルト

4294967295

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

limit: ポートが加入できるマルチキャストグループの最大数を設定します。設定範囲は 0～4294967295 です。

vlan *vlan-list*: VLAN を指定します。半角スペースで区切り、10 まで設定することができます。VLAN を範囲で指定する形式は *start-vlan-id* **to** *end-vlan-id* です。設定範囲は 1～4094 です。指定しない場合、すべての VLAN に適用します。

説明

igmp-snooping group-limit コマンドはポートが加入できるマルチキャストグループの最大数を設定します。

undo igmp-snooping group-limit コマンドはデフォルトに戻します。

このコマンドはポートがダイナミックに加入するマルチキャストグループでのみ適用します。

例

VLAN 2 の GigabitEthernet 1/0/1 が加入できるマルチキャストグループの最大数を 10 に設定します。

<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

Syntax

igmp-snooping group-policy *ipv4-acl-number* [**vlan** *vlan-list*]

undo igmp-snooping group-policy [**vlan** *vlan-list*]

デフォルト

ポートでマルチキャストグループポリシーは設定されていません。ポートに接続されたホストはすべてのマルチキャストグループに加入することができます。

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

ipv4-acl-number: 標準 IPv4 ACL あるいは拡張 IPv4 ACL を指定します。設定範囲は 2000～3999 です。受信ホストは ACL が許可するマルチキャストグループのみ加入することができます。ACL が存在しない、あるいは ACL に正常なルールがないとき、受信ホストはマルチキャストグループに加入することができません。

vlan *vlan-list*: VLAN を指定します。半角スペースで区切り、10 まで設定することができます。VLAN を範囲で指定する形式は *start-vlan-id* **to** *end-vlan-id* です。設定範囲は 1～4094 です。指定しない場合、すべての VLAN に適用します。

説明

igmp-snooping group-policy コマンドは受信ホストが加入するマルチキャストグループを管理するため、ポートでマルチキャストグループポリシーを設定します。

undo igmp-snooping group-policy コマンドはポートのマルチキャストグループポリシーを削除します。

マルチキャストグループポリシーはホストが加入するマルチキャストグループを管理する IGMP report をフィルタします。

スタティックメンバポートは IGMP report を送信しないため、**group-policy** コマンドはスタティックメンバポートに適用されません。

IGMP-snooping view のすべてのポートでグローバルにマルチキャストグループポリシーを設定することができます。また interface view のポートでマルチキャストグループポリシーを設定することができます。ポートでは **igmp-snooping group-policy** コマンドは IGMP-snooping view の **group-policy** コマンドより優先されます。

IPv4 ACL でルールを設定するとき、以下の制限とガイドラインに従ってください。

- 標準 IPv4 ACL の **source** *source-address source-wildcard* パラメータはマルチキャストグループアドレスを指定します。
- 拡張 IPv4 ACL の **source** *source-address source-wildcard* パラメータは IGMP report のマルチキャスト送信元アドレスを指定します。**destination** *dest-address dest-wildcard* パラメータはマルチキャストグループアドレスを指定します。

  以下の IGMP report に一致するように、マルチキャスト送信元アドレス **source** *source-address source-wildcard* を 0.0.0.0 に設定します。

  - IGMPv1、IGMPv2 の report
  - マルチキャスト送信元アドレスを送信しない IGMPv3 IS_EX、IGMPv3 TO_EX の report
- ACL ルールの **time-range** *time-range-name* パラメータ、**fragment** パラメータを除く他のオプションパラメータは無視します。

異なる VLAN のポートに異なる ACL のルールを設定することができます。同一 VLAN で複数の ACL を設定した場合、最後に行った ACL のルールが適用されます。

例

ポートに接続されたホストがマルチキャストグループ 225.1.1.1 のみ加入できるように VLAN 2 の GigabitEthernet 1/0/1 でマルチキャストグループポリシーを設定します。

```
<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
```

関連コマンド

group-policy (IGMP-snooping view)

1.1.26 igmp-snooping host-aging-time

Syntax

igmp-snooping host-aging-time *seconds*

undo igmp-snooping host-aging-time

デフォルト

260 秒

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

seconds: VLAN のダイナミックメンバポートのエージングタイマを設定します。設定範囲は 1～8097894 秒です。

説明

igmp-snooping host-aging-time コマンドは VLAN のダイナミックメンバポートのエージングタイマを設定します。

undo igmp-snooping host-aging-time コマンドはデフォルトに戻します。

このコマンドを実行する前に VLAN で IGMP snooping 機能を有効にしてください。

このコマンドは **host-aging-time** コマンドと同一機能ですが、適用範囲が異なります。

- IGMP-snooping view の **host-aging-time** コマンドはすべての VLAN に適用されます。
- **igmp-snooping host-aging-time** コマンドは現在の VLAN に適用されます。

VLAN では **igmp-snooping host-aging-time** コマンドは IGMP-snooping view の **host-aging-time** コマンドより優先されます。

マルチキャストグループメンバを間違って削除しないようにするため、ダイナミックメンバポートのエージングタイマを、以下の式で計算された値よりも大きい値に設定してください。

[IGMP general クエリの間隔] ＋ [IGMP general クエリの最大応答時間]

ダイナミックメンバポートのエージングタイマを以下の式で計算した値に設定することを推奨します。

[IGMP general クエリの間隔] × 2 ＋ [IGMP general クエリの最大応答時間]

例

VLAN 2 の IGMP snooping を有効にし、VLAN のダイナミックメンバポートのエージングタイマを 300 秒に設定します。

<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

関連コマンド

- **host-aging-time (IGMP-snooping view)**
- **igmp-snooping enable**

1.1.27 igmp-snooping host-join

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** }

デフォルト

設定なし

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

group-address: マルチキャストグループの IP アドレスを指定します。設定範囲は 224.0.1.0～239.255.255.255 です。

source-ip *source-address*: マルチキャストソースの IP アドレスを指定します。マルチキャストソースを指定した場合、ポートをマルチキャストソースとグループのシミュレーティッドメンバホストとして設定します。マルチキャストソースを指定しない場合、マルチキャストグループのポートをシミュレーティッドメンバホストとして設定します。このパラメータは IGMPv3 snooping が動作する装置で有効です。

vlan *vlan-id*: VLAN の ID を指定します。設定範囲は 1～4094 です。

all: すべてのマルチキャストグループを指定します。

説明

igmp-snooping host-join コマンドはポートをマルチキャストグループのシミュレーティッドメンバホストとして設定します。

undo igmp-snooping host-join コマンドはシミュレーティッドメンバホストの設定を削除します。

IGMP version と、シミュレーティッドメンバホストが動作する IGMP snooping のバージョンは同一にしてください。スタティックメンバポートと異なり、シミュレーティッドメンバホストとして設定されたポートはダイナミックメンバポートのようにエージアウトします。

例

VLAN 2 のマルチキャストソースとマルチキャストグループの（1.1.1.1, 232.1.1.1）のシミュレーティッドメンバポートを GigabitEthernet 1/0/1 に設定します。

<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

Syntax

igmp-snooping last-member-query-interval *interval*

undo igmp-snooping last-member-query-interval

デフォルト

1 秒

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

interval: IGMP last member クエリ間隔を設定します。設定範囲は 1～25 秒です。

説明

igmp-snooping last-member-query-interval コマンドは VLAN の IGMP last member クエリ間隔を設定します。

undo igmp-snooping last-member-query-interval コマンドはデフォルトに戻します。

このコマンドを実行する前に VLAN で IGMP snooping 機能を有効にしてください。

このコマンドは **last-member-query-interval** コマンドと同一機能ですが、適用範囲が異なります。

- IGMP-snooping view の **last-member-query-interval** コマンドはすべての VLAN に適用されます。
- **igmp-snooping last-member-query-interval** コマンドは現在の VLAN に適用されます。

VLAN では **igmp-snooping last-member-query-interval** コマンドは IGMP-snooping view の **last-member-query-interval** コマンドより優先されます。

例

VLAN 2 の IGMP snooping を有効にし、VLAN 2 の IGMP last member クエリ間隔を 3 秒に設定します。

<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

関連コマンド

- **igmp-snooping enable**
- **last-member-query-interval (IGMP-snooping view)**

1.1.29 igmp-snooping leave source-ip

Syntax

igmp-snooping leave source-ip *ip-address*

undo igmp-snooping leave source-ip

デフォルト

IGMP leave クエリの送信元 IP アドレスは現在の VLAN インタフェースの IP アドレスです。現在の VLAN インタフェースに IP アドレスがない場合、送信元 IP アドレスは 0.0.0.0 です。

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

ip-address: IGMP leave メッセージの送信元 IP アドレスを指定します。

説明

igmp-snooping leave source-ip コマンドは IGMP leave メッセージの送信元 IP アドレスを設定します。

undo igmp-snooping leave source-ip コマンドはデフォルトに戻します。

このコマンドを実行する前に VLAN で IGMP snooping 機能を有効にしてください。

例

VLAN 2 で IGMP snooping を有効にし、IGMP leave メッセージの送信元 IP アドレスを 10.1.1.1 に設定します。

<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

関連コマンド

igmp-snooping enable

1.1.30 igmp-snooping max-response-time

Syntax

igmp-snooping max-response-time *seconds*

undo igmp-snooping max-response-time

デフォルト

10 秒

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

seconds: IGMP general クエリの最大応答時間を設定します。設定範囲は 1～3174 秒です。

説明

igmp-snooping max-response-time コマンドは VLAN の IGMP general クエリの最大応答時間を設定します。

undo igmp-snooping max-response-time コマンドはデフォルトに戻します。

このコマンドを実行する前に VLAN で IGMP snooping 機能を有効にしてください。

このコマンドは **max-response-time** コマンドと同一機能ですが、適用範囲が異なります。

- IGMP-snooping view の **max-response-time** コマンドはすべての VLAN に適用されます。
- **igmp-snooping max-response-time** コマンドは現在の VLAN に適用されます。

VLAN では **igmp-snooping max-response-time** コマンドは IGMP-snooping view の **max-response-time** コマンドより優先されます。

マルチキャストグループメンバを間違って削除しないようにするため、IGMP general クエリの最大応答時間は IGMP general クエリよりも小さいに設定してください。

例

VLAN 2 の IGMP snooping を有効にし、VLAN 2 の IGMP general クエリの最大応答時間を 5 秒に設定します。

<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

関連コマンド

- **igmp-snooping enable**

- **igmp-snooping query-interval**
- **max-response-time (IGMP-snooping view)**

1.1.31 igmp-snooping overflow-replace

Syntax

igmp-snooping overflow-replace [**vlan** *vlan-list*]

undo igmp-snooping overflow-replace [**vlan** *vlan-list*]

デフォルト

無効

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

vlan *vlan-list*: VLAN を指定します。半角スペースで区切り、10 まで設定することができます。VLAN を範囲で指定する形式は *start-vlan-id* **to** *end-vlan-id* です。設定範囲は 1～4094 です。指定しない場合、すべての VLAN に適用します。

説明

igmp-snooping overflow-replace コマンドはポートでマルチキャストグループ置き換え機能を有効にします。

undo igmp-snooping overflow-replace コマンドはポートでマルチキャストグループ置き換え機能を無効にします。

このコマンドはポートがダイナミックに加入するマルチキャストグループでのみ適用します。

このコマンドは **overflow-replace** コマンドと同一機能ですが、適用範囲が異なります。

- IGMP-snooping view の **overflow-replace** コマンドはすべてのポートに適用されます。
- **igmp-snooping overflow-replace** コマンドは現在のポートに適用されます。

ポートでは **igmp-snooping overflow-replace** コマンドは IGMP-snooping view の **overflow-replace** コマンドより優先されます。

例

GigabitEthernet 1/0/1 の VLAN2 でマルチキャストグループ置き換え機能を有効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] igmp-snooping overflow-replace vlan 2

関連コマンド

overflow-replace (IGMP-snooping view)

1.1.32 igmp-snooping proxy enable

Syntax

igmp-snooping proxy enable

undo igmp-snooping proxy enable

デフォルト

無効

View

VLAN view

定義済みユーザロール

network-admin

説明

igmp-snooping proxy enable コマンドは VLAN で IGMP snooping プロキシ—機能を有効にします。

undo igmp-snooping proxy enable コマンドは VLAN で IGMP snooping プロキシ—機能を無効にします。

このコマンドを実行する前に VLAN で IGMP snooping 機能を有効にしてください。

igmp-snooping proxy enable コマンドはマルチキャスト VLAN のサブ VLAN には適用しません。

例

IGMP snooping を有効にし、VLAN 2 で IGMP snooping プロキシ—機能を有効にします。

<Switch> system-view

[Switch] igmp-snooping

[Switch-igmp-snooping] quit

[Switch] vlan 2

[Switch-vlan2] igmp-snooping enable

[Switch-vlan2] igmp-snooping proxy enable

関連コマンド

- **igmp-snooping enable**
- **subvlan (multicast-VLAN view)**

1.1.33 igmp-snooping querier

Syntax

igmp-snooping querier

undo igmp-snooping querier

デフォルト

無効

View

VLAN view

定義済みユーザロール

network-admin

説明

igmp-snooping querier コマンドは IGMP snooping クエリアを有効にします。

undo igmp-snooping querier コマンドは IGMP snooping クエリアを無効にします。

このコマンドを実行する前に、VLAN の IGMP snooping 機能を有効にしてください。

このコマンドは、マルチキャスト VLAN からサブ VLAN を削除した後、サブ VLAN に適用されます。

例

VLAN 2 の IGMP snooping を有効にし、IGMP snooping クエリアを有効にします。

<Switch> system-view

[Switch] igmp-snooping

[Switch-igmp-snooping] quit

[Switch] vlan 2

[Switch-vlan2] igmp-snooping enable

[Switch-vlan2] igmp-snooping querier

関連コマンド

- **igmp-snooping enable**
- **subvlan (multicast VLAN view)**

1.1.34 igmp-snooping query-interval

Syntax

igmp-snooping query-interval *interval*

undo igmp-snooping query-interval

デフォルト

125 秒

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

interval: IGMP general クエリの送信間隔を設定します。設定範囲は 2～31744 秒です。

説明

igmp-snooping query-interval コマンドは VLAN の IGMP general クエリ送信間隔を設定します。

undo igmp-snooping query-interval コマンドはデフォルトに戻します。

このコマンドを実行する前に、VLAN の IGMP snooping 機能を有効にしてください。

間違ってマルチキャストグループメンバを削除しないように、IGMP general クエリの最大応答時間より IGMP general クエリの送信間隔を大きくしてください。

例

VLAN 2 の IGMP snooping を有効にし、IGMP general クエリ送信間隔を 20 秒に設定します。

<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

関連コマンド

- **igmp-snooping enable**
- **igmp-snooping max-response-time**
- **igmp-snooping querier**
- **max-response-time**

1.1.35 igmp-snooping report source-ip

Syntax

igmp-snooping report source-ip *ip-address*

undo igmp-snooping report source-ip

デフォルト

IGMP report の送信元 IP アドレスは、現在の VLAN インタフェースの IP アドレスです。現在の VLAN インタフェースに IP アドレスが設定されていない場合、送信元 IP アドレスは 0.0.0.0 です。

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

ip-address: IGMP report の送信元 IP アドレスを指定します。

説明

igmp-snooping report source-ip コマンドは IGMP report の送信元 IP アドレスを設定します。

undo igmp-snooping report source-ip コマンドはデフォルトに戻します。

このコマンドを実行する前に、VLAN の IGMP snooping 機能を有効にしてください。

例

VLAN 2 で IGMP snooping を有効にし、IGMP report の送信元 IP アドレスを 10.1.1.1 に設定します。

<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

関連コマンド

igmp-snooping enable

1.1.36 igmp-snooping router-aging-time

Syntax

igmp-snooping router-aging-time *seconds*

undo igmp-snooping router-aging-time

デフォルト

260 秒

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

seconds: VLAN のダイナミックルータポートのエージングタイマを設定します。設定範囲は 1～8097894 秒です。

説明

igmp-snooping router-aging-time コマンドは VLAN のダイナミックルータポートのエージングタイマを設定します。

undo igmp-snooping router-aging-time コマンドはデフォルトに戻します。

このコマンドを実行する前に、VLAN の IGMP snooping 機能を有効にしてください。

このコマンドは **router-aging-time** コマンドと同一機能ですが、適用範囲が異なります。

- IGMP-snooping view の **router-aging-time** コマンドはすべての VLAN に適用されます。
- **igmp-snooping router-aging-time** コマンドは現在の VLAN に適用されます。

VLAN では **igmp-snooping router-aging-time** コマンドは IGMP-snooping view の **router-aging-time** コマンドより優先されます。

例

VLAN 2 の IGMP snooping を有効にし、ダイナミックルータポートのエージングタイマを 100 秒に設定します。

<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

関連コマンド

- **igmp-snooping enable**
- **router-aging-time (IGMP-snooping view)**

1.1.37 igmp-snooping source-deny

Syntax

igmp-snooping source-deny

undo igmp-snooping source-deny

デフォルト

無効

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

説明

igmp-snooping source-deny コマンドは、すべての受信したマルチキャストデータパケットを廃棄するため、ポートでマルチキャストソースポートフィルタを有効にします。

undo igmp-snooping source-deny コマンドは現在のポートでマルチキャストソースポートフィルタを無効にします。

このコマンドは **source-deny** コマンドと同一機能ですが、適用範囲が異なります。

- IGMP-snooping view の **source-deny** マンドはすべてのポートに適用されます。
- **igmp-snooping source-deny** コマンドは現在のポートに適用されます。

ポートでは **igmp-snooping source-deny** コマンドは IGMP-snooping view の **source-deny** コマンドの優先度は同一です。最後に行われた設定が適用されます。

例

GigabitEthernet 1/0/1 でマルチキャストソースポートフィルタを有効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] igmp-snooping source-deny

関連コマンド

source-deny (IGMP-snooping view)

1.1.38 igmp-snooping special-query source-ip

Syntax

igmp-snooping special-query source-ip *ip-address*

undo igmp-snooping special-query source-ip

デフォルト

VLAN で IGMP group-specific クエリの送信元 IP アドレスは以下のいずれかとなります。

- VLAN の IGMP snooping クエリアが IGMP general クエリを受信したとき、IGMP group-specific クエリの送信元 IP アドレスは IGMP general クエリの送信元 IP アドレスです。
- VLAN の IGMP snooping クエリアが IGMP general クエリを受信していない場合、IGMP group-specific クエリの送信元 IP アドレスは現在の VLAN インタフェースの IP アドレスです。
- VLAN の IGMP snooping クエリアが IGMP general クエリを受信しておらず、現在の VLAN インタフェースに IP アドレスが設定されていない場合、送信元 IP アドレスは 0.0.0.0 です。

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

ip-address: IGMP group-specific クエリの送信元 IP アドレスを指定します。

説明

igmp-snooping special-query source-ip コマンドは IGMP group-specific クエリの送信元 IP アドレスを設定します。

undo igmp-snooping special-query source-ip コマンドはデフォルトに戻します。

このコマンドを実行する前に、VLAN の IGMP snooping 機能を有効にしてください。

例

VLAN 2 の IGMP snooping を有効にし、IGMP group-specific クエリの送信元 IP アドレス 10.1.1.1 を設定します。

<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

関連コマンド

igmp-snooping enable

1.1.39 igmp-snooping static-group

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** }

デフォルト

設定なし

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

group-address: マルチキャストグループの IP アドレスを指定します。設定範囲は 224.0.1.0～239.255.255.255 です。

source-ip *source-address*: マルチキャストソースの IP アドレスを指定します。マルチキャストソースを指定した場合、ポートをマルチキャストソースとグループのスタティックメンバポートとして設定します。マルチキャストソースを指定しない場合、ポートをマルチキャストグループのスタティックメンバポートとして設定します。このパラメータは IGMPv3 snooping が動作する装置で有効です。

vlan *vlan-id*: VLAN の ID を指定します。設定範囲は 1～4094 です。

all: すべての VLAN を指定します。

説明

igmp-snooping static-group コマンドはマルチキャストグループのスタティックメンバポートを設定します。

undo igmp-snooping static-group コマンドはスタティックメンバポートを削除します。

例

VLAN 2 のマルチキャストソースとマルチキャストグループの（1.1.1.1, 225.0.0.1）のスタティックメンバポートを GigabitEthernet 1/0/1 に設定します。

<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

Syntax

igmp-snooping static-router-port vlan *vlan-id*

undo igmp-snooping static-router-port { **all** | **vlan** *vlan-id* }

デフォルト

設定なし

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

all: すべての VLAN を指定します。

vlan *vlan-id*: VLAN の ID を指定します。設定範囲は 1～4094 です。

説明

igmp-snooping static-router-port コマンドはスタティックルータポートを設定します。

undo igmp-snooping static-router-port コマンドはスタティックルータポートを削除します。

例

VLAN 2 の GigabitEthernet 1/0/1 をスタティックルータポートに設定します。

<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

Syntax

igmp-snooping version *version-number*

undo igmp-snooping version

デフォルト

2

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

version-number: IGMP snooping のバージョンを指定します。2 あるいは 3 です。

説明

igmp-snooping version コマンドは IGMP snooping のバージョンを指定します。

undo igmp-snooping version コマンドはデフォルトに戻します。

このコマンドを実行する前に、VLAN の IGMP snooping 機能を有効にしてください。

例

VLAN 2 の IGMP snooping を有効にし、IGMP snooping のバージョンを 3 に指定します。

<Switch> system-view

[Switch] igmp-snooping

[Switch-igmp-snooping] quit

[Switch] vlan 2

[Switch-vlan2] igmp-snooping enable

[Switch-vlan2] igmp-snooping version 3

関連コマンド

igmp-snooping enable

1.1.42 last-member-query-interval (IGMP-snooping view)

Syntax

last-member-query-interval *interval*

undo last-member-query-interval

デフォルト

1 秒

View

IGMP-snooping view

定義済みユーザロール

network-admin

パラメータ

interval: IGMP last member クエリ間隔を設定します。設定範囲は 1～25 秒です。

説明

last-member-query-interval コマンドはグローバルで IGMP last member クエリ間隔を設定します。

undo last-member-query-interval コマンドはデフォルトに戻します。

このコマンドは **igmp-snooping last-member-query-interval** コマンドと同一機能ですが、適用範囲が異なります。

- IGMP-snooping view の **last-member-query-interval** コマンドはすべての VLAN に適用されます。
- **igmp-snooping last-member-query-interval** コマンドは現在の VLAN に適用されます。

VLAN では **igmp-snooping last-member-query-interval** コマンドは IGMP-snooping view の **last-member-query-interval** コマンドより優先されます。

例

IGMP last member クエリ間隔を 3 秒に設定します。

<Switch> system-view

[Switch] igmp-snooping

[Switch-igmp-snooping] last-member-query-interval 3

関連コマンド

igmp-snooping last-member-query-interval

1.1.43 mac-address multicast

Syntax

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*]

Layer 2 aggregate interface view、Layer 2 Ethernet interface view：

mac-address multicast *mac-address* **vlan** *vlan-id*

undo mac-address [**multicast**] *mac-address* **vlan** *vlan-id*

デフォルト

設定なし

View

System view

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

mac-address: マルチキャスト MAC アドレスを指定します。形式は H-H-H です。マルチキャスト MAC アドレスは未使用でなくてはいけません。マルチキャスト MAC アドレスは最上位オクテットの最下位ビット（LSB）が 1 です。

interface *interface-list*: インタフェースを指定します。半角スペースで区切り、4 まで設定するか、インタフェースの範囲で設定することができます。インタフェースを範囲で指定する形式は *start-interface-type interface-number* **to** *end-interface-type interface-number* です。*interface-type* と *interface-number* はインタフェースのタイプと番号を指定します。インタフェースのタイプはレイヤ 2 Ethernet インタフェースとアグリゲートインタフェースが含まれます。

vlan *vlan-id*: VLAN の ID を指定します。設定範囲は 1～4094 です。指定した VLAN は事前に存在する必要があります。指定したインタフェースが VLAN に所属していない場合、画面に表示されます。

説明

mac-address multicast コマンドはスタティックマルチキャスト MAC アドレスエントリを設定します。

undo mac-address multicast コマンドはスタティックマルチキャスト MAC アドレスエントリを削除します。

このコマンドを実行する前に IP マルチキャストルーティングを有効にする必要はありません。

system view で指定したインタフェース、あるいは interface view で現在のインタフェースにスタティックマルチキャスト MAC アドレスエントリを設定することができます。

undo mac-address multicast コマンドで **multicast** を指定しない場合、スタティックユニキャスト MAC アドレスエントリとマルチキャスト MAC アドレスエントリを含むすべての MAC アドレスエントリを削除します。

例

VLAN 2 に 0100-0001-0001 のマルチキャスト MAC アドレスエントリを作成し、VLAN 2 の GigabitEthernet 1/0/1～GigabitEthernet 1/0/5 を出力ポートに指定します。

<Switch> system-view

[Switch] mac-address multicast 0100-0001-0001 interface gigabitethernet 1/0/1 to gigabitethernet 1/0/5 vlan 2

GigabitEthernet 1/0/1 でスタティックマルチキャスト MAC アドレスエントリを設定します。マルチキャスト MAC アドレスは 0100-0001-0001、出力インタフェースは GigabitEthernet 1/0/1、VLAN は 2 です。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] mac-address multicast 0100-0001-0001 vlan 2

関連コマンド

display mac-address multicast

1.1.44 max-response-time (IGMP-snooping view)

Syntax

max-response-time *seconds*

undo max-response-time

デフォルト

10 秒

View

IGMP-snooping view

定義済みユーザロール

network-admin

パラメータ

seconds: IGMP general クエリの最大応答時間を設定します。設定範囲は 1～3174 秒です。

説明

max-response-time コマンドはグローバルで IGMP general クエリの最大応答時間を設定します。

undo max-response-time コマンドはデフォルトに戻します。

このコマンドは **igmp-snooping max-response-time** コマンドと同一機能ですが、適用範囲が異なります。

- IGMP-snooping view の **max-response-time** コマンドはすべての VLAN に適用されます。
- **igmp-snooping max-response-time** コマンドは現在の VLAN に適用されます。

VLAN では **igmp-snooping max-response-time** コマンドは IGMP-snooping view の **max-response-time** コマンドより優先されます。

マルチキャストグループメンバを間違って削除しないようにするため、IGMP general クエリの最大応答時間は IGMP general クエリよりも小さいに設定してください。

例

グローバルで IGMP general クエリの最大応答時間を 5 秒に設定します。

<Switch> system-view

[Switch] igmp-snooping

[Switch-igmp-snooping] max-response-time 5

関連コマンド

- **igmp-snooping max-response-time**
- **igmp-snooping query-interval**

1.1.45 overflow-replace (IGMP-snooping view)

Syntax

overflow-replace [**vlan** *vlan-list*]

undo overflow-replace [**vlan** *vlan-list*]

デフォルト

無効

View

IGMP-snooping view

定義済みユーザロール

network-admin

パラメータ

vlan *vlan-list*: VLAN を指定します。半角スペースで区切り、10 まで設定することができます。VLAN を範囲で指定する形式は *start-vlan-id* **to** *end-vlan-id* です。設定範囲は 1～4094 です。指定しない場合、すべての VLAN に適用します。

説明

overflow-replace コマンドはグローバルでマルチキャストグループ置き換え機能を有効にします。

undo overflow-replace コマンドはグローバルでマルチキャストグループ置き換え機能を無効にします。

このコマンドはポートがダイナミックに加入するマルチキャストグループでのみ適用します。マルチキャストグループのスタティックメンバポートを設定した場合、マルチキャストグループに適用されません。

このコマンドは **igmp-snooping overflow-replace** コマンドと同一機能ですが、適用範囲が異なります。

- IGMP-snooping view の **overflow-replace** コマンドはすべてのポートに適用されます。
- **igmp-snooping overflow-replace** コマンドは現在のポートに適用されます。

ポートでは **igmp-snooping overflow-replace** コマンドは IGMP-snooping view の **overflow-replace** コマンドより優先されます。

例

VLAN2 でマルチキャストグループ置き換え機能を有効にします。

<Switch> system-view

[Switch] igmp-snooping

[Switch-igmp-snooping] overflow-replace vlan 2

関連コマンド

igmp-snooping overflow-replace

1.1.46 report-aggregation (IGMP-snooping view)

Syntax

report-aggregation

undo report-aggregation

デフォルト

有効

View

IGMP-snooping view

定義済みユーザロール

network-admin

説明

report-aggregation コマンドは IGMP report 抑制機能を有効にします。

undo report-aggregation コマンドは IGMP report 抑制機能を無効にします。

例

IGMP report 抑制機能を無効にします。

<Switch> system-view

[Switch] igmp-snooping

[Switch-igmp-snooping] undo report-aggregation

1.1.47 reset igmp-snooping group

Syntax

reset igmp-snooping group { *group-address* [*source-address*] | **all** } [**vlan** *vlan-id*]

View

User view

定義済みユーザロール

network-admin

パラメータ

group-address: マルチキャストグループの IP アドレスを指定します。設定範囲は 224.0.1.0～239.255.255.255 です。

source-address: マルチキャストソースの IP アドレスを指定します。指定しない場合、すべてのマルチキャストソースのダイナミック IGMP snooping 転送エントリを削除します。

all: すべてのマルチキャストグループを指定します。

vlan *vlan-id*: VLAN の ID を指定します。設定範囲は 1～4094 です。指定しない場合、すべての VLAN のダイナミック IGMP snooping 転送エントリを削除します。

説明

reset igmp-snooping group コマンドはダイナミック IGMP snooping 転送エントリを削除します。

例

すべてのダイナミック IGMP snooping 転送エントリを削除します。

<Switch> reset igmp-snooping group all

関連コマンド

display igmp-snooping group

1.1.48 reset igmp-snooping router-port

Syntax

reset igmp-snooping router-port { **all** | **vlan** *vlan-id*]

View

User view

定義済みユーザロール

network-admin

パラメータ

all: すべての VLAN を指定します。

vlan *vlan-id*: VLAN の ID を指定します。設定範囲は 1～4094 です。指定しない場合、すべての VLAN のダイナミックルータポートを削除します。

説明

reset igmp-snooping router-port コマンドはダイナミックルータポートの情報を削除します。

例

すべてのダイナミックルータポートの情報を削除します。

<Switch> reset igmp-snooping router-port all

関連コマンド

display igmp-snooping router-port

1.1.49 reset igmp-snooping statistics

Syntax

reset igmp-snooping statistics

View

User view

定義済みユーザロール

network-admin

説明

reset igmp-snooping statistics コマンドは IGMP snooping によって学習した IGMP メッセージと PIMv2 hello メッセージの統計情報を削除します。

例

IGMP snooping によって学習した IGMP メッセージと PIMv2 hello メッセージの統計情報を削除します。

<Switch> reset igmp-snooping statistics

関連コマンド

display igmp-snooping statistics

1.1.50 router-aging-time (IGMP-snooping view)

Syntax

router-aging-time *seconds*

undo router-aging-time

デフォルト

260 秒

View

IGMP-snooping view

定義済みユーザロール

network-admin

パラメータ

seconds: ダイナミックルータポートのエージングタイマを設定します。設定範囲は 1～8097894 秒です。

説明

router-aging-time コマンドはグローバルでダイナミックルータポートのエージングタイマを設定します。

undo router-aging-time コマンドはデフォルトに戻します。

このコマンドは **igmp-snooping router-aging-time** コマンドと同一機能ですが、適用範囲が異なります。

- IGMP-snooping view の **router-aging-time** コマンドはすべての VLAN に適用されます。
- **igmp-snooping router-aging-time** コマンドは現在の VLAN に適用されます。

VLAN では **igmp-snooping router-aging-time** コマンドは IGMP-snooping view の **router-aging-time** コマンドより優先されます。

例

グローバルでダイナミックルータポートのエージングタイマを 100 秒に設定します。

<Switch> system-view

[Switch] igmp-snooping

[Switch-igmp-snooping] router-aging-time 100

関連コマンド

igmp-snooping router-aging-time

1.1.51 source-deny (IGMP-snooping view)

Syntax

source-deny port *interface-list*

undo source-deny port *interface-list*

デフォルト

無効

View

IGMP-snooping view

定義済みユーザロール

network-admin

パラメータ

port *interface-list*: ポートリストを指定します。ポートのアイテムを半角スペースで区切り、ポートのタイプと番号を指定するか、ポートの範囲で指定します。ポートを範囲で指定する形式は *start-interface-type interface-number* **to** *end-interface-type interface-number* です。

説明

source-deny コマンドはすべての受信したマルチキャストデータパケットを廃棄するため、ポートでマルチキャストソースポートのフィルタを有効にします。

undo source-deny コマンドはポートでマルチキャストソースポートのフィルタを無効にします。

このコマンドは **igmp-snooping source-deny** コマンドと同一機能ですが、適用範囲が異なります。

- IGMP-snooping view の **source-deny** マンドはすべてのポートに適用されます。
- **igmp-snooping source-deny** コマンドは現在のポートに適用されます。

ポートでは **igmp-snooping source-deny** コマンドは IGMP-snooping view の **source-deny** コマンドの優先度は同一です。最後に行われた設定が適用されます。

例

GigabitEthernet 1/0/1～GigabitEthernet 1/0/4 でマルチキャストソースポートのフィルタを有効にします。

<Switch> system-view

[Switch] igmp-snooping

[Switch-igmp-snooping] source-deny port gigabitethernet 1/0/1 to gigabitethernet 1/0/4

関連コマンド

igmp-snooping source-deny

目次

このセクションのページは **6-x-x** です。

2 章 マルチキャスト VLAN 2-1
2.1 マルチキャスト VLAN 設定コマンド 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 2-4
2.1.4 multicast-vlan 2-6
2.1.5 multicast-vlan entry-limit 2-8
2.1.6 port (multicast-VLAN view) 2-8
2.1.7 port multicast-vlan 2-9
2.1.8 reset multicast-vlan group 2-10
2.1.9 subvlan (multicast-VLAN view) 2-11

2章 マルチキャスト VLAN

2.1 マルチキャストVLAN設定コマンド

2.1.1 display multicast-vlan

Syntax

display multicast-vlan [*vlan-id*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

vlan-id: マルチキャスト VLAN の ID を指定します。設定範囲は 1～4094 です。指定しない場合、すべてのマルチキャスト VLAN の情報を表示します。

説明

display multicast-vlan コマンドはマルチキャスト VLAN の情報を表示します。

例

すべてのマルチキャスト VLAN の情報を表示します。

<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):
```

表 2-1 コマンド出力

フィールド	説明
Total 2 multicast VLANs	マルチキャストVLANの総数です。
Sub-VLAN list(3 in total)	マルチキャストVLANのサブVLANと、サブVLANの総数です。
Port list(3 in total)	マルチキャストVLANのポートリストとポートの総数です。

2.1.2 display multicast-vlan forwarding-table

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*] *

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

group-address: マルチキャストグループの IP アドレスを指定します。設定範囲は 224.0.0.0～239.255.255.255 です。マルチキャストグループを指定しない場合、すべてのマルチキャストグループのマルチキャスト VLAN 転送エントリを表示します。

mask { *mask-length* | *mask* }: マルチキャストグループアドレスのマスク長あるいはサブネットマスクを指定します。マスク長の設定範囲は 4～32 です。デフォルトは 32 です。マスクのデフォルトは 255.255.255.255 です。

source-address: マルチキャストソースの IP アドレスを指定します。マルチキャストソースを指定しない場合、すべてのマルチキャストソースのマルチキャスト VLAN 転送エントリを表示します。

mask { *mask-length* | *mask* }: マルチキャストソースアドレスのマスク長あるいはサブネットマスクを指定します。マスク長の設定範囲は 0～32 です。デフォルトは 32 です。マスクのデフォルトは 255.255.255.255 です。

slot *slot-number*: IRF スタックメンバ装置を指定します。*slot-number* は IRF スタックメンバ装置の ID を示します。指定しない場合、IRF スタックユニットのマスタ装置のマルチキャスト VLAN 転送エントリを表示します。

subvlan *vlan-id*: サブ VLAN の ID を指定します。指定しない場合、すべてのサブ VLAN のマルチキャスト VLAN 転送エントリを表示します。

vlan *vlan-id*: マルチキャスト VLAN の ID を指定します。設定範囲は 1～4094 です。指定しない場合、すべてのマルチキャスト VLAN のマルチキャスト VLAN 転送エントリを表示します。

説明

display multicast-vlan forwarding-table コマンドはマルチキャスト VLAN 転送エントリを表示します。

例

すべてのマルチキャスト VLAN 転送エントリを表示します。

<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
```

表 2-2 コマンド出力

フィールド	説明
Multicast VLAN 100 Forwarding Table	マルチキャストVLAN 100の転送テーブルです。
Total 1 entries, 1 matched	転送エントリ（S,G）の総数と一致するエントリの総数です。
00001	（S,G）エントリのシーケンス番号です。
(1.1.1.1, 255.0.0.1)	（S,G）エントリです。Sが**0.0.0.0**の場合、すべてのマルチキャストソースを示します。
Flags	（S,G）エントリの現在の状態です。1つのフラグあるいは複数のフラグの合計を示します。たとえば、0x10000はエントリが1つのフラグ0x10000のみあることを示します。このフィールドの値を表 2-3に示します。
List of sub-VLANs (3 in total)	マルチキャストVLANのサブVLANとサブVLANの総数です。

表 2-3 フィールドの値

値	意味
0x1	エントリが非アクティブ状態です。
0x4	エントリがアップデートに失敗しています。
0x8	エントリがサブVLAN情報のアップデートに失敗しています。
0x200	エントリが円滑な状態です。
0x10000	エントリがマルチキャストVLANの転送エントリです。

2.1.3 display multicast-vlan group

Syntax

display multicast-vlan group [*source-address* | *group-address* | **slot** *slot-number* | **verbose** | **vlan** *vlan-id*] *

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

source-address: マルチキャストソースの IP アドレスを指定します。マルチキャストソースを指定しない場合、マルチキャスト VLAN のすべてのマルチキャストソースのマルチキャストグループの情報を表示します。

group-address: マルチキャストグループの IP アドレスを指定します。設定範囲は 224.0.1.0～239.255.255.255 です。マルチキャストグループを指定しない場合、マルチキャスト VLAN のすべてのマルチキャストグループの情報を表示します。

slot *slot-number*: IRF スタックメンバ装置を指定します。*slot-number* は IRF スタックメンバ装置の ID を示します。指定しない場合、IRF スタックユニットのマスタ装置のマルチキャスト VLAN のマルチキャストグループの情報を表示します。

verbose: 詳細情報を表示します。

vlan *vlan-id*: マルチキャスト VLAN の ID を指定します。設定範囲は 1～4094 です。指定しない場合、すべてのマルチキャスト VLAN のマルチキャストグループの情報を表示します。

説明

display multicast-vlan group コマンドはマルチキャスト VLAN のマルチキャストグループの情報を表示します。

例

すべてのマルチキャスト VLAN のすべてのマルチキャストグループの詳細情報を表示します。

<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):
```

表 2-4 コマンド出力

フィールド	説明
Total 6 entries	（S,G）エントリの総数です。
Multicast VLAN 10: Total 3 entries	マルチキャストVLAN 10の（S,G）エントリの総数です。

フィールド	説明
(0.0.0.0, 226.1.1.6)	（S,G）エントリです。Sが**0.0.0.0**の場合、すべてのマルチキャストソースを示します。
Flags	（S,G）エントリの現在の状態です。1つのフラグあるいは複数のフラグの合計を示します。たとえば、0x70000020はエントリがフラグ0x20、0x10000000、0x20000000、0x40000000があることを示します。このフィールドの値を表 2-5に示します。
Sub-VLANs (1 in total)	マルチキャストVLANのサブVLANとサブVLANの総数です。

表 2-5 フィールドの値

値	意味
0x10	エントリがマルチキャストVLANによって作成されました。
0x20	エントリがマルチキャストVLANのサブVLANによって作成されました。
0x40	エントリが削除されました。
0x10000000	この値は以下の状態の1つを示します。 ● エントリが新規に作成されました。 ● 装置は（S,G）エントリに一致するIGMP クエリを受信しましたが、IGMP general クエリ送信間隔内に一致するIGMPv1 reportを受信していません。
0x20000000	装置はIGMP general クエリ送信間隔内に（S,G）エントリに一致するIGMPv2あるいはIGMPv3 reportを受信していません。
0x40000000	装置はIGMP general クエリ送信間隔内に（S,G）エントリに一致するIGMPv3 IS_EX(NULL) reportを受信していません。

関連コマンド

reset multicast-vlan group

2.1.4 multicast-vlan

Syntax

multicast-vlan *vlan-id*

undo multicast-vlan { **all** | *vlan-id* }

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

vlan-id: VLAN の ID を指定します。設定範囲は 1～4094 です。

all: すべてのマルチキャスト VLAN を指定します。

説明

multicast-vlan コマンドはマルチキャスト VLAN を設定し、multicast VLAN view に移行します。

undo multicast-vlan コマンドはマルチキャスト VLAN を削除します。

装置のマルチキャスト VLAN の総数はシステムがサポートする最大数を超過することができません。

マルチキャスト VLAN として設定されている VLAN で、IGMP snooping を有効にしてください。

IP マルチキャストルーティングが有効な装置でマルチキャスト VLAN を設定しないでください。

例

VLAN 100 で IGMP snooping を有効にします。マルチキャスト VLAN として VLAN 100 を設定し、multicast VLAN view に移行します。

<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]

関連コマンド

igmp-snooping enable

2.1.5 multicast-vlan entry-limit

Syntax

multicast-vlan entry-limit *limit*

undo multicast-vlan entry-limit

デフォルト

2000

View

System view

定義済みユーザロール

network-admin

パラメータ

limit: マルチキャスト VLAN 転送エントリの最大数を設定します。設定範囲は 0～2000 です。

説明

multicast-vlan entry-limit コマンドはマルチキャスト VLAN 転送エントリの最大数を設定します。

undo multicast-vlan entry-limit コマンドはデフォルトに戻します。

例

マルチキャスト VLAN 転送エントリの最大数を 128 に設定します。

<Switch> system-view

[Switch] multicast-vlan entry-limit 128

関連コマンド

entry-limit (IGMP-snooping view)

2.1.6 port (multicast-VLAN view)

Syntax

port *interface-list*

undo port { **all** | *interface-list* }

デフォルト

設定なし

View

Multicast VLAN view

定義済みユーザロール

network-admin

パラメータ

interface-list: ポートあるいはポート範囲を指定します。形式は *interface-type interface-number* です。ポート範囲の形式は *interface-type interface-number* **to** *interface-type interface-number* です。

all: 現在のマルチキャスト VLAN のすべてのユーザポートを指定します。

説明

port コマンドはマルチキャスト VLAN にユーザポートを割り当てます。

undo port コマンドはマルチキャスト VLAN からユーザポートを取り外します。

マルチキャスト VLAN のユーザポートとして Ethernet ポートとアグリゲートインタフェースを割り当てることができます。ポートは 1 つのマルチキャスト VLAN にのみ所属することができます。

ポートが所属している VLAN で IGMP snooping を有効にする必要があります。

例

GigabitEthernet 1/0/1～GigabitEthernet 1/0/3 をマルチキャスト VLAN 100 に割り当てます。

<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

Syntax

port multicast-vlan *vlan-id*

undo port multicast-vlan

デフォルト

設定なし

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id: マルチキャスト VLAN の ID を指定します。設定範囲は 1～4094 です。

説明

port multicast-vlan コマンドはマルチキャスト VLAN にポートを割り当てます。

undo port multicast-vlan コマンドはデフォルトに戻します。

ポートは 1 つのマルチキャスト VLAN にのみ所属することができます。

ポートが所属している VLAN で IGMP snooping を有効にする必要があります。

例

GigabitEthernet 1/0/1 をマルチキャスト VLAN 100 に割り当てます。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] port multicast-vlan 100

2.1.8 reset multicast-vlan group

Syntax

reset multicast-vlan group [*source-address* [**mask** { *mask-length* | *mask* }] | *group-address* [**mask** { *mask-length* | *mask* }] | **vlan** *vlan-id*] *

View

User view

定義済みユーザロール

network-admin

パラメータ

source-address: マルチキャストソースの IP アドレスを指定します。マルチキャストソースを指定しない場合、すべてのマルチキャストソースのマルチキャスト VLAN 転送エントリを削除します。

mask { *mask-length* | *mask* }: マルチキャストソースアドレスのマスク長あるいはサブネットマスクを指定します。マスク長の設定範囲は 0～32 です。デフォルトは 32 です。マスクのデフォルトは 255.255.255.255 です。

group-address: マルチキャストグループの IP アドレスを指定します。設定範囲は 224.0.1.0～239.255.255.255 です。マルチキャストグループを指定しない場合、すべてのマルチキャストグループのマルチキャスト VLAN 転送エントリを削除します。

mask { *mask-length* | *mask* }: マルチキャストソースアドレスのマスク長あるいはサブネットマスクを指定します。マスク長の設定範囲は 4～32 です。デフォルトは 32 です。マスクのデフォルトは 255.255.255.255 です。

vlan *vlan-id*: マルチキャスト VLAN の ID を指定します。設定範囲は 1～4094 です。指定しない場合、すべてのマルチキャスト VLAN のマルチキャスト VLAN 転送エントリを削除します。

説明

reset multicast-vlan group コマンドはマルチキャスト VLAN 転送エントリを削除します。

例

すべてのマルチキャスト VLAN 転送エントリを削除します。

<Switch> reset multicast-vlan group

関連コマンド

display multicast-vlan group

2.1.9 subvlan (multicast-VLAN view)

Syntax

subvlan *vlan-list*

undo subvlan { **all** | *vlan-list* }

デフォルト

設定なし

View

Multicast VLAN view

定義済みユーザロール

network-admin

パラメータ

vlan-list: VLAN を指定します。半角スペースで区切り 10 まで設定するか、VLAN の範囲で設定することができます。VLAN を範囲で指定する形式は *start-vlan-id* **to** *end-vlan-id* です。設定範囲は 1～4094 です。サブ VLAN として設定される VLAN は事前に作成され

ている必要があります。マルチキャスト VLAN に指定されている VLAN あるいはサブ VLAN 以外である必要があります。

all: 現在のマルチキャスト VLAN のすべてのサブ VLAN を指定します。

説明

subvlan コマンドはマルチキャスト VLAN にサブ VLAN を割り当てます。

undo subvlan コマンドはマルチキャスト VLAN からサブ VLAN を削除します。

サブ VLAN として設定される VLAN で、IGMP snooping を有効にしてください。

例

マルチキャスト VLAN 100 のサブ VLAN として VLAN 10～VLAN 15 を設定します。

<Switch> system-view

[Switch] multicast-vlan 100

[Switch-mvlan-100] subvlan 10 to 15

目次

このセクションのページは **6-x-x** です。

3 章 MLD スヌーピング 3-1
3.1 MLD スヌーピング設定コマンド 3-1
3.1.1 display ipv6 l2-multicast ip 3-1
3.1.2 display ipv6 l2-multicast ip forwarding 3-3
3.1.3 display ipv6 l2-multicast mac 3-4
3.1.4 display ipv6 l2-multicast mac forwarding 3-5
3.1.5 display mld-snooping 3-6
3.1.6 display mld-snooping group 3-9
3.1.7 display mld-snooping router-port 3-11
3.1.8 display mld-snooping static-group 3-12
3.1.9 display mld-snooping static-router-port 3-14
3.1.10 display mld-snooping statistics 3-15
3.1.11 dot1p-priority (MLD-snooping view) 3-17
3.1.12 dscp 3-18
3.1.13 enable (MLD-snooping view) 3-18
3.1.14 entry-limit (MLD-snooping view) 3-19
3.1.15 fast-leave (MLD-snooping view) 3-20
3.1.16 group-policy (MLD-snooping view) 3-21
3.1.17 host-aging-time (MLD-snooping view) 3-23
3.1.18 last-listener-query-interval (MLD-snooping view) 3-24
3.1.19 max-response-time (MLD-snooping view) 3-25
3.1.20 mld-snooping 3-26
3.1.21 mld-snooping done source-ip 3-27
3.1.22 mld-snooping dot1p-priority 3-28
3.1.23 mld-snooping drop-unknown 3-29
3.1.24 mld-snooping enable 3-30
3.1.25 mld-snooping fast-leave 3-31
3.1.26 mld-snooping general-query source-ip 3-32
3.1.27 mld-snooping group-limit 3-33
3.1.28 mld-snooping group-policy 3-34
3.1.29 mld-snooping host-aging-time 3-36
3.1.30 mld-snooping host-join 3-37
3.1.31 mld-snooping last-listener-query-interval 3-39
3.1.32 mld-snooping max-response-time 3-40
3.1.33 mld-snooping overflow-replace 3-41
3.1.34 mld-snooping querier 3-42

3.1.35 mld-snooping query-interval 3-43
3.1.36 mld-snooping report source-ip 3-44
3.1.37 mld-snooping router-aging-time 3-45
3.1.38 mld-snooping source-deny 3-46
3.1.39 mld-snooping special-query source-ip 3-47
3.1.40 mld-snooping static-group 3-49
3.1.41 mld-snooping static-router-port 3-50
3.1.42 mld-snooping version 3-51
3.1.43 overflow-replace (MLD-snooping view) 3-52
3.1.44 report-aggregation (MLD-snooping view) 3-53
3.1.45 reset mld-snooping group 3-53
3.1.46 reset mld-snooping router-port 3-54
3.1.47 reset mld-snooping statistics 3-55
3.1.48 router-aging-time (MLD-snooping view) 3-56
3.1.49 source-deny (MLD-snooping view) 3-57
3.1.50 version (MLD-snooping view) 3-58

3章 MLD スヌーピング

3.1 MLDスヌーピング設定コマンド

3.1.1 display ipv6 l2-multicast ip

Syntax

display ipv6 l2-multicast ip [**group** *ipv6-group-address* | **source** *ipv6-source-address*] * [**vlan** *vlan-id*] [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

group *ipv6-group-address*: IPv6 マルチキャストグループを IPv6 アドレスで指定します。IPv6 マルチキャストグループを指定しない場合、このコマンドはすべてのレイヤ 2 IPv6 マルチキャストグループの情報を表示します。

source *ipv6-source-address*: IPv6 アドレスで IPv6 マルチキャスト送信元を指定します。IPv6 マルチキャスト送信元を指定しない場合、このコマンドはすべての IPv6 マルチキャストソースのレイヤ 2 IPv6 マルチキャストグループの情報を表示します。

vlan *vlan-id*: VLAN ID で VLAN を指定します。設定範囲は 1～4094 です。VLAN を指定しない場合、このコマンドは、すべての VLAN のレイヤ 2 IPv6 マルチキャストグループの情報を表示します。

slot *slot-number*: メンバ ID によって IRF スタックメンバ装置を指定します。メンバ装置を指定しない場合、このコマンドはマスタ装置のレイヤ 2 IP マルチキャストグループの情報を表示します。

説明

display ipv6l2-multicast ip コマンドは、レイヤ 2 IPv6 マルチキャストグループの情報を表示します。

例

VLAN2 のレイヤ 2 IPv6 マルチキャストグループの情報を表示します。

<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)
```

表 3-1 コマンド出力

フィールド	説明
Total 1 entries	レイヤ2 IPv6マルチキャストグループの総数です。
VLAN 2: Total 1 entries	VLAN2のレイヤ2 IPv6マルチキャストグループの総数です。
(::, FF1E::101)	(S, G)エントリ。S位置の二重コロン(:)は、すべてのIPv6マルチキャストソースを意味します。
Attribute	エントリ属性です。 • **dynamic**ーエントリはダイナミックプロトコルによって作成されます。 • **static**ーエントリはスタティックプロトコルによって作成されます。 • **pim**ーエントリは IPv6 PIM によって作成されます。 • **kernel**ーエントリはカーネルから取得されます。 • **success**ー処理に成功しました。 • **fail**ー処理に失敗しました。
Host ports (1 in total)	メンバポートおよびメンバポートの総数です。
(S, SUC)	ポート属性です。 • **D**ーダイナミックポートです。 • **S**ースタティックポートです。 • **P**ーIPv6PIM ポートです。 • **K**ーカーネルから取得されたポートです。 • **R**ー(*、*)エントリから学習したポートです。 • **W**ー(*,G 様)エントリから学習したポートです。 • **SUC**ー処理に成功しました。 • **F**ー処理に失敗しました。

3.1.2 display ipv6 l2-multicast ip forwarding

Syntax

display ipv6 l2-multicast ip forwarding [**group** *ipv6-group-address* | **source** *ipv6-source-address*] * [**vlan** *vlan-id*] [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

group *ipv6-group-address*: IPv6 マルチキャストグループの IPv6 アドレスを指定します。IPv6 マルチキャストグループを指定しない場合、すべての IPv6 マルチキャストグループのレイヤ 2 IPv6 マルチキャストグループエントリを表示します。

source *ipv6-source-address*: IPv6 マルチキャストソースの IPv6 アドレスを指定します。IPv6 マルチキャストソースを指定しない場合、すべての IPv6 マルチキャストソースのレイヤ 2 IPv6 マルチキャストグループエントリを表示します。

vlan *vlan-id*: VLAN の ID を指定します。設定範囲は 1～4094 です。指定しない場合、すべての VLAN のレイヤ 2 IPv6 マルチキャストグループエントリを表示します。

slot *slot-number*: IRF スタックメンバ装置を指定します。*slot-number* は IRF スタックメンバ装置の ID を示します。指定しない場合、IRF スタックユニットのマスタ装置のレイヤ 2 IPv6 マルチキャストグループエントリを表示します。

説明

display ipv6 l2-multicast ip forwarding コマンドはレイヤ 2 IPv6 マルチキャストグループエントリを表示します。

例

VLAN 2 のレイヤ 2 IPv6 マルチキャストグループエントリを表示します。

<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
```

表 3-2 コマンド出力

フィールド	説明
Total 1 entries	レイヤ2 IPv6マルチキャストグループエントリの総数です。
VLAN 2: Total 1 IP entries	VLAN 2のレイヤ2 IPv6マルチキャストグループエントリの総数です。
(::, FF1E::101)	（S,G）エントリです。Sがダブルコロン（::）の場合、すべてのIPv6マルチキャストソースを示します。
Host ports (3 in total)	メンバポートとメンバポートの総数です。

3.1.3 display ipv6 l2-multicast mac

Syntax

display ipv6 l2-multicast mac [*mac-address*] [**vlan** *vlan-id*] [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

mac-address: IPv6 MAC アドレスで IPv6 MAC マルチキャストグループを指定します。指定しない場合、すべての IPv6 MAC マルチキャストグループの IPv6 MAC マルチキャストグループエントリを表示します。

vlan *vlan-id*: VLAN の ID を指定します。設定範囲は 1～4094 です。指定しない場合、すべての VLAN の IPv6 MAC マルチキャストグループエントリを表示します。

slot *slot-number*: IRF スタックメンバ装置を指定します。*slot-number* は IRF スタックメンバ装置の ID を示します。指定しない場合、IRF スタックユニットのマスタ装置の IPv6 MAC マルチキャストグループエントリを表示します。

説明

display ipv6 l2-multicast mac コマンドはレイヤ 2 IPv6 マルチキャスト MAC マルチキャストグループの情報を表示します。

例

VLAN2 のレイヤ 2 IPv6 マルチキャスト MAC マルチキャストグループの情報を表示します。

<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
```

表 3-3 コマンド出力

フィールド	説明
Total 1 entries	レイヤ2 IPv6MACマルチキャストグループの総数です。
VLAN 2: Total 1 entries	VLAN2内のレイヤ2 IPv6MACマルチキャストグループの総数です。
MAC group address	レイヤ2 IPv6MACマルチキャストグループのIPv6アドレスです。
Attribute	エントリ属性です。 • **success**–処理に成功しました。 • **fail**–処理に失敗しました。
Host ports (1 in total)	メンバポートおよびメンバポートの総数です。

3.1.4 display ipv6 l2-multicast mac forwarding

Syntax

display ipv6 l2-multicast mac forwarding [*mac-address*] [**vlan** *vlan-id*] [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

mac-address: IPv6 MACアドレスで IPv6 MACマルチキャストグループを指定します。指定しない場合、すべての IPv6 MACマルチキャストグループの IPv6 MACマルチキャストグループエントリを表示します。

vlan *vlan-id*: VLAN の ID を指定します。設定範囲は 1～4094 です。指定しない場合、すべての VLAN の IPv6 MAC マルチキャストグループエントリを表示します。

slot *slot-number*: IRF スタックメンバ装置を指定します。*slot-number* は IRF スタックメンバ装置の ID を示します。指定しない場合、IRF スタックユニットのマスタ装置の IPv6 MAC マルチキャストグループエントリを表示します。

説明

display ipv6 l2-multicast mac forwarding コマンドは IPv6 MAC マルチキャストグループエントリを表示します。

例

VLAN 2 の IPv6 MAC マルチキャストグループエントリを表示します。

<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
```

表 3-4 コマンド出力

フィールド	説明
Total 1 MAC entries	IPv6 MAC マルチキャストグループエントリの総数です。
VLAN 2: Total 1 MAC entries	VLAN 2 の IPv6 MAC マルチキャストグループエントリの総数です。
MAC group address	IPv6 MAC マルチキャストグループのアドレスです。
Host ports (3 in total)	メンバポートとメンバポートの総数です。

3.1.5 display mld-snooping

Syntax

display mld-snooping [**global** | **vlan** *vlan-id*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

global:グローバルの MLD snooping の状態を表示します。

vlan *vlan-id*: VLAN の ID を指定します。設定範囲は 1～4094 です。

説明

display mld-snooping コマンドは MLD snooping の状態を表示します。

パラメータを指定しない場合、グローバルとすべての VLAN の MLD snooping の状態を表示します。

例

グローバルとすべての VLAN の MLD snooping の状態を表示します。

<Switch> display mld-snooping

```
MLD snooping information: Global
 MLD snooping: Enabled
 Drop-unknown: Disabled
 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: Disabled
 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: Disabled
 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
```

表 3-5 コマンド出力

フィールド	説明
MLD snooping	MLD snoopingの状態です。 ● **Enabled**－有効です。 ● **Disabled**－無効です。
Drop-unknown	未知のIPv6マルチキャストデータの廃棄機能の状態です。 ● **Enabled**－有効です。 ● **Disabled**－無効です。
Version	MLD snoopingのバージョンです。
Host-aging-time	ダイナミックメンバポートのエージングタイマです。
Router-aging-time	ダイナミックルータポートのエージングタイマです。
Max-response-time	MLD general クエリの最大応答時間です。
Last-listener-query-interval	MLD multicast-address-specificの送信間隔です。
Report-aggregation	MLD report抑制機能の状態です。 ● **Enabled**－有効です。 ● **Disabled**－無効です。

フィールド	説明
Dot1p-priority	MLDメッセージの802.1pプライオリティです。プライオリティが設定されていない場合、ハイフン（--）が表示されます。
Querier	MLD snoopingのquerierの状態です。 ● **Enabled**ー有効です。 ● **Disabled**ー無効です。
Query-interval	MLD general クエリの送信間隔です。
General-query source IP	MLD general クエリの送信元IPアドレスです。
Special-query source IP	MLD multicast-address-specific クエリの送信元IPアドレスです。
Report source IP	MLD reportの送信元IPアドレスです。
Done source IP	MLD done messageの送信元IPアドレスです。
Host-tracking	host trackingの状態です。 ● **Enabled**ー有効です。 ● **Disabled**ー無効です。
Proxy Status of IGMP	MLD snooping proxyの状態です。 ● **Enabled**ー有効です。 ● **Disabled**ー無効です。

3.1.6 display mld-snooping group

Syntax

display mld-snooping group [*ipv6-group-address* | *ipv6-source-address*] * [**vlan** *vlan-id*] [**verbose**] [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ipv6-group-address: IPv6 マルチキャストグループの IPv6 アドレスを指定します。設定範囲は FFxy::/16（FFx0::/16、FFx1::/16、FFx2::/16、FF0y::を除きます）です。x と y は 16 進数の 0～F です。IPv6 マルチキャストグループを指定しない場合、すべての IPv6 マルチキャストグループのダイナミック MLD snooping 転送エントリを表示します。

ipv6-source-address: IPv6 マルチキャストソースの IPv6 アドレスを指定します。IPv6 マルチキャストソースを指定しない場合、すべての IPv6 マルチキャストソースのダイナミック MLD snooping 転送エントリを表示します。

vlan *vlan-id*: VLAN の ID を指定します。設定範囲は 1～4094 です。指定しない場合、すべての VLAN のダイナミック MLD snooping 転送エントリを表示します。

verbose: 詳細な情報を表示します。指定しない場合、概要情報を表示します。

slot *slot-number*: IRF スタックメンバ装置を指定します。*slot-number* は IRF スタックメンバ装置の ID を示します。指定しない場合、IRF スタックユニットのマスタ装置のダイナミック MLD snooping 転送エントリを表示します。

説明

display mld-snooping group コマンドはダイナミック MLD snooping 転送エントリを表示します。

例

VLAN 2 のダイナミック MLD snooping 転送エントリの詳細情報を表示します。

<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)
```

表 3-6 コマンド出力

フィールド	説明
Total 1 entries	ダイナミックMLD snooping転送エントリの総数です。
VLAN 2: Total 1 entries	VLAN 2のダイナミックMLD snooping転送エントリの総数です。
(::, FF1E::101)	（S,G）エントリです。Sがダブルコロン（::）の場合、すべてのIPv6マルチキャストソースを示します。
Attribute	エントリ属性です。 ● **global port**—エントリにグローバルポートがあります。 ● **local port**—エントリに指定された装置上のポートがあります。 ● **slot**—エントリにほかのメンバ装置上のポートがあります。メンバ装置上にない情報は表示されません。

フィールド	説明
FSM information	エントリの有限状態装置（Finite state machine）情報です。 ● **delete**—エントリの属性が削除されています。 ● **dummy**—エントリが新規で一時的なエントリです。 ● **no info**—エントリが存在しません。
Host slots (0 in total)	メンバIDとメンバ装置が指定されていないとき、指定されたメンバ装置、あるいはマスタ装置を除いたメンバ装置の総数です。
Host ports (1 in total)	メンバポートとメンバポートの総数です。
(00:03:23)	ダイナミックメンバポートの残りのエージング時間です。 アグリゲートインタフェースのようなグローバルポートでは常に表示されます。 グローバルポートでない場合、以下のときに表示されます。 ● 指定されたメンバ装置のポートです。 ● ポートがマスタ装置にあり、メンバ装置が指定されていません。

関連コマンド

reset mld-snooping group

3.1.7 display mld-snooping router-port

Syntax

display mld-snooping router-port [**vlan** *vlan-id*] [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

vlan *vlan-id*: VLAN の ID を指定します。設定範囲は 1～4094 です。

slot *slot-number*: IRF スタックメンバ装置を指定します。*slot-number* は IRF スタックメンバ装置の ID を示します。指定しない場合、IRF スタックユニットのマスタ装置のダイナミックルータポートの情報を表示します。

説明

display mld-snooping router-port コマンドはダイナミックルータポートの情報を表示します。

例

VLAN 2 のダイナミックルータポートの情報を表示します。

<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)
```

表 3-7 コマンド出力

フィールド	説明
VLAN 2	VLAN IDです。
Router slots (0 in total)	メンバIDとメンバ装置が指定されていないとき、指定されたメンバ装置、あるいはマスタ装置を除いたメンバ装置の総数です。
Router ports (2 in total)	ダイナミックルータポートと、ダイナミックルータポートの総数です。
(00:01:30)	ダイナミックルータポートの残りのエージング時間です。 グローバルポートでは常に表示されます。 グローバルポートでない場合、以下のときに表示されます。 • 指定されたメンバ装置のポートです。 • ポートがマスタ装置にあり、メンバ装置が指定されていません。

関連コマンド

reset mld-snooping router-port

3.1.8 display mld-snooping static-group

Syntax

display mld-snooping static-group [*ipv6-group-address* | *ipv6-source-address*] * [**vlan** *vlan-id*] [**verbose**] [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ipv6-group-address: IPv6 マルチキャストグループの IPv6 アドレスを指定します。設定範囲は FFxy::/16（FFx0::/16、FFx1::/16、FFx2::/16、FF0y::を除きます）です。x と y は 16 進数の 0～F です。IPv6 マルチキャストグループを指定しない場合、すべての IPv6 マルチキャストグループのスタティック MLD snooping 転送エントリを表示します。

ipv6-source-address: IPv6 マルチキャストソースの IPv6 アドレスを指定します。IPv6 マルチキャストソースを指定しない場合、すべての IPv6 マルチキャストソースのスタティック MLD snooping 転送エントリを表示します。

vlan *vlan-id*: VLAN の ID を指定します。設定範囲は 1～4094 です。指定しない場合、すべての VLAN のスタティック MLD snooping 転送エントリを表示します。

verbose: 詳細な情報を表示します。指定しない場合、概要情報を表示します。

slot *slot-number*: IRF スタックメンバ装置を指定します。*slot-number* は IRF スタックメンバ装置の ID を示します。指定しない場合、IRF スタックユニットのマスタ装置のスタティック MLD snooping 転送エントリを表示します。

説明

display mld-snooping static-group コマンドはスタティック MLD snooping 転送エントリを表示します。

例

VLAN 2 のスタティック MLD snooping 転送エントリの詳細情報を表示します。

<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
```

表 3-8 コマンド出力

フィールド	説明
Total 1 entries	スタティックMLD snooping転送エントリの総数です。

フィールド	説明
VLAN 2: Total 1 entries	VLAN 2のスタティックMLD snooping転送エントリの総数です。
(::, FF1E::101)	（S,G）エントリです。Sがダブルコロン（::）の場合、すべてのIPv6マルチキャストソースを示します。
Attribute	エントリ属性です。 ● **global port**—エントリにグローバルポートがあります。 ● **local port**—エントリに指定された装置上のポートがあります。 ● **slot**—エントリはほかのメンバ装置にありますが情報が表示されるメンバ装置にないポートがあります。
FSM information	エントリの有限状態装置（Finite state machine）情報です。 ● **delete**—エントリの属性が削除されています。 ● **dummy**—エントリが新規で一時的なエントリです。 ● **no info**—エントリが存在しません。
Host slots (0 in total)	メンバIDとメンバ装置が指定されていないとき、指定されたメンバ装置、あるいはマスタ装置を除いたメンバ装置の総数です。
Host ports (1 in total)	メンバポートとメンバポートの総数です。

3.1.9 display mld-snooping static-router-port

Syntax

display mld-snooping static-router-port [**vlan** *vlan-id*] [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

vlan *vlan-id*: VLAN の ID を指定します。設定範囲は 1～4094 です。

slot *slot-number*: IRF スタックメンバ装置を指定します。*slot-number* は IRF スタックメンバ装置の ID を示します。指定しない場合、IRF スタックユニットのマスタ装置のスタティックルータポートの情報を表示します。

説明

display mld-snooping static-router-port コマンドはスタティックルータポートの情報を表示します。

例

VLAN 2 のスタティックルータポートの情報を表示します。

<Switch> display mld-snooping static-router-port vlan 2

```
VLAN 2:
  Router ports (2 in total):
    GE1/0/1
    GE1/0/2
```

表 3-9 コマンド出力

フィールド	説明
VLAN 2	VLAN IDです。
Router slots (0 in total)	メンバIDとメンバ装置が指定されていないとき、指定されたメンバ装置、あるいはマスタ装置を除いたメンバ装置の総数です。
Router ports (2 in total)	スタティックルータポートとスタティックルータポートの総数です。

3.1.10 display mld-snooping statistics

Syntax

display mld-snooping statistics

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display mld-snooping statistics コマンドは MLD snooping によって学習した MLD メッセージと PIM hello メッセージの統計情報を表示します。

例

MLD snooping によって学習した MLD メッセージと IPv6 PIM hello メッセージの統計情報を表示します。

<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
```

表 3-10 コマンド出力

フィールド	説明
general queries	MLD general クエリの数です。
specific queries	MLD multicast-address-specific クエリの数です。
reports	MLD reportの数です。
dones	MLD doneメッセージの数です。
reports with right and wrong records	正確、不正確な記録のMLD reportの数です。
specific sg queries	MLD multicast-address-and-source-specific クエリの数です。
IPv6 PIM hello	IPv6 PIM helloメッセージの数です。
error MLD messages	エラーがあるMLDメッセージの数です。

関連コマンド

reset mld-snooping statistics

3.1.11 dot1p-priority (MLD-snooping view)

Syntax

dot1p-priority *priority*

undo dot1p-priority

デフォルト

MLD メッセージの 802.1p 優先度はデフォルトで設定されていません。装置によって作成される MLD メッセージの優先度は 0 です。MLD メッセージを転送する場合、優先度は変更しません。

View

MLD-snooping view

定義済みユーザロール

network-admin

パラメータ

priority: MLD メッセージの 802.1p 優先度を指定します。設定範囲は 0～7 です。値が高いほど優先度が高くなります。

説明

dot1p-priority コマンドはグローバルで MLD メッセージの 802.1p 優先度を設定します。

undo dot1p-priority コマンドはデフォルトに戻します。

このコマンドは **mld-snooping dot1p-priority** コマンドと同一機能ですが、適用範囲が異なります。

- MLD-snooping view の **dot1p-priority** コマンドはすべての VLAN に適用されます。
- **mld-snooping dot1p-priority** コマンドは現在の VLAN に適用されます。

VLAN では **mld-snooping dot1p-priority** コマンドは MLD-snooping view の **dot1p-priority** コマンドより優先されます。

例

グローバルで MLD メッセージの 802.1p 優先度を 3 に設定します。

<Switch> system-view

[Switch] mld-snooping

[Switch-mld-snooping] dot1p-priority 3

関連コマンド

mld-snooping dot1p-priority

3.1.12 dscp

Syntax

dscp *dscp-value*

undo dscp

デフォルト

48

View

MLD-snooping view

定義済みユーザロール

network-admin

パラメータ

dscp-value: DSCP 値を指定します。設定範囲は 0～63 です。

説明

dscp コマンドは、送信 MLD プロトコルパケットの DSCP 値を設定します。

undo dscp コマンドは、設定をデフォルトに戻します。

DSCP 値は、パケットの転送優先順位を決定するために、IPv6 パケットの Traffic Class フィールドで伝送されます。DSCP 値が大きいほど、優先順位が高くなります。

例

送信 MLD プロトコルパケットの DSCP 値を 63 に設定します。

<Switch> system-view

[Switch] mld-snooping

[Switch-mld-snooping] dscp 63

3.1.13 enable (MLD-snooping view)

Syntax

enable vlan *vlan-list*

undo enable vlan *vlan-list*

デフォルト

無効

View

MLD-snooping view

定義済みユーザロール

network-admin

パラメータ

vlan *vlan-list*: VLAN を指定します。半角スペースで区切り、10 まで設定することができます。VLAN を範囲で指定する形式は *start-vlan-id* **to** *end-vlan-id* です。設定範囲は 1～4094 です。指定しない場合、すべての VLAN に適用します。

説明

enable コマンドは VLAN の MLD snooping を有効にします。

undo enable コマンドは VLAN の MLD snooping を無効にします。

このコマンドを実行する前に、グローバルで MLD snooping 機能を有効にしてください。

このコマンドは **mld-snooping enable** コマンドと同一機能ですが、適用範囲が異なります。

- MLD-snooping view の **enable** コマンドは指定された VLAN に適用されます。
- **mld-snooping enable** コマンドは現在の VLAN に適用されます。

VLAN では **mld-snooping enable** コマンドは MLD-snooping view の **enable** コマンドの優先度は同一です。最後に行われた設定が適用されます。

例

グローバルで MLD snooping を有効にし、VLAN 2～VLAN 10 で MLD snooping を有効にします。

<Switch> system-view

[Switch] mld-snooping

[Switch-mld-snooping] enable vlan 2 to 10

関連コマンド

- **mld-snooping**
- **mld-snooping enable**

3.1.14 entry-limit (MLD-snooping view)

Syntax

entry-limit *limit*

undo entry-limit

デフォルト

4294967295

View

MLD-snooping view

定義済みユーザロール

network-admin

パラメータ

limit: MLD snooping 転送エントリのグローバルの最大数を指定します。設定範囲は 0～4294967295 です。

説明

entry-limit コマンドはダイナミックエントリとスタティックエントリを含む MLD snooping 転送エントリのグローバルの最大数を設定します。

undo entry-limit コマンドはデフォルトに戻します。

例

MLD snooping 転送エントリのグローバルの最大数を 512 に設定します。

<Switch> system-view

[Switch] mld-snooping

[Switch-mld-snooping] entry-limit 512

3.1.15 fast-leave (MLD-snooping view)

Syntax

fast-leave [**vlan** *vlan-list*]

undo fast-leave [**vlan** *vlan-list*]

デフォルト

無効

View

MLD-snooping view

定義済みユーザロール

network-admin

パラメータ

vlan *vlan-list*: VLAN を指定します。半角スペースで区切り、10 まで設定することができます。VLAN を範囲で指定する形式は *start-vlan-id* **to** *end-vlan-id* です。設定範囲は 1～4094 です。指定しない場合、すべての VLAN に適用します。

説明

fast-leave コマンドはグローバルに fast-leave 処理機能を有効にします。

undo fast-leave コマンドはグローバルに fast-leave 処理機能を無効にします。

ポートが done メッセージを受信したとき、装置はマルチキャストグループの転送エントリから迅速にポートを削除します。

このコマンドは **mld-snooping fast-leave** コマンドと同一機能ですが、適用範囲が異なります。

- MLD-snooping view の **fast-leave** コマンドはすべてのポートに適用されます。
- **mld-snooping fast-leave** コマンドは現在のポートに適用されます。

ポートでは **mld-snooping fast-leave** コマンドは MLD-snooping view の **fast-leave** コマンドより優先されます。

例

VLAN 2 でグローバルに MLD snooping の fast-leave 処理機能を有効にします。

<Switch> system-view

[Switch] mld-snooping

[Switch-mld-snooping] fast-leave vlan 2

関連コマンド

mld-snooping fast-leave

3.1.16 group-policy (MLD-snooping view)

Syntax

group-policy *ipv6-acl-number* [**vlan** *vlan-list*]

undo group-policy [**vlan** *vlan-list*]

デフォルト

IPv6 マルチキャストグループポリシーはグローバルで設定されていません。受信ホストはすべての IPv6 マルチキャストグループに加入することができます。

View

MLD-snooping view

定義済みユーザロール

network-admin

パラメータ

ipv6-acl-number: 標準 IPv6 ACL あるいは拡張 IPv6 ACL を指定します。設定範囲は 2000～3999 です。受信ホストは ACL が許可する IPv6 マルチキャストグループのみ加入することができます。ACL が存在しない、あるいは ACL に正常なルールがないとき、受信ホストは IPv6 マルチキャストグループに加入することができません。

vlan *vlan-list*: VLAN を指定します。半角スペースで区切り、10 まで設定することができます。VLAN を範囲で指定する形式は *start-vlan-id* **to** *end-vlan-id* です。設定範囲は 1～4094 です。指定しない場合、すべての VLAN に適用します。

説明

group-policy コマンドは受信ホストが加入する IPv6 マルチキャストグループを管理するため、グローバルで IPv6 マルチキャストグループポリシーを設定します。

undo group-policy コマンドはグローバルの IPv6 マルチキャストグループポリシーを削除します。

IPv6 マルチキャストグループポリシーはホストが加入する IPv6 マルチキャストグループを管理する MLD report をフィルタします。

スタティックメンバポートは MLD report を送信しないため、**group-policy** コマンドはスタティックメンバポートに適用されません。

MLD-snooping view のすべてのポートでグローバルにマルチキャストグループポリシーを設定することができます。また interface view のポートでマルチキャストグループポリシーを設定することができます。ポートでは **mld-snooping group-policy** コマンドは MLD-snooping view の **group-policy** コマンドより優先されます。

IPv6 ACL でルールを設定するとき、以下の制限とガイドラインに従ってください。

- 標準 IPv6 ACL の **source** *source-address source-prefix* パラメータは IPv6 マルチキャストグループアドレスを指定します。
- 拡張 IPv6 ACL の **source** *source-address source-prefix* パラメータは MLD report の IPv6 マルチキャスト送信元アドレスを指定します。**destination** *dest-address dest-prefix* パラメータは IPv6 マルチキャストグループアドレスを指定します。

  以下の MLD report に一致するように、マルチキャスト送信元アドレス **source** *source-address source-prefix* を 0::0 に設定します。

  - MLDv1 report
  - IPv6 マルチキャスト送信元アドレスを送信しない MLDv2 IS_EX、MLDv2 TO_EX の report
  - ほかのパラメータで、ACL ルールの **time-range** *time-range-name* パラメータ、**fragment** パラメータのみが適用されます。

異なる VLAN のポートに異なる ACL のルールを設定することができます。同一 VLAN で複数の ACL を設定した場合、最後に行った ACL のルールが適用されます。

例

VLAN 2 のホストがマルチキャストグループ FF03::101 のみ加入できるように VLAN 2 の IPv6 マルチキャストグループポリシーをグローバルに設定します。

<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

関連コマンド

mld-snooping group-policy

3.1.17 host-aging-time (MLD-snooping view)

Syntax

host-aging-time *seconds*

undo host-aging-time

デフォルト

260 秒

View

MLD-snooping view

定義済みユーザロール

network-admin

パラメータ

seconds: ダイナミックメンバポートのエージングタイマを設定します。設定範囲は 1～8097894 秒です。

説明

host-aging-time コマンドはグローバルでダイナミックメンバポートのエージングタイマを設定します。

undo host-aging-time コマンドはデフォルトに戻します。

このコマンドは **mld-snooping host-aging-time** コマンドと同一機能ですが、適用範囲が異なります。

- MLD-snooping view の **host-aging-time** コマンドはすべての VLAN に適用されます。

- **mld-snooping host-aging-time** コマンドは現在の VLAN に適用されます。

VLAN では **mld-snooping host-aging-time** コマンドは MLD-snooping view の **host-aging-time** コマンドより優先されます。

IPv6 マルチキャストグループメンバを間違って削除しないようにするため、ダイナミックメンバポートのエージングタイマを、以下の式で計算された値よりも大きい値に設定してください。

[MLD general クエリの間隔] ＋ [MLD general クエリの最大応答時間]

ダイナミックメンバポートのエージングタイマを以下の式で計算した値に設定することを推奨します。

[MLD general クエリの間隔] × 2 ＋ [MLD general クエリの最大応答時間]

例

グローバルでダイナミックメンバポートのエージングタイマを 300 秒に設定します。

<Switch> system-view

[Switch] mld-snooping

[Switch-mld-snooping] host-aging-time 300

関連コマンド

mld-snooping host-aging-time

3.1.18 last-listener-query-interval (MLD-snooping view)

Syntax

last-listener-query-interval *interval*

undo last-listener-query-interval

デフォルト

1 秒

View

MLD-snooping view

定義済みユーザロール

network-admin

パラメータ

interval: MLD last listener クエリ間隔を設定します。設定範囲は 1～25 秒です。

説明

last-listener-query-interval コマンドはグローバルで MLD last listener クエリ間隔を設定します。

undo last-listener-query-interval コマンドはデフォルトに戻します。

このコマンドは **mld-snooping last-listener-query-interval** コマンドと同一機能ですが、適用範囲が異なります。

- MLD-snooping view の **last-listener-query-interval** コマンドはすべての VLAN に適用されます。
- **mld-snooping last-listener-query-interval** コマンドは現在の VLAN に適用されます。

VLAN では **mld-snooping last-listener-query-interval** コマンドは MLD-snooping view の **last-listener-query-interval** コマンドより優先されます。

例

MLD last listener クエリ間隔を 3 秒に設定します。

<Switch> system-view

[Switch] mld-snooping

[Switch-mld-snooping] last-listener-query-interval 3

関連コマンド

mld-snooping last-listener-query-interval

3.1.19 max-response-time (MLD-snooping view)

Syntax

max-response-time *seconds*

undo max-response-time

デフォルト

10 秒

View

MLD-snooping view

定義済みユーザロール

network-admin

パラメータ

seconds: MLD general クエリの最大応答時間を設定します。設定範囲は 1～3174 秒です。

説明

max-response-time コマンドはグローバルで MLD general クエリの最大応答時間を設定します。

undo max-response-time コマンドはデフォルトに戻します。

このコマンドは **mld-snooping max-response-time** コマンドと同一機能ですが、適用範囲が異なります。

- MLD-snooping view の **max-response-time** コマンドはすべての VLAN に適用されます。
- **mld-snooping max-response-time** コマンドは現在の VLAN に適用されます。

VLAN では **mld-snooping max-response-time** コマンドは MLD-snooping view の **max-response-time** コマンドより優先されます。

IPv6 マルチキャストグループメンバを間違って削除しないようにするため、MLD general クエリの最大応答時間は MLD general クエリよりも小さいに設定してください。

例

グローバルで MLD general クエリの最大応答時間を 5 秒に設定します。

<Switch> system-view

[Switch] mld-snooping

[Switch-mld-snooping] max-response-time 5

関連コマンド

- **mld-snooping max-response-time**
- **mld-snooping query-interval**

3.1.20 mld-snooping

Syntax

mld-snooping

undo mld-snooping

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

mld-snooping コマンドはグローバルで MLD snooping を有効にし、MLD-snooping view に移行します。

undo mld-snooping コマンドはグローバルで MLD snooping を無効にします。

例

グローバルで MLD snooping を有効にし、MLD-snooping view に移行します。

<Switch> system-view

[Switch] mld-snooping

[Switch-mld-snooping]

関連コマンド

- **enable (MLD-snooping view)**
- **mld-snooping enable**

3.1.21 mld-snooping done source-ip

Syntax

mld-snooping done source-ip *ipv6-address*

undo mld-snooping done source-ip

デフォルト

MLD done メッセージの送信元 IPv6 アドレスは現在の VLAN インタフェースの IPv6 リンクローカルアドレスです。現在の VLAN インタフェースに IPv6 リンクローカルアドレスがない場合、送信元 IPv6 アドレスは FE80::02FF:FFFF:FE00:0001 です。

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

ipv6-address: MLD done メッセージの送信元 IPv6 アドレスを指定します。

説明

mld-snooping done source-ip コマンドは MLD done メッセージの送信元 IPv6 アドレスを設定します。

undo mld-snooping done source-ip コマンドはデフォルトに戻します。

このコマンドを実行する前に VLAN で MLD snooping を有効にしてください。

例

VLAN 2 で MLD snooping を有効にし、MLD done メッセージの送信元 IPv6 アドレスを FE80:0:0:1::1 に設定します。

<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

関連コマンド

- **enable (MLD-snooping view)**
- **mld-snooping enable**

3.1.22 mld-snooping dot1p-priority

Syntax

mld-snooping dot1p-priority *priority*

undo mld-snooping dot1p-priority

デフォルト

MLD メッセージの 802.1p 優先度はデフォルトで設定されていません。装置によって作成される MLD メッセージの優先度は 0 です。MLD メッセージを転送する場合、優先度は変更しません。

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

priority: MLD メッセージの 802.1p 優先度を指定します。設定範囲は 0～7 です。値が高いほど優先度が高くなります。

説明

mld-snooping dot1p-priority コマンドは VLAN の MLD メッセージの 802.1p 優先度を設定します。

undo mld-snooping dot1p-priority コマンドはデフォルトに戻します。

このコマンドを実行する前に VLAN で MLD snooping を有効にしてください。

このコマンドは MLD-snooping view の **dot1p-priority** コマンドと同一機能ですが、適用範囲が異なります。

- MLD-snooping view の **dot1p-priority** コマンドはすべての VLAN に適用されます。
- **mld-snooping dot1p-priority** コマンドは現在の VLAN に適用されます。

VLAN では **mld-snooping dot1p-priority** コマンドは MLD-snooping view の **dot1p-priority** コマンドより優先されます。

例

VLAN 2 で MLD snooping を有効にし、MLD メッセージの 802.1p 優先度を 3 に設定します。

<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

関連コマンド

- **dot1p-priority (MLD-snooping view)**
- **enable (MLD-snooping view)**
- **mld-snooping enable**

3.1.23 mld-snooping drop-unknown

Syntax

mld-snooping drop-unknown

undo mld-snooping drop-unknown

デフォルト

VLAN の未知の IPv6 マルチキャストデータの廃棄機能は無効です。未知の IPv6 マルチキャストデータは VLAN にフラッディングされます。

View

VLAN view

定義済みユーザロール

network-admin

説明

mld-snooping drop-unknown コマンドは VLAN の未知の IPv6 マルチキャストデータの廃棄機能を有効にします。

undo mld-snooping drop-unknown コマンドは VLAN の未知の IPv6 マルチキャストデータの廃棄機能を無効にします。

このコマンドを実行する前に VLAN で MLD snooping 機能を有効にしてください。

例

MLD snooping を有効にし、VLAN 2 の未知の IPv6 マルチキャストデータの廃棄機能を有効にします。

<Switch> system-view

[Switch] mld-snooping

[Switch-mld-snooping] quit

[Switch] vlan 2

[Switch-vlan2] mld-snooping enable

[Switch-vlan2] mld-snooping drop-unknown

関連コマンド

- **enable (MLD-snooping view)**
- **mld-snooping enable**

3.1.24 mld-snooping enable

Syntax

mld-snooping enable

undo mld-snooping enable

デフォルト

無効

View

VLAN view

定義済みユーザロール

network-admin

説明

mld-snooping enable コマンドは VLAN の MLD snooping を有効にします。

undo mld-snooping enable コマンドは VLAN の MLD snooping を無効にします。

このコマンドを実行する前にグローバルで MLD snooping 機能を有効にしてください。

このコマンドは **enable** コマンドと同一機能ですが、適用範囲が異なります。

- MLD-snooping view の **enable** コマンドは指定された VLAN に適用されます。
- **mld-snooping enable** コマンドは現在の VLAN に適用されます。

VLAN では **mld-snooping enable** コマンドは MLD-snooping view の **enable** コマンドの優先度は同一です。最後に行われた設定が適用されます。

例

グローバルと VLAN 2 の MLD snooping を有効にします。

<Switch> system-view

[Switch] mld-snooping

[Switch-mld-snooping] quit

[Switch] vlan 2

[Switch-vlan2] mld-snooping enable

関連コマンド

- **enable (MLD-snooping view)**
- **mld-snooping**

3.1.25 mld-snooping fast-leave

Syntax

mld-snooping fast-leave [**vlan** *vlan-list*]

undo mld-snooping fast-leave [**vlan** *vlan-list*]

デフォルト

無効

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

vlan *vlan-list*: VLAN を指定します。半角スペースで区切り、10 まで設定することができます。VLAN を範囲で指定する形式は *start-vlan-id* **to** *end-vlan-id* です。設定範囲は 1～4094 です。指定しない場合、すべての VLAN に適用します。

説明

mld-snooping fast-leave コマンドはポートで fast-leave 処理機能を有効にします。

undo mld-snooping fast-leave コマンドはポートで fast-leave 処理機能を無効にします。

この機能は、ポートが done メッセージを受信したとき、装置がマルチキャストグループの転送エントリから迅速にポートを削除します。

このコマンドは MLD-snooping view の **fast-leave** コマンドと同一機能ですが、適用範囲が異なります。

- MLD-snooping view の **fast-leave** コマンドはすべてのポートに適用されます。
- **mld-snooping fast-leave** コマンドは現在のポートに適用されます。

ポートでは **mld-snooping fast-leave** コマンドは MLD-snooping view の **fast-leave** コマンドより優先されます。

例

GigabitEthernet 1/0/1 の VLAN 2 で fast-leave 処理機能を有効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] mld-snooping fast-leave vlan 2

関連コマンド

fast-leave (MLD-snooping view)

3.1.26 mld-snooping general-query source-ip

Syntax

mld-snooping general-query source-ip *ipv6-address*

undo mld-snooping general-query source-ip

デフォルト

MLD general クエリの送信元 IPv6 アドレスは現在の VLAN インタフェースの IPv6 リンクローカルアドレスです。現在の VLAN インタフェースに IPv6 リンクローカルアドレスがない場合、送信元 IPv6 アドレスは FE80::02FF:FFFF:FE00:0001 です。

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

ipv6-address: MLD general クエリの IPv6 アドレスを指定します。

説明

mld-snooping general-query source-ip コマンドは MLD general クエリの送信元 IPv6 アドレスを設定します。

undo mld-snooping general-query source-ip コマンドはデフォルトに戻します。

このコマンドを実行する前に VLAN で MLD snooping を有効にしてください。

例

VLAN 2 で MLD snooping を有効にし、MLD general クエリの送信元 IPv6 アドレス FE80:0:0:1::1 を設定します。

<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

関連コマンド

- **enable (MLD-snooping view)**
- **mld-snooping enable**

3.1.27 mld-snooping group-limit

Syntax

mld-snooping group-limit *limit* [**vlan** *vlan-list*]

undo mld-snooping group-limit [**vlan** *vlan-list*]

デフォルト

4294967295

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

limit: ポートが加入できるマルチキャストグループの最大数を設定します。設定範囲は 0 ～4294967295 です。

vlan *vlan-list*: VLAN を指定します。半角スペースで区切り、10 まで設定することができます。VLAN を範囲で指定する形式は *start-vlan-id* **to** *end-vlan-id* です。設定範囲は 1～4094 です。指定しない場合、すべての VLAN に適用します。

説明

mld-snooping group-limit コマンドはポートが加入できる IPv6 マルチキャストグループの最大数を設定します。

undo mld-snooping group-limit コマンドはデフォルトに戻します。

このコマンドはポートがダイナミックに加入する IPv6 マルチキャストグループでのみ適用します。

例

VLAN 2 の GigabitEthernet 1/0/1 が加入できる IPv6 マルチキャストグループの最大数を 10 に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] mld-snooping group-limit 10 vlan 2

3.1.28 mld-snooping group-policy

Syntax

mld-snooping group-policy *ipv6-acl-number* [**vlan** *vlan-list*]

undo mld-snooping group-policy [**vlan** *vlan-list*]

デフォルト

ポートで IPv6 マルチキャストグループポリシーは設定されていません。ポートに接続されたホストはすべての IPv6 マルチキャストグループに加入することができます。

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

ipv6-acl-number: 標準 IPv6 ACL あるいは拡張 IPv6 ACL を指定します。設定範囲は 2000～3999 です。受信ホストは ACL が許可する IPv6 マルチキャストグループのみ加入することができます。ACL が存在しない、あるいは ACL に正常なルールがないとき、受信ホストは IPv6 マルチキャストグループに加入することができません。

vlan *vlan-list*: VLAN を指定します。半角スペースで区切り、10 まで設定することができます。VLAN を範囲で指定する形式は *start-vlan-id* **to** *end-vlan-id* です。設定範囲は 1～4094 です。指定しない場合、すべての VLAN に適用します。

説明

mld-snooping group-policy コマンドは受信ホストが加入する IPv6 マルチキャストグループを管理するため、ポートで IPv6 マルチキャストグループポリシーを設定します。

undo mld-snooping group-policy コマンドはポートの IPv6 マルチキャストグループポリシーを削除します。

IPv6 マルチキャストグループポリシーはホストが加入する IPv6 マルチキャストグループを管理する MLD report をフィルタします。

スタティックメンバポートは MLD report を送信しないため、**group-policy** コマンドはスタティックメンバポートに適用されません。

MLD-snooping view のすべてのポートでグローバルにマルチキャストグループポリシーを設定することができます。また interface view のポートでマルチキャストグループポリシーを設定することができます。ポートでは **mld-snooping group-policy** コマンドは MLD-snooping view の **group-policy** コマンドより優先されます。

IPv6 ACL でルールを設定するとき、以下の制限とガイドラインに従ってください。

- 標準 IPv6 ACL の **source** *source-address source-prefix* パラメータは IPv6 マルチキャストグループアドレスを指定します。
- 拡張 IPv6 ACL の **source** *source-address source-prefix* パラメータは MLD report の IPv6 マルチキャスト送信元アドレスを指定します。**destination** *dest-address dest-prefix* パラメータは IPv6 マルチキャストグループアドレスを指定します。

  以下の MLD report に一致するように、マルチキャスト送信元アドレス **source** *source-address source-prefix* を 0::0 に設定します。

  - MLDv1 report
  - IPv6 マルチキャスト送信元アドレスを送信しない MLDv2 IS_EX、MLDv2 TO_EX の report
- ほかのパラメータで、ACL ルールの **time-range** *time-range-name* パラメータ、**fragment** パラメータのみが適用されます。

異なる VLAN のポートに異なる ACL のルールを設定することができます。同一 VLAN で複数の ACL を設定した場合、最後に行った ACL のルールが適用されます。

例

ポートに接続されたホストがマルチキャストグループ FF03::101 のみ加入できるように VLAN 2 の GigabitEthernet 1/0/1 で IPv6 マルチキャストグループポリシーを設定します。

<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

関連コマンド

group-policy (MLD-snooping view)

3.1.29 mld-snooping host-aging-time

Syntax

mld-snooping host-aging-time *seconds*

undo mld-snooping host-aging-time

デフォルト

260 秒

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

seconds: VLAN のダイナミックメンバポートのエージングタイマを設定します。設定範囲は 1～8097894 秒です。

説明

mld-snooping host-aging-time コマンドは VLAN のダイナミックメンバポートのエージングタイマを設定します。

undo mld-snooping host-aging-time コマンドはデフォルトに戻します。

このコマンドを実行する前に VLAN で MLD snooping 機能を有効にしてください。

このコマンドは **host-aging-time** コマンドと同一機能ですが、適用範囲が異なります。

- MLD-snooping view の **host-aging-time** コマンドはすべての VLAN に適用されます。
- **mld-snooping host-aging-time** コマンドは現在の VLAN に適用されます。

VLAN では **mld-snooping host-aging-time** コマンドは MLD-snooping view の **host-aging-time** コマンドより優先されます。

IPv6 マルチキャストグループメンバを間違って削除しないようにするため、ダイナミックメンバポートのエージングタイマを、以下の式で計算された値よりも大きい値に設定してください。

[MLD general クエリの間隔] ＋ [MLD general クエリの最大応答時間]

ダイナミックメンバポートのエージングタイマを以下の式で計算した値に設定することを推奨します。

[MLD general クエリの間隔] × 2 ＋ [MLD general クエリの最大応答時間]

例

VLAN 2 の MLD snooping を有効にし、VLAN のダイナミックメンバポートのエージングタイマを 300 秒に設定します。

```
<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
```

関連コマンド

- **enable (MLD-snooping view)**
- **host-aging-time (MLD-snooping view)**
- **mld-snooping enable**

3.1.30 mld-snooping host-join

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** }

デフォルト

設定なし

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

ipv6-group-address: IPv6 マルチキャストグループの IPv6 アドレスを指定します。0::0 あるいは設定範囲を指定します。設定範囲は FFxy::/16（FFx0::/16、FFx1::/16、FFx2::/16、FF0y::を除きます）です。x と y は 16 進数の 0～F です。

source-ip *ipv6-source-address*: IPv6 マルチキャストソースの IPv6 アドレスを指定します。IPv6 マルチキャストソースを指定した場合、ポートを IPv6 マルチキャストソースとグループのシミュレーティッドメンバホストとして設定します。IPv6 マルチキャストソースを指定しない場合、ポートを IPv6 マルチキャストグループのシミュレーティッドメンバホストとして設定します。このパラメータは MLDv2 snooping が動作する装置で有効です。

vlan *vlan-id*: VLAN の ID を指定します。設定範囲は 1～4094 です。

all: すべての IPv6 マルチキャストグループを指定します。

説明

mld-snooping host-join コマンドは IPv6 マルチキャストグループのポートをマルチキャストグループのシミュレーティッドメンバホストとして設定します。

undo mld-snooping host-join コマンドはデフォルトに戻します。

スタティックメンバポートと異なり、シミュレーティッドメンバホストとして設定されたポートはダイナミックメンバポートのようにエージアウトします。MLD version と、シミュレーティッドメンバホストが動作する MLD snooping のバージョンは同一にしてください。

例

VLAN2 の IPv6 マルチキャストソースとマルチキャストグループの(*, FF3E::101)のシミュレーティッドメンバホストを GigabitEthernet 1/0/1 に設定します。

<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

3.1.31 mld-snooping last-listener-query-interval

Syntax

mld-snooping last-listener-query-interval *interval*

undo mld-snooping last-listener-query-interval

デフォルト

1 秒

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

interval: MLD last listener クエリ間隔を設定します。設定範囲は 1～25 秒です。

説明

mld-snooping last-listener-query-interval コマンドは VLAN の MLD last listener クエリ間隔を設定します。

undo mld-snooping last-listener-query-interval コマンドはデフォルトに戻します。

このコマンドを実行する前に VLAN で MLD snooping 機能を有効にしてください。

このコマンドは **last-listener-query-interval** コマンドと同一機能ですが、適用範囲が異なります。

- MLD-snooping view の **last-listener-query-interval** コマンドはすべての VLAN に適用されます。
- **mld-snooping last-listener-query-interval** コマンドは現在の VLAN に適用されます。

VLAN では **mld-snooping last-listener-query-interval** コマンドは MLD-snooping view の **last-listener-query-interval** コマンドより優先されます。

例

VLAN 2 の MLD snooping を有効にし、VLAN 2 の MLD last listener クエリ間隔を 3 秒に設定します。

<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
```

関連コマンド

- **enable (MLD-snooping view)**
- **last-listener-query-interval (MLD-snooping view)**
- **mld-snooping enable**

3.1.32 mld-snooping max-response-time

Syntax

mld-snooping max-response-time *seconds*

undo mld-snooping max-response-time

デフォルト

10 秒

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

seconds: MLD general クエリの最大応答時間を設定します。設定範囲は 1～3174 秒です。

説明

mld-snooping max-response-time コマンドは VLAN の MLD general クエリの最大応答時間を設定します。

undo mld-snooping max-response-time コマンドはデフォルトに戻します。

このコマンドを実行する前に VLAN で MLD snooping 機能を有効にしてください。

このコマンドは **max-response-time** コマンドと同一機能ですが、適用範囲が異なります。

- MLD-snooping view の **max-response-time** コマンドはすべての VLAN に適用されます。
- **mld-snooping max-response-time** コマンドは現在の VLAN に適用されます。

VLAN では **mld-snooping max-response-time** コマンドは MLD-snooping view の **max-response-time** コマンドより優先されます。

IPv6 マルチキャストグループメンバを間違って削除しないようにするため、MLD general クエリの最大応答時間は MLD general クエリよりも小さいに設定してください。

例

VLAN 2 の MLD snooping を有効にし、VLAN 2 の MLD general クエリの最大応答時間を 5 秒に設定します。

```
<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
```

関連コマンド

- **enable (MLD-snooping view)**
- **max-response-time (MLD-snooping view)**
- **mld-snooping enable**
- **mld-snooping query-interval**

3.1.33 mld-snooping overflow-replace

Syntax

mld-snooping overflow-replace [**vlan** *vlan-list*]

undo mld-snooping overflow-replace [**vlan** *vlan-list*]

デフォルト

無効

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

vlan *vlan-list*: VLAN を指定します。半角スペースで区切り、10 まで設定することができます。VLAN を範囲で指定する形式は *start-vlan-id* **to** *end-vlan-id* です。設定範囲は 1～4094 です。指定しない場合、すべての VLAN に適用します。

説明

mld-snooping overflow-replace コマンドはポートで IPv6 マルチキャストグループ置き換え機能を有効にします。

undo mld-snooping overflow-replace コマンドはポートで IPv6 マルチキャストグループ置き換え機能を無効にします。

このコマンドはポートがダイナミックに加入する IPv6 マルチキャストグループでのみ適用します。

このコマンドは **overflow-replace** コマンドと同一機能ですが、適用範囲が異なります。

- MLD-snooping view の **overflow-replace** コマンドはすべてのポートに適用されます。
- **mld-snooping overflow-replace** コマンドは現在のポートに適用されます。

ポートでは **mld-snooping overflow-replace** コマンドは MLD-snooping view の **overflow-replace** コマンドより優先されます。

例

GigabitEthernet 1/0/1 の VLAN2 で IPv6 マルチキャストグループ置き換え機能を有効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] mld-snooping overflow-replace vlan 2

関連コマンド

overflow-replace (MLD-snooping view)

3.1.34 mld-snooping querier

Syntax

mld-snooping querier

undo mld-snooping querier

デフォルト

無効

View

VLAN view

定義済みユーザロール

network-admin

説明

mld-snooping querier コマンドは MLD snooping クエリアを有効にします。

undo mld-snooping querier コマンドは MLD snooping クエリアを無効にします。

このコマンドを実行する前に、VLAN の MLD snooping 機能を有効にしてください。

このコマンドは、IPv6 マルチキャスト VLAN からサブ VLAN を削除した後、サブ VLAN に適用されます。

例

VLAN 2 の MLD snooping を有効にし、MLD snooping クエリアを有効にします。

<Switch> system-view

[Switch] mld-snooping

[Switch-mld-snooping] quit

[Switch] vlan 2

[Switch-vlan2] mld-snooping enable

[Switch-vlan2] mld-snooping querier

関連コマンド

- **enable (MLD-snooping view)**
- **mld-snooping enable**
- **subvlan (IPv6 multicast-VLAN view)**

3.1.35 mld-snooping query-interval

Syntax

mld-snooping query-interval *interval*

undo mld-snooping query-interval

デフォルト

125 秒

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

interval: MLD general クエリの送信間隔を設定します。設定範囲は 2～31744 秒です。

説明

mld-snooping query-interval コマンドは VLAN の MLD general クエリ送信間隔を設定します。

undo mld-snooping query-interval コマンドはデフォルトに戻します。

このコマンドを実行する前に、VLAN の MLD snooping 機能を有効にしてください。

間違って IPv6 マルチキャストグループメンバを削除しないように、MLD general クエリの最大応答時間より MLD general クエリの送信間隔を大きくしてください。

例

VLAN 2 の MLD snooping を有効にし、MLD general クエリ送信間隔を 20 秒に設定します。

<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

関連コマンド

- **enable (MLD-snooping view)**
- **max-response-time**
- **mld-snooping enable**
- **mld-snooping max-response-time**
- **mld-snooping querier**

3.1.36 mld-snooping report source-ip

Syntax

mld-snooping report source-ip *ipv6-address*

undo mld-snooping report source-ip

デフォルト

MLD report の送信元 IPv6 アドレスは、現在の VLAN インタフェースの IPv6 リンクローカルアドレスです。現在の VLAN インタフェースに IPv6 リンクローカルアドレスが設定されていない場合、送信元 IP アドレスは FE80::02FF:FFFF:FE00:0001 です。

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

ipv6-address: MLD report の送信元 IPv6 アドレスを指定します。

説明

mld-snooping report source-ip コマンドは MLD report の送信元 IPv6 アドレスを設定します。

undo mld-snooping report source-ip コマンドはデフォルトに戻します。

このコマンドを実行する前に、VLAN の MLD snooping 機能を有効にしてください。

例

VLAN 2 で MLD snooping を有効にし、MLD report の送信元 IPv6 アドレスを FE80:0:0:1::1 に設定します。

<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

関連コマンド

- **enable (MLD-snooping view)**
- **mld-snooping enable**

3.1.37 mld-snooping router-aging-time

Syntax

mld-snooping router-aging-time *seconds*

undo mld-snooping router-aging-time

デフォルト

260 秒

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

seconds: VLAN のダイナミックルータポートのエージングタイマを設定します。設定範囲は 1～8097894 秒です。

説明

mld-snooping router-aging-time コマンドは VLAN のダイナミックルータポートのエージングタイマを設定します。

undo mld-snooping router-aging-time コマンドはデフォルトに戻します。

このコマンドを実行する前に、VLAN の MLD snooping 機能を有効にしてください。

このコマンドは **router-aging-time** コマンドと同一機能ですが、適用範囲が異なります。

- MLD-snooping view の **router-aging-time** コマンドはすべての VLAN に適用されます。
- **mld-snooping router-aging-time** コマンドは現在の VLAN に適用されます。

VLAN では **mld-snooping router-aging-time** コマンドは MLD-snooping view の **router-aging-time** コマンドより優先されます。

例

VLAN 2 の MLD snooping を有効にし、ダイナミックルータポートのエージングタイマを 100 秒に設定します。

```
<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
```

関連コマンド

- **enable (MLD-snooping view)**
- **mld-snooping enable**
- **router-aging-time (MLD-snooping view)**

3.1.38 mld-snooping source-deny

Syntax

mld-snooping source-deny

undo mld-snooping source-deny

デフォルト

無効

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

説明

mld-snooping source-deny コマンドはすべての受信した IPv6 マルチキャストデータパケットを廃棄するため、ポートで IPv6 マルチキャストソースポートフィルタを有効にします。

undo mld-snooping source-deny コマンドはポートで IPv6 マルチキャストソースポートフィルタを無効にします。

このコマンドは **source-deny** コマンドと同一機能ですが、適用範囲が異なります。

- MLD-snooping view の **source-deny** マンドはすべてのポートに適用されます。
- **mld-snooping source-deny** コマンドは現在のポートに適用されます。

ポートでは **mld-snooping source-deny** コマンドは MLD-snooping view の **source-deny** コマンドの優先度は同一です。最後に行われた設定が適用されます。

例

GigabitEthernet 1/0/1 で IPv6 マルチキャストソースポートフィルタを有効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] mld-snooping source-deny

関連コマンド

source-deny (MLD-snooping view)

3.1.39 mld-snooping special-query source-ip

Syntax

mld-snooping special-query source-ip *ipv6-address*

undo mld-snooping special-query source-ip

デフォルト

VLAN で MLD group-specific クエリの送信元 IPv6 アドレスは以下のいずれかとなります。

- MLD snooping クエリアが MLD general クエリを受信したとき、MLD multicast-address-specific クエリの送信元 IPv6 アドレスは MLD general クエリの IPv6 アドレスです。
- MLD snooping クエリアが MLD general クエリを受信しないとき、送信元 IPv6 アドレスは現在の VLAN インタフェースの IPv6 リンクローカルアドレスです。
- 現在の VLAN インタフェースに IPv6 リンクローカルアドレスが設定されていない場合、送信元 IPv6 アドレスは FE80::02FF:FFFF:FE00:0001 です。

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

ipv6-address: MLD multicast-address-specific クエリの送信元 IPv6 アドレスを指定します。

説明

mld-snooping special-query source-ip コマンドは MLD multicast-address-specific クエリの送信元 IPv6 アドレスを設定します。

undo mld-snooping special-query source-ip コマンドはデフォルトに戻します。

このコマンドを実行する前に、VLAN の MLD snooping 機能を有効にしてください。

例

VLAN 2 の MLD snooping を有効にし、MLD multicast-address-specific クエリの送信元 IPv6 アドレス FE80:0:0:1::1 を設定します。

<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

関連コマンド

- **enable (MLD-snooping view)**
- **mld-snooping enable**

3.1.40 mld-snooping static-group

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** }

デフォルト

設定なし

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

ipv6-group-address: IPv6 マルチキャストグループの IPv6 アドレスを指定します。0::0 あるいは設定範囲を指定します。設定範囲は FFxy::/16（FFx0::/16、FFx1::/16、FFx2::/16、FF0y::を除きます）です。x と y は 16 進数の 0～F です。

source-ip *ipv6-source-address*: IPv6 マルチキャストソースの IPv6 アドレスを指定します。IPv6 マルチキャストソースを指定した場合、ポートを IPv6 マルチキャストソースとグループのスタティックメンバポートとして設定します。IPv6 マルチキャストソースを指定しない場合、ポートを IPv6 マルチキャストグループのスタティックメンバポートとして設定します。このパラメータは MLDv2 snooping が動作する装置で有効です。

vlan *vlan-id*: VLAN の ID を指定します。設定範囲は 1～4094 です。

all: すべての VLAN を指定します。

説明

mld-snooping static-group コマンドは指定された IPv6 マルチキャストグループあるいは指定された IPv6 マルチキャストソースとグループのスタティックメンバポートを設定します。

undo mld-snooping static-group コマンドはスタティックメンバポートを削除します。

例

VLAN2 の IPv6 マルチキャストソースとマルチキャストグループの(*, FF3E::101)のスタティックメンバポートを GigabitEthernet 1/0/1 に設定します。

<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

3.1.41 mld-snooping static-router-port

Syntax

mld-snooping static-router-port vlan *vlan-id*

undo mld-snooping static-router-port { **all** | **vlan** *vlan-id* }

デフォルト

設定なし

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

all: すべての VLAN を指定します。

vlan *vlan-id*: VLAN の ID を指定します。設定範囲は 1～4094 です。

説明

mld-snooping static-router-port コマンドはスタティックルータポートを設定します。

undo mld-snooping static-router-port コマンドはスタティックルータポートを削除します。

例

VLAN 2 の GigabitEthernet 1/0/1 をスタティックルータポートに設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] mld-snooping static-router-port vlan 2

3.1.42 mld-snooping version

Syntax

mld-snooping version *version-number*

undo mld-snooping version

デフォルト

1

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

version-number: MLD snooping のバージョンを指定します。1 あるいは 2 です。

説明

mld-snooping version コマンドは VLAN の MLD snooping のバージョンを指定します。

undo mld-snooping version コマンドはデフォルトに戻します。

このコマンドを実行する前に、VLAN の MLD snooping 機能を有効にしてください。

このコマンドは **version** コマンドと同一機能ですが、適用範囲が異なります。

- MLD-snooping view の **version** コマンドは指定された VLAN に適用されます。
- **mld-snooping version** コマンドは現在の VLAN に適用されます。

VLAN では **mld-snooping version** コマンドは MLD-snooping view の **version** コマンドの優先度は同一です。最後に行われた設定が適用されます。

例

VLAN 2 の MLD snooping を有効にし、MLD snooping のバージョンを 2 に指定します。

<Switch> system-view

[Switch] mld-snooping

[Switch-mld-snooping] quit

[Switch] vlan 2

[Switch-vlan2] mld-snooping enable

[Switch-vlan2] mld-snooping version 2

関連コマンド

- **enable (MLD-snooping view)**
- **mld-snooping enable**

- **version (MLD-snooping view)**

3.1.43 overflow-replace (MLD-snooping view)

Syntax

overflow-replace [**vlan** *vlan-list*]

undo overflow-replace [**vlan** *vlan-list*]

デフォルト

無効

View

MLD-snooping view

定義済みユーザロール

network-admin

パラメータ

vlan *vlan-list*: VLAN を指定します。半角スペースで区切り、10 まで設定することができます。VLAN を範囲で指定する形式は *start-vlan-id* **to** *end-vlan-id* です。設定範囲は 1～4094 です。指定しない場合、すべての VLAN に適用します。

説明

overflow-replace コマンドはグローバルで IPv6 マルチキャストグループ置き換え機能を有効にします。

undo overflow-replace コマンドはグローバルで IPv6 マルチキャストグループ置き換え機能を無効にします。

このコマンドはポートがダイナミックに加入する IPv6 マルチキャストグループでのみ適用します。

このコマンドは **mld-snooping overflow-replace** コマンドと同一機能ですが、適用範囲が異なります。

- MLD-snooping view の **overflow-replace** コマンドはすべてのポートに適用されます。
- **mld-snooping overflow-replace** コマンドは現在のポートに適用されます。

ポートでは **mld-snooping overflow-replace** コマンドは MLD-snooping view の **overflow-replace** コマンドより優先されます。

例

VLAN2 で IPv6 マルチキャストグループ置き換え機能を有効にします。

<Switch> system-view

[Switch] mld-snooping

[Switch-mld-snooping] overflow-replace vlan 2

関連コマンド

mld-snooping overflow-replace

3.1.44 report-aggregation (MLD-snooping view)

Syntax

report-aggregation

undo report-aggregation

デフォルト

有効

View

MLD-snooping view

定義済みユーザロール

network-admin

説明

report-aggregation コマンドは MLD report 抑制機能を有効にします。

undo report-aggregation コマンドは MLD report 抑制機能を無効にします。

例

MLD report 抑制機能を無効にします。

<Switch> system-view

[Switch] mld-snooping

[Switch-mld-snooping] undo report-aggregation

3.1.45 reset mld-snooping group

Syntax

reset mld-snooping group { *ipv6-group-address* [*ipv6-source-address*] | **all** } [**vlan** *vlan-id*]

View

User view

定義済みユーザロール

network-admin

パラメータ

ipv6-group-address: IPv6 マルチキャストグループの IPv6 アドレスを指定します。設定範囲は FFxy::/16（FFx0::/16、FFx1::/16、FFx2::/16、FF0y::を除きます）です。x と y は 16 進数の 0～F です。

ipv6-source-address: IPv6 マルチキャストソースの IPv6 アドレスを指定します。指定しない場合、すべての IPv6 マルチキャストソースのダイナミック MLD snooping 転送エントリを削除します。

all: すべての IPv6 マルチキャストグループを指定します。

vlan *vlan-id*: VLAN の ID を指定します。設定範囲は 1～4094 です。指定しない場合、すべての VLAN のダイナミック MLD snooping 転送エントリを削除します。

説明

reset mld-snooping group コマンドは IPv6 マルチキャストグループのダイナミック MLD snooping 転送エントリを削除します。

例

すべての IPv6 マルチキャストグループのダイナミック MLD snooping 転送エントリを削除します。

<Switch> reset mld-snooping group all

関連コマンド

display mld-snooping group

3.1.46 reset mld-snooping router-port

Syntax

reset mld-snooping router-port { **all** | **vlan** *vlan-id* }

View

User view

定義済みユーザロール

network-admin

パラメータ

all: すべての VLAN を指定します。

vlan *vlan-id*: VLAN の ID を指定します。設定範囲は 1～4094 です。指定しない場合、すべてのダイナミックルータポートの情報を削除します。

説明

reset mld-snooping router-port コマンドはダイナミックルータポートの情報を削除します。

例

すべてのダイナミックルータポートの情報を削除します。

<Switch> reset mld-snooping router-port all

関連コマンド

display mld-snooping router-port

3.1.47 reset mld-snooping statistics

Syntax

reset mld-snooping statistics

View

User view

定義済みユーザロール

network-admin

説明

reset mld-snooping statistics コマンドは MLD snooping によって学習したすべての MLD メッセージと IPv6 PIM hello メッセージの統計情報を削除します。

例

MLD snooping によって学習したすべての MLD メッセージと IPv6 PIM hello メッセージの統計情報を削除します。

<Switch> reset mld-snooping statistics

関連コマンド

display mld-snooping statistics

3.1.48 router-aging-time (MLD-snooping view)

Syntax

router-aging-time *seconds*

undo router-aging-time

デフォルト

260 秒

View

MLD-snooping view

定義済みユーザロール

network-admin

パラメータ

seconds: ダイナミックルータポートのエージングタイマを設定します。設定範囲は 1～8097894 秒です。

説明

router-aging-time コマンドはグローバルでダイナミックルータポートのエージングタイマを設定します。

undo router-aging-time コマンドはデフォルトに戻します。

このコマンドは **mld-snooping router-aging-time** コマンドと同一機能ですが、適用範囲が異なります。

- MLD-snooping view の **router-aging-time** コマンドはすべての VLAN に適用されます。
- **mld-snooping router-aging-time** コマンドは現在の VLAN に適用されます。

VLAN では **mld-snooping router-aging-time** コマンドは MLD-snooping view の **router-aging-time** コマンドより優先されます。

例

グローバルでダイナミックルータポートのエージングタイマを 100 秒に設定します。

<Switch> system-view

[Switch] mld-snooping

[Switch-mld-snooping] router-aging-time 100

関連コマンド

mld-snooping router-aging-time

3.1.49 source-deny (MLD-snooping view)

Syntax

source-deny port *interface-list*

undo source-deny port *interface-list*

デフォルト

無効

View

MLD-snooping view

定義済みユーザロール

network-admin

パラメータ

port *interface-list*: ポートリストを指定します。ポートのアイテムを半角スペースで区切り、ポートのタイプと番号を指定するか、ポートの範囲で指定します。ポートを範囲で指定する形式は *start-interface-type interface-number* **to** *end-interface-type interface-number* です。

説明

source-deny コマンドはすべての受信した IPv6 マルチキャストデータパケットを廃棄するため、ポートで IPv6 マルチキャストソースポートのフィルタを有効にします。

undo source-deny コマンドはポートで IPv6 マルチキャストソースポートのフィルタを無効にします。

このコマンドは **mld-snooping source-deny** コマンドと同一機能ですが、適用範囲が異なります。

- MLD-snooping view の **source-deny** マンドはすべてのポートに適用されます。
- **mld-snooping source-deny** コマンドは現在のポートに適用されます。

ポートでは **mld-snooping source-deny** コマンドは MLD-snooping view の **source-deny** コマンドの優先度は同一です。最後に行われた設定が適用されます。

例

GigabitEthernet 1/0/1～GigabitEthernet 1/0/4 で IPv6 マルチキャストデータのソースポートのフィルタを有効にします。

<Switch> system-view

[Switch] mld-snooping

[Switch-mld-snooping] source-deny port gigabitethernet 1/0/1 to gigabitethernet 1/0/4

関連コマンド

mld-snooping source-deny

3.1.50 version (MLD-snooping view)

Syntax

version *version-number* **vlan** *vlan-list*

undo version vlan *vlan-list*

デフォルト

1

View

MLD-snooping view

定義済みユーザロール

network-admin

パラメータ

version-number: MLD snooping のバージョンを指定します。1 あるいは 2 です。

vlan *vlan-list*: VLAN を指定します。半角スペースで区切り、10 まで設定することができます。VLAN を範囲で指定する形式は *start-vlan-id* **to** *end-vlan-id* です。設定範囲は 1～4094 です。指定しない場合、すべての VLAN に適用します。

説明

version コマンドは VLAN の MLD snooping のバージョンを指定します。

undo version コマンドはデフォルトに戻します。

このコマンドを実行する前に、VLAN の MLD snooping 機能を有効にしてください。

このコマンドは **version** コマンドと同一機能ですが、適用範囲が異なります。

- MLD-snooping view の **version** コマンドは指定された VLAN に適用されます。
- **mld-snooping version** コマンドは現在の VLAN に適用されます。

VLAN では **mld-snooping version** コマンドは MLD-snooping view の **version** コマンドの優先度は同一です。最後に行われた設定が適用されます。

例

VLAN 2～VLAN 10 の MLD snooping を有効にし、MLD snooping のバージョンを 2 に指定します。

<Switch> system-view

[Switch] mld-snooping

[Switch-mld-snooping] enable vlan 2 to 10

[Switch-mld-snooping] version 2 vlan 2 to 10

関連コマンド

- **enable (MLD-snooping view)**
- **mld-snooping enable**
- **mld-snooping version**

目次

このセクションのページは **6-x-x** です。

4 章 IPv6 マルチキャスト VLAN 4-1
4.1 IPv6 マルチキャスト VLAN 設定コマンド 4-1
4.1.1 display ipv6 multicast-vlan 4-1
4.1.2 display ipv6 multicast-vlan forwarding-table 4-2
4.1.3 display ipv6 multicast-vlan group 4-4
4.1.4 ipv6 multicast-vlan 4-6
4.1.5 ipv6 multicast-vlan entry-limit 4-8
4.1.6 ipv6 port multicast-vlan 4-8
4.1.7 port (IPv6 multicast VLAN view) 4-9
4.1.8 reset ipv6 multicast-vlan group 4-10
4.1.9 subvlan (IPv6 multicast VLAN view) 4-11

4章 IPv6 マルチキャスト VLAN

4.1 IPv6マルチキャストVLAN設定コマンド

4.1.1 display ipv6 multicast-vlan

Syntax

display ipv6 multicast-vlan [*vlan-id*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

vlan-id: IPv6 マルチキャスト VLAN の ID を指定します。設定範囲は 1～4094 です。指定しない場合、すべての IPv6 マルチキャスト VLAN の情報を表示します。

説明

display ipv6 multicast-vlan コマンドは IPv6 マルチキャスト VLAN の情報を表示します。

例

すべての IPv6 マルチキャスト VLAN の情報を表示します。

<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):
```

表 4-1 コマンド出力

フィールド	説明
Total 2 IPv6 multicast VLANs	IPv6マルチキャストVLANの総数です。
Sub-VLAN list(3 in total)	IPv6マルチキャストVLANのサブVLANのリストと、サブVLANの総数です。
Port list(3 in total)	IPv6マルチキャストVLANのポートリストとポートの総数です。

4.1.2 display ipv6 multicast-vlan forwarding-table

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*] *

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ipv6-source-address: IPv6 マルチキャストソースの IPv6 アドレスを指定します。IPv6 マルチキャストソースを指定しない場合、すべての IPv6 マルチキャストソースの IPv6 マルチキャスト VLAN 転送エントリを表示します。

prefix-length: IPv6 マルチキャストソースの IPv6 アドレスのプレフィックス長を指定します。設定範囲は 0～128 です。デフォルトは 128 です。

ipv6-group-address: IPv6 マルチキャストグループの IPv6 アドレスを指定します。設定範囲は FFxy::/16 です。x と y は 16 進数の 0～F です。IPv6 マルチキャストグループを指定しない場合、すべての IPv6 マルチキャストグループの IPv6 マルチキャスト VLAN 転送エントリを表示します。

prefix-length: IPv6 マルチキャストグループの IPv6 アドレスのプレフィックス長を指定します。設定範囲は 8～128 です。デフォルトは 128 です。

slot *slot-number*: IRF スタックメンバ装置を指定します。*slot-number* は IRF スタックメンバ装置の ID を示します。指定しない場合、IRF スタックユニットのマスタ装置の IPv6 マルチキャスト VLAN 転送エントリを表示します。

subvlan *vlan-id*: サブ VLAN の ID を指定します。指定しない場合、すべてのサブ VLAN の IPv6 マルチキャスト VLAN 転送エントリを表示します。

vlan *vlan-id*: IPv6 マルチキャスト VLAN の ID を指定します。設定範囲は 1～4094 です。指定しない場合、すべての IPv6 マルチキャスト VLAN の IPv6 マルチキャスト VLAN 転送エントリを表示します。

説明

display ipv6 multicast-vlan forwarding-table コマンドは IPv6 マルチキャスト VLAN 転送エントリを表示します。

例

すべての IPv6 マルチキャスト VLAN 転送エントリを表示します。

<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
```

表 4-2 コマンド出力

フィールド	説明
IPv6 multicast VLAN 100 Forwarding Table	IPv6マルチキャストVLAN 100の転送テーブルです。
Total 1 entries, 1 matched	転送エントリの総数と一致するエントリの総数です。
00001	（S,G）エントリのシーケンス番号です。
(1::1, FF0E::1)	（S,G）エントリです。Sがダブルコロン（::）の場合、すべてのIPv6マルチキャストソースを示します。
Flags	（S,G）エントリの現在の状態です。ビットが異なるとエントリの状態が異なります。1つのフラグあるいは複数のフラグの合計を示します。たとえば、0x10000はエントリが1つのフラグ0x10000のみあることを示します。このフィールドの値を表 4-3に示します。
List of sub-VLANs (3 in total)	IPv6マルチキャストVLANのサブVLANとサブVLANの総数です。

表 4-3 フィールドの値

値	意味
0x1	エントリが非アクティブ状態です。
0x4	エントリがアップデートに失敗しています。
0x8	エントリがサブVLAN情報のアップデートに失敗しています。
0x200	エントリが円滑な状態です。
0x10000	エントリがマルチキャストVLANの転送エントリです。

4.1.3 display ipv6 multicast-vlan group

Syntax

display ipv6 multicast-vlan group [*ipv6-source-address* | *ipv6-group-address* | **slot** *slot-number* | **verbose** | **vlan** *vlan-id*] *

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ipv6-source-address: IPv6 マルチキャストソースの IPv6 アドレスを指定します。IPv6 マルチキャストソースを指定しない場合、IPv6 マルチキャスト VLAN のすべての IPv6 マルチキャストソースの IPv6 マルチキャストグループの情報を表示します。

ipv6-group-address: IPv6 マルチキャストグループの IPv6 アドレスを指定します。設定範囲は FFxy::/16（FFx0::/16、FFx1::/16、FFx2::/16、FF0y::を除きます）です。x と y は 16 進数の 0～F です。IPv6 マルチキャストグループを指定しない場合、IPv6 マルチキャスト VLAN のすべての IPv6 マルチキャストグループの情報を表示します。

slot *slot-number*: IRF スタックメンバ装置を指定します。*slot-number* は IRF スタックメンバ装置の ID を示します。指定しない場合、IRF スタックユニットのマスタ装置の IPv6 マルチキャスト VLAN の IPv6 マルチキャストグループの情報を表示します。

verbose: 詳細情報を表示します。指定しない場合、概要情報を表示します。

vlan *vlan-id*: IPv6 マルチキャスト VLAN の ID を指定します。設定範囲は 1～4094 です。指定しない場合、すべての IPv6 マルチキャスト VLAN の IPv6 マルチキャストグループの情報を表示します。

説明

display ipv6 multicast-vlan group コマンドは IPv6 マルチキャスト VLAN の IPv6 マルチキャストグループの情報を表示します。

例

すべての IPv6 マルチキャスト VLAN のすべての IPv6 マルチキャストグループの詳細情報を表示します。

<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):
```

表 4-4 コマンド出力

フィールド	説明
Total 6 entries	（S,G）エントリの総数です。
IPv6 multicast VLAN 10: Total 3 entries	IPv6マルチキャストVLAN 10の（S,G）エントリの総数です。

フィールド	説明
(::, FF0E::10)	（S,G）エントリです。Sがダブルコロン（::）の場合、すべてのIPv6マルチキャストソースを示します。
Flags	（S,G）エントリの現在の状態です。1つのフラグあるいは複数のフラグの合計を示します。たとえば、0x70000020はエントリがフラグ0x20、0x10000000、0x20000000、0x40000000があることを示します。このフィールドの値を表 4-5に示します。
Sub-VLANs (1 in total)	IPv6マルチキャストVLANのサブVLANとサブVLANの総数です。

表 4-5 フラグフィールドの値

値	意味
0x10	エントリがIPv6マルチキャストVLANによって作成されました。
0x20	エントリがIPv6マルチキャストVLANのサブVLANによって作成されました。
0x40	エントリが削除されました。
0x10000000	この値は以下の状態の1つを示します。 ● エントリが新規に作成されました。 ● 装置はMLD general クエリ送信間隔内に一致するMLD reportを受信しました。
0x20000000	装置はMLD general クエリ送信間隔内にエントリに一致するMLDv1あるいはMLDv2 reportを受信していません。
0x40000000	装置はMLD general クエリ送信間隔内にエントリに一致するMLDv2 IS_EX (NULL) reportを受信していません。

関連コマンド

reset ipv6 multicast-vlan group

4.1.4 ipv6 multicast-vlan

Syntax

ipv6 multicast-vlan *vlan-id*

undo ipv6 multicast-vlan { **all** | *vlan-id* }

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

vlan-id: VLAN の ID を指定します。設定範囲は 1～4094 です。

all: すべての IPv6 マルチキャスト VLAN を指定します。

説明

ipv6 multicast-vlan コマンドは IPv6 マルチキャスト VLAN を設定し、IPv6 multicast VLAN view に移行します。

undo ipv6 multicast-vlan コマンドは IPv6 マルチキャスト VLAN を削除します。

装置の IPv6 マルチキャスト VLAN の総数はシステムがサポートする最大数を超過することができません。

IPv6 マルチキャスト VLAN として設定されている VLAN で、MLD snooping を有効にしてください。

IPv6 マルチキャストルーティングが有効な装置で IPv6 マルチキャスト VLAN を設定しないでください。

例

VLAN 100 で MLD snooping を有効にします。IPv6 マルチキャスト VLAN として VLAN 100 を設定し、IPv6 multicast VLAN view に移行します。

<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]

関連コマンド

mld-snooping enable

4.1.5 ipv6 multicast-vlan entry-limit

Syntax

ipv6 multicast-vlan entry-limit *limit*

undo ipv6 multicast-vlan entry-limit

デフォルト

500

View

System view

定義済みユーザロール

network-admin

パラメータ

limit: IPv6 マルチキャスト VLAN 転送エントリの最大数を設定します。設定範囲は 0～500 です。

説明

ipv6 multicast-vlan entry-limit コマンドは IPv6 マルチキャスト VLAN 転送エントリの最大数を設定します。

undo ipv6 multicast-vlan entry-limit コマンドはデフォルトに戻します。

例

IPv6 マルチキャスト VLAN 転送エントリの最大数を 100 に設定します。

<Switch> system-view

[Switch] ipv6 multicast-vlan entry-limit 100

関連コマンド

entry-limit (MLD-snooping view)

4.1.6 ipv6 port multicast-vlan

Syntax

ipv6 port multicast-vlan *vlan-id*

undo ipv6 port multicast-vlan

デフォルト

設定なし

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id: IPv6 マルチキャスト VLAN の ID を指定します。設定範囲は 1～4094 です。

説明

ipv6 port multicast-vlan コマンドは IPv6 マルチキャスト VLAN にポートを割り当てます。

undo ipv6 port multicast-vlan コマンドはデフォルトに戻します。

ポートは 1 つの IPv6 マルチキャスト VLAN にのみ所属することができます。

IPv6 マルチキャスト VLAN に割り当てられているポートでは、ポートが所属している VLAN で MLD snooping を有効にする必要があります。

例

GigabitEthernet 1/0/1 を IPv6 マルチキャスト VLAN 100 に割り当てます。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] ipv6 port multicast-vlan 100

4.1.7 port (IPv6 multicast VLAN view)

Syntax

port *interface-list*

undo port { **all** | *interface-list* }

デフォルト

設定なし

View

IPv6 multicast VLAN view

定義済みユーザロール

network-admin

パラメータ

interface-list: ポートあるいはポート範囲を指定します。形式は *interface-type interface-number* です。ポート範囲の形式は *interface-type interface-number* **to** *interface-type interface-number* です。

all: 現在の IPv6 マルチキャスト VLAN のすべてのユーザポートを指定します。

説明

port コマンドは IPv6 マルチキャスト VLAN にユーザポートを割り当てます。

undo port コマンドは IPv6 マルチキャスト VLAN からユーザポートを取り外します。

IPv6 マルチキャスト VLAN のユーザポートとして Ethernet ポートとアグリゲートインタフェースを割り当てることができます。ポートは 1 つの IPv6 マルチキャスト VLAN にのみ所属することができます。

IPv6 マルチキャスト VLAN に割り当てられているポートでは、ポートが所属している VLAN で MLD snooping を有効にする必要があります。

例

GigabitEthernet 1/0/1～GigabitEthernet 1/0/5 を IPv6 マルチキャスト VLAN 100 に割り当てます。

<Switch> system-view

[Switch] ipv6 multicast-vlan 100

[Switch-ipv6-mvlan-100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/5

4.1.8 reset ipv6 multicast-vlan group

Syntax

reset ipv6 multicast-vlan group [*ipv6-group-address* [*prefix-length*] | *ipv6-source-address* [*prefix-length*] | **vlan** *vlan-id*] *

View

User view

定義済みユーザロール

network-admin

パラメータ

ipv6-group-address: IPv6 マルチキャストグループの IPv6 アドレスを指定します。設定範囲は FFxy::/16（FFx0::/16、FFx1::/16、FFx2::/16、FF0y::を除きます）です。x と y は 16 進数の 0～F です。IPv6 マルチキャストグループを指定しない場合、すべての IPv6 マルチキャストグループの IPv6 マルチキャスト VLAN 転送エントリを削除します。

prefix-length: IPv6 マルチキャストグループの IPv6 アドレスのプレフィックス長を指定します。設定範囲は 8～128 です。デフォルトは 128 です。

ipv6-source-address: IPv6 マルチキャストソースの IPv6 アドレスを指定します。IPv6 マルチキャストソースを指定しない場合、すべての IPv6 マルチキャストソースの IPv6 マルチキャスト VLAN 転送エントリを削除します。

prefix-length: IPv6 マルチキャストソースの IPv6 アドレスのプレフィックス長を指定します。設定範囲は 0～128 です。デフォルトは 128 です。

vlan *vlan-id*: VLAN の ID を指定します。設定範囲は 1～4094 です。指定しない場合、すべての IPv6 マルチキャスト VLAN の IPv6 マルチキャスト VLAN 転送エントリを削除します。

説明

reset ipv6 multicast-vlan group コマンドは IPv6 マルチキャスト VLAN 転送エントリを削除します。

例

すべての IPv6 マルチキャスト VLAN 転送エントリを削除します。

<Switch> reset ipv6 multicast-vlan group

関連コマンド

display ipv6 multicast-vlan group

4.1.9 subvlan (IPv6 multicast VLAN view)

Syntax

subvlan *vlan-list*

undo subvlan { **all** | *vlan-list* }

デフォルト

設定なし

View

IPv6 multicast VLAN view

定義済みユーザロール

network-admin

パラメータ

vlan-list: VLAN を指定します。半角スペースで区切り 10 まで設定するか、VLAN の範囲で設定することができます。VLAN を範囲で指定する形式は *start-vlan-id* **to** *end-vlan-id* です。設定範囲は 1～4094 です。

all: 現在の IPv6 マルチキャスト VLAN のすべてのサブ VLAN を指定します。

説明

subvlan コマンドは IPv6 マルチキャスト VLAN にサブ VLAN を割り当てます。

undo subvlan コマンドは IPv6 マルチキャスト VLAN からサブ VLAN を削除します。

IPv6 マルチキャスト VLAN のサブ VLAN として設定される VLAN で、MLD snooping を有効にしてください。

例

IPv6 マルチキャスト VLAN 100 のサブ VLAN として VLAN 10～VLAN 15 を設定します。

<Switch> system-view

[Switch] ipv6 multicast-vlan 100

[Switch-ipv6-mvlan-100] subvlan 10 to 15

QX-S5100G シリーズ Ethernet スイッチ

コマンドマニュアル

7.MCE

本マニュアルは以下に示す章で構成されています。

01-MCE

02-IPv6 MCE

目次

このセクションのページは **7-x-x** です。

1 章 MCE 1-1
1.1 MCE 設定コマンド 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 1-3
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) 1-10
1.1.11 vpn-target 1-10

1章 MCE

1.1 MCE設定コマンド

1.1.1 address-family ipv4 (VPN instance view)

Syntax

address-family ipv4

undo address-family ipv4

View

VPN instance view

定義済みユーザロール

network-admin

説明

address-family ipv4 コマンドは VPN インスタンスで IPv4 VPN view に移行します。

undo address-family ipv4 コマンドは IPv4 VPN view のすべての設定を削除します。

IPv4 VPN view では受信ルーティングポリシー、送信ルーティングポリシーのような IPv4 VPN のパラメータを設定することができます。

例

IPv4 VPN view に移行します。

<Switch> system-view

[Switch] ip vpn-instance vpn1

[Switch-vpn-instance-vpn1] address-family ipv4

[Switch-vpn-ipv4-vpn1]

関連コマンド

address-family ipv6 (VPN instance view)

1.1.2 description (VPN instance view)

Syntax

description *text*

undo description

デフォルト

設定なし

View

VPN instance view

定義済みユーザロール

network-admin

パラメータ

text: VPN インスタンスの記述を指定します。設定範囲は 1～79 文字です。大文字、小文字を区別します。

説明

description コマンドは VPN インスタンスの記述を設定します。

undo description コマンドは記述を削除します。

例

VPN インスタンス **vpn1** の記述を **This is vpn1** に設定します。

<Switch> system-view

[Switch] ip vpn-instance vpn1

[Switch-vpn-instance-vpn1] description This is vpn1

1.1.3 display ip vpn-instance

Syntax

display ip vpn-instance [**instance-name** *vpn-instance-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

instance-name *vpn-instance-name*: 指定された VPN インスタンスの情報を表示します。

vpn-instance-name の設定範囲は 1～31 文字です。VPN インスタンスを指定しない場合、すべての VPN インスタンスの概要情報を表示します。

説明

display ip vpn-instance コマンドは VPN インスタンスの情報を表示します。

例

すべての VPN インスタンスの概要情報を表示します。

<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
```

表 1-1 コマンド出力

フィールド	説明
VPN-Instance Name	VPNインスタンスの名前です。
RD	VPNインスタンスのRDです。
Create Time	VPNインスタンスが作成された時間です。

1.1.4 export route-policy

Syntax

export route-policy *route-policy*

undo export route-policy

デフォルト

設定なし

View

VPN instance view, IPv4 VPN view, IPv6 VPN view

定義済みユーザロール

network-admin

パラメータ

route-policy: ルーティングポリシーを指定します。設定範囲は 1～63 文字です。大文字、小文字を区別します。

説明

export route-policy コマンドは VPN インスタンスに送信ルーティングポリシーを適用します。

undo export route-policy コマンドはデフォルトに戻します。

配信されたルートをフィルタする、あるいは VPN インスタンスのルート属性を変更するため、送信ルーティングポリシーを指定することができます。

このコマンドを複数回実行すると、最新の設定が有効になります。

VPN instance view で指定された送信ルーティングポリシーは IPv4 VPN と IPv6 VPN の両方に適用します。

IPv4 VPN view あるいは IPv6 VPN view で指定された送信ルーティングポリシーは IPv4 VPN あるいは IPv6 VPN のいずれかに適用します。

IPv4/IPv6 VPN は VPN instance view で指定された送信ルーティングポリシーより、IPv4 VPN view あるいは IPv6 VPN view で指定された送信ルーティングポリシーが適しています。

例

送信ルーティングポリシー**poly-1** を VPN インスタンス **vpn1** に適用します。

<Switch> system-view

[Switch] ip vpn-instance vpn1

[Switch-vpn-instance-vpn1] export route-policy poly-1

関連コマンド

- **import route-policy**
- **route-policy** (コマンドマニュアルのセクション 5 *ルーティングプロトコル*)

1.1.5 import route-policy

Syntax

import route-policy *route-policy*

undo import route-policy

デフォルト

受信ターゲット属性に一致するすべてのルートが受け入れられます。

View

VPN instance view, IPv4 VPN view, IPv6 VPN view

定義済みユーザロール

network-admin

パラメータ

route-policy: ルーティングポリシーを指定します。設定範囲は 1～63 文字です。大文字、小文字を区別します。

説明

import route-policy コマンドは VPN インスタンスに受信ルーティングポリシーを適用します。

undo import route-policy コマンドはデフォルトに戻します。

VPN インスタンスの受信ルートをフィルタする、あるいはルートの属性を変更するため、受信ルーティングポリシーを設定することができます。

このコマンドを複数回実行すると、最新の設定が有効になります。

VPN instance view で指定された受信ルーティングポリシーは IPv4 VPN と IPv6 VPN の両方に適用します。

IPv4 VPN view あるいは IPv6 VPN view で指定された受信ルーティングポリシーは IPv4 VPN あるいは IPv6 VPN のいずれかに適用します。

IPv4/IPv6 VPN は VPN instance view で指定された受信ルーティングポリシーより、IPv4 VPN view あるいは IPv6 VPN view で指定された受信ルーティングポリシーが適しています。

例

受信ルーティングポリシー**poly-1** を VPN インスタンス **vpn1** に適用します。

<Switch> system-view

[Switch] ip vpn-instance vpn1

[Switch-vpn-instance-vpn1] import route-policy poly-1

関連コマンド

- **export route-policy**
- **route-policy**(コマンドマニュアルのセクション 5 *ルーティングプロトコル*)

1.1.6 ip binding vpn-instance

Syntax

ip binding vpn-instance *vpn-instance-name*

undo ip binding vpn-instance

デフォルト

インタフェースは VPN インスタンスに関連づけられておらず、パブリックネットワークに属しています。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

vpn-instance-name: VPN インスタンスを指定します。設定範囲は 1～31 文字です。大文字、小文字を区別します。

説明

ip binding vpn-instance コマンドはインタフェースに VPN インスタンスを関連づけます。

undo ip binding vpn-instance コマンドはデフォルトに戻します。

VPN インスタンスをサイトに接続されたインタフェース、CE に接続されたインタフェースに関連づけるため、MCE で **ip binding vpn-instance** コマンドを使用します。

ip binding vpn-instance コマンドあるいは **undo ip binding vpn-instance** コマンドはインタフェースの IP アドレス、ルーティングプロトコルの設定を削除します。

指定された VPN インスタンスは system view で **ip vpn-instance** コマンドを使用して設定されている必要があります。

新しい VPN インスタンスをインタフェースに関連づけるため、最初に **undo ip binding vpn-instance** コマンドを実行して既存の関連付けを削除します。

例

VPN インタフェース 1 を VPN インスタンス **vpn1** に関連づけます。

<Switch> system-view

[Switch] interface vlan-interface 1

[Switch-Vlan-interface1] ip binding vpn-instance vpn1

関連コマンド

ip vpn-instance (system view)

1.1.7 ip vpn-instance (system view)

Syntax

ip vpn-instance *vpn-instance-name*

undo ip vpn-instance *vpn-instance-name*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

vpn-instance-name: VPN インスタンスを指定します。設定範囲は 1～31 文字です。大文字、小文字を区別します。

説明

ip vpn-instance コマンドは VPN インスタンスを作成し、VPN instance view に移行します。

undo ip vpn-instance コマンドは VPN インスタンスを削除します。

例

VPN インスタンス **vpn1** を作成し、view に移行します。

<Switch> system-view

[Switch] ip vpn-instance vpn1

[Switch-vpn-instance-vpn1]

関連コマンド

route-distinguisher

1.1.8 route-distinguisher (VPN instance view)

Syntax

route-distinguisher *route-distinguisher*

undo route-distinguisher

デフォルト

設定なし

View

VPN instance view

定義済みユーザロール

network-admin

パラメータ

route-distinguisher: VPN インスタンスの RD を指定します。設定範囲は以下の形式で 3～21 文字です。

- 16 ビット AS 番号 : 32 ビットユーザによって定義された番号です。たとえば、101:3 です。
- 32 ビット IP アドレス : 16 ビットユーザによって定義された定義番号です。たとえば、192.168.122.15:1 です。
- 32 ビット AS 番号 : 16 ビットユーザによって定義された定義番号です。たとえば、65536:1 です。AS 番号の最小値は 65536 です。

説明

route-distinguisher コマンドは VPN インスタンスの RD を設定します。

undo route-distinguisher コマンドはデフォルトに戻します。

RD は VPN が同一アドレス空間を使用できるように有効にします。RD と IPv4 プレフィックスは、固有の VPN IPv4 プレフィックスを構成します。

VPN-IPv4 アドレスのグローバル一意性を保証するには、RD 内の AS 番号または IP アドレスをプライベート AS 番号またはプライベート IP アドレスに設定しないでください。

VPN インスタンスの RD を変更する場合、**undo route-distinguisher** コマンドで RD を削除し、新しい RD を設定するため、**route-distinguisher** コマンドを使用する必要があります。

例

VPN インスタンス **vpn1** の RD を 22:1 に設定します。

<Switch> system-view

[Switch] ip vpn-instance vpn1

[Switch-vpn-instance-vpn1] route-distinguisher 22:1

1.1.9 routing-table limit

Syntax

routing-table limit *number* { *warn-threshold* | **simply-alert** }

undo routing-table limit

デフォルト

設定なし

View

VPN instance view, IPv4 VPN view, IPv6 VPN view

定義済みユーザロール

network-admin

パラメータ

number: アクティブルートの最大数を指定します。VPN instance view あるいは IPv6 VPN view の設定範囲は 1～1280 です。IPv4 VPN view の設定範囲は 1～5120 です。

warn-threshold: warning しきい値を指定します。設定範囲は 1～100%です。既存のアクティブルート数とアクティブルートの最大数の割合が指定したしきい値を超過したとき、システムはアラームメッセージを表示しますが、新規のアクティブルートを許可し続けます。VPN インスタンスのアクティブルートが最大値に到達したとき、アクティブルートは追加されません。

simply-alert: アクティブルートが最大値を超過したとき、システムはアクティブルートを受信しますが、システムログメッセージを作成します。

説明

routing-table limit コマンドは VPN インスタンスのアクティブルートの最大数を指定します。

undo routing-table limit コマンドはデフォルトに戻します。

VPN インスタンスのアクティブルートの最大数を設定すると、PE がルートを過剰に学習するのを防ぐことができます。

VPN instance view で設定された制限は IPv4 VPN と IPv6 VPN の両方に適用します。

IPv4 VPN view あるいは IPv6 VPN view で設定された制限は IPv4 VPN あるいは IPv6 VPN のいずれかに適用します。

IPv4/IPv6 VPN は VPN instance view で設定された制限より、IPv4 VPN view あるいは IPv6 VPN view で設定された制限が適しています。

例

VPN インスタンス **vpn1** で 1000 のアクティブルートをサポートするように設定します。アクティブルートが上限を超過したとき、新しいアクティブルートを受信し、システムログメッセージを作成します。

```
<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)

Syntax

vpn-instance-capability simple

undo vpn-instance-capability

デフォルト

有効

View

OSPF view

定義済みユーザロール

network-admin

説明

vpn-instance-capability simple コマンドは OSPF VRF プロセスのルーティングループの検出を無効にします。

undo vpn-instance-capability コマンドはルーティングループの検出を有効にします。

MCE が PE から OSPF ルートを受信するには、MCE で OSPF VRF プロセスのルーティングループの検出を無効にする必要があります。

このコマンドは OSPF VRF プロセスにのみ適用します。

例

OSPF VRF プロセス 100 のルーティングループの検出を無効にします。

<Switch> system-view

[Switch] ospf 100 vpn-instance vpna

[Switch-ospf-100] vpn-instance-capability simple

1.1.11 vpn-target

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**] }

デフォルト

設定なし

View

VPN instance view, IPv4 VPN view, IPv6 VPN view

定義済みユーザロール

network-admin

パラメータ

vpn-target&<1-8>: 半角スペースで区切り、8 つまでルートターゲットを指定します。ルートターゲットは以下の形式を使用します。設定範囲は 3～21 です。

- 16 ビット AS 番号 : 32 ビットユーザによって定義された番号です。たとえば、101:3 です。
- 32 ビット IP アドレス : 16 ビットユーザによって定義された定義番号です。たとえば、192.168.122.15:1 です。
- 32 ビット AS 番号 : 16 ビットユーザによって定義された定義番号です。たとえば、65536:1 です。AS 番号の最小値は 65536 です。

both: 受信ターゲットと送信ターゲットの両方のルートターゲットを指定します。**both** パラメータ、**export-extcommunity** パラメータ、**import-extcommunity** パラメータが指定されない場合、デフォルトで **both** パラメータが指定されます。

export-extcommunity: 送信ターゲットとしてルートターゲットを指定します。

import-extcommunity: 受信ターゲットとしてルートターゲットを指定します。

all: すべてのルートターゲットを削除します。

説明

vpn-target コマンドは VPN インスタンスのルートターゲットを設定します。

undo vpn-target コマンドは VPN インスタンスの指定した、あるいはすべてのルートターゲットを削除します。

VPN インスタンスは VPN ルーティング情報の配信を管理するため、ルートターゲットを使用します。PE は設定された送信ターゲットを、ピアに配信されたルートのルートターゲットの属性に追加します。

ピアはローカルの送信ターゲットが受信したルートのルートターゲットに一致するかどうか確認します。ルータターゲットに一致した場合、ピアは VPN インスタンスのルーティングテーブルにルートを追加します。

vpn-target コマンドを繰り返して、複数のルートターゲットを設定できます。

VPN instance view で設定されたルータターゲットは IPv4 VPN と IPv6 VPN の両方に適用します。

IPv4 VPN view あるいは IPv6 VPN view で設定されたルータターゲットは IPv4 VPN あるいは IPv6 VPN のいずれかに適用します。

IPv4/IPv6 VPN は VPN instance view で設定されたルータターゲットより、IPv4 VPN view あるいは IPv6 VPN view で設定されたルータターゲットが優先されます。

例

VPN インスタンス **vpn1** のルートターゲットを設定します。

```
<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
```

目次

このセクションのページは **7-x-x** です。

2 章 IPv6 MCE 2-1
2.1 IPv6 MCE 設定コマンド 2-1
2.1.1 address-family ipv6 (VPN instance view) 2-1
2.1.2 vpn-instance-capability simple (OSPFv3 view) 2-2

2章 IPv6 MCE

MCE と IPv6 MCE の両方で有効なコマンドは、オペレーションマニュアルのセクション *7 MCE”MCE”* を参照してください。

2.1 IPv6 MCE設定コマンド

2.1.1 address-family ipv6 (VPN instance view)

Syntax

address-family ipv6

undo address-family ipv6

View

VPN instance view

定義済みユーザロール

network-admin

説明

address-family ipv6 コマンドは VPN インスタンスで IPv6 VPN view に移行します。

undo address-family ipv6 コマンドは IPv6 VPN view のすべての設定を削除します。

IPv6 VPN viewでは受信ルーティングポリシー、送信ルーティングポリシーのような IPv6 VPN のパラメータを設定することができます。

例

IPv6 VPN view に移行します。

<Switch> system-view

[Switch] ip vpn-instance vpn1

[Switch-vpn-instance-vpn1] address-family ipv6

[Switch-vpn-ipv6-vpn1]

関連コマンド

address-family ipv4 (VPN instance view)

2.1.2 vpn-instance-capability simple (OSPFv3 view)

Syntax

vpn-instance-capability simple

undo vpn-instance-capability

デフォルト

有効

View

OSPFv3 view

定義済みユーザロール

network-admin

説明

vpn-instance-capability simple コマンドは OSPFv3 VRF プロセスのルーティングループ検出を無効にします。

undo vpn-instance-capability コマンドは OSPFv3 VRF プロセスのルーティングループ検出を有効にします。

MCE が PE から OSPFv3 ルートを受信するには、MCE で OSPFv3 VRF プロセスのルーティングループの検出を無効にする必要があります。

このコマンドは OSPFv3 VRF プロセスにのみ適用します。

例

OSPFv3 VRF プロセス 100 のルーティングループの検出を無効にします。

<Switch> system-view

[Switch] ospfv3 100 vpn-instance vpn1

[Switch-ospfv3-100] vpn-instance-capability simple

QX-S5100G シリーズ Ethernet スイッチ

コマンドマニュアル

8.ACL and QoS

本マニュアルは以下に示す章で構成されています。

01-ACL
02-QoS ポリシー
03-プライオリティマッピング
04-トラフィックポリシング、GTS、ラインレート
05-輻輳制御
06-データバッファ
07-タイムレンジ

目次

このセクションのページは **8-x-x** です。

1 章 ACL 1-1
1.1 ACL 設定コマンド 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 acl name 1-5
1.1.5 description 1-6
1.1.6 display acl 1-7
1.1.7 display packet-filter 1-9
1.1.8 display packet-filter statistics 1-11
1.1.9 display packet-filter statistics sum 1-14
1.1.10 display packet-filter verbose 1-16
1.1.11 display qos-acl resource 1-19
1.1.12 packet-filter 1-21
1.1.13 packet-filter filter 1-22
1.1.14 reset acl counter 1-23
1.1.15 reset packet-filter statistics 1-24
1.1.16 rule (IPv4 advanced ACL view) 1-25
1.1.17 rule (IPv4 basic ACL view) 1-31
1.1.18 rule (IPv6 advanced ACL view) 1-33
1.1.19 rule (IPv6 basic ACL view) 1-40
1.1.20 rule (Layer 2 ACL view) 1-42
1.1.21 rule comment 1-44
1.1.22 step 1-45

1章 ACL

1.1 ACL設定コマンド

1.1.1 acl

Syntax

acl [**ipv6**] **number** *acl-number* [**match-order** { **auto** | **config** }]

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**] **number** *acl-number*

undo acl [**ipv6**] { **all** | { **advanced** | **basic** } { *acl-number* | **name** *acl-name* } }

undo acl mac { **all** | *acl-number* | **name** *acl-name* }

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

ipv6: IPv6 ACL を指定します。指定しない場合、IPv4 ACL を指定します。

basic: 標準 ACL を指定します。

advanced: 拡張 ACL を指定します。

mac: L2 ACL を指定します。

acl-number: ACL の番号を指定します。以下に設定範囲を示します。

- 2000～2999：標準 ACL です。
- 3000～3999：拡張 ACL です。
- 4000～4999：L2 ACL です。

name *acl-name*: ACL を識別しやすくするため、ACL 名を指定します。設定範囲は 1～63 です。大文字、小文字は区別しません。最初の文字は英字を使用する必要があります。混乱を避けるため、**all** は使用できません。

match-order: パケットを比較する ACL ルールの順番を設定します。

- **auto**: 深さ優先順序に従って ACL ルールを比較します。
- **config**: ルール ID の昇順に従って ACL ルールを比較します。小さいルール ID は優先度が高くなります。ACL ルールの順序を指定しない場合、デフォルトで **config** が適用されます。

all: すべての ACL を指定します。

説明

acl コマンドは ACL を作成し、ACL の view に移行します。すでに ACL が作成されている場合、その view に移行します。

undo acl コマンドは指定された、あるいはすべての ACL を削除します。

ルールが含まれていない ACL のみ、比較順序を変更することができます。

ACL のルールが一致順序を含む、あるいは以下の一致基準が有効である場合、一致するパケットはソフトウェアベースのパケット転送を行います。

- 送信元 IP アドレス、宛先 IP アドレス
- 送信元ポート、宛先ポート
- トランスポートレイヤプロトコル
- ICMP あるいは ICMPv6 のメッセージタイプ、メッセージコード、メッセージ名
- ロギング
- タイムレンジ

ソフトウェアベースのパケット転送は、転送エントリのため、コントロールプレーンにパケットを送信します。これは装置のパケット転送に影響します。

例

標準 IPv4 ACL 2000 を作成し、その view に移行します。

<Switch> system-view

[Switch] acl basic 2000

[Switch-acl-ipv4-basic-2000]

ACL 名が flow の標準 IPv4 ACL を作成し、その view に移行します。

<Switch> system-view

[Switch] acl basic name flow

[Switch-acl-ipv4-basic-flow]

拡張 IPv4 ACL 3000 を作成し、その view に移行します。

<Switch> system-view

[Switch] acl advanced 3000

[Switch-acl-ipv4-adv-3000]

標準 IPv6 ACL 2000 を作成し、その view に移行します。

<Switch> system-view

[Switch] acl ipv6 basic 2000

[Switch-acl-ipv6-basic-2000]

ACL 名が flow の標準 IPv6 ACL を作成し、その view に移行します。

<Switch> system-view

[Switch] acl ipv6 basic name flow

[Switch-acl-ipv6-basic-flow]

ACL 名が flow の拡張 IPv4 ACL を作成し、その view に移行します。

<Switch> system-view

[Switch] acl ipv6 advanced name abc

[Switch-acl-ipv6-adv-abc]

L2 ACL 4000 を作成し、その view に移行します。

<Switch> system-view

[Switch] acl mac 4000

[Switch-acl-mac-4000]

ACL 名が flow の L2 ACL を作成し、その view に移行します。

<Switch> system-view

[Switch] acl mac name flow

[Switch-acl-mac-flow]

関連コマンド

display acl

1.1.2 acl copy

Syntax

acl [**ipv6** | **mac**] **copy** { *source-acl-number* | **name** *source-acl-name* } **to** { *dest-acl-number* | **name** *dest-acl-name* }

View

System view

定義済みユーザロール

network-admin

パラメータ

ipv6: IPv6 ACL を指定します。

mac: L2 ACL を指定します。

source-acl-number: ACL の番号を指定します。以下に設定範囲を示します。

- 2000～2999：標準 ACL です。
- 3000～3999：拡張 ACL です。
- 4000～4999：L2 ACL です。**mac** の指定が必要です。

name *source-acl-name*: ACL 名を指定します。設定範囲は 1～63 です。大文字、小文字は区別しません。

dest-acl-number: 新しい ACL の番号を指定します。以下に設定範囲を示します。

- 2000～2999：標準 ACL です。
- 3000～3999：拡張 ACL です。
- 4000～4999：L2 ACL です。

name *dest-acl-name*: ACL 名を指定します。設定範囲は 1～63 です。大文字、小文字は区別しません。最初の文字は英字を使用する必要があります。混乱を避けるため、**all** は使用できません。

説明

acl copy コマンドは既存の ACL をコピーします。

新しい ACL は既存の ACL と同一タイプにする必要があります。

新しい ACL は既存の ACL とカテゴリ、同一内容ですが、ACL 名と ACL 番号が異なります。

IPv4 ACL を指定する場合、**ipv6** パラメータあるいは **mac** パラメータを指定しないでください。

例

標準 IPv4 ACL 2001 をコピーし、標準 IPv4 ACL 2002 を作成します。

<Switch> system-view

[Switch] acl copy 2001 to 2002

ACL 名が test の標準 IPv4 ACL をコピーし、ACL 名が paste の標準 IPv4 ACL を作成します。

<Switch> system-view

[Switch] acl copy name test to name paste

1.1.3 acl logging interval

Syntax

acl logging interval *interval*

undo acl logging interval

デフォルト

0 です。パケットフィルタリングのログは出力されません。

View

System view

定義済みユーザロール

network-admin

パラメータ

interval: パケットフィルタリングのログが作成され、出力される間隔を指定します。設定範囲は 0～1440 分です。5 の倍数にする必要があります。パケットフィルタリングのログを無効にする場合、0 に設定します。

説明

acl logging interval コマンドはパケットフィルタリングのログを作成し、出力する間隔を設定します。

undo acl logging interval コマンドはデフォルトに戻します。

ログを作成する場合､IPv4 あるいは IPv6 ACL ルールで **logging** パラメータが必要です。

パケットフィルタリングのログエントリを作成するため、ACL モジュールを設定することができます。そしてログを設定された出力間隔で information center に送信します。ログエントリは、パケットに一致する数、および ACL ルールを記録します。ACL が初回に一致した場合、装置は即座に、パケットに一致するログを記録し、ログエントリを出力します。information center の詳細は、オペレーションマニュアルのセクション 11 *システム管理* “*Information Center*”を参照してください。

例

パケットフィルタリングのログを作成し、出力する間隔を 10 分に設定します。

<Switch> system-view

[Switch] acl logging interval 10

関連コマンド

- **rule (IPv4 advanced ACL view)**
- **rule (IPv4 basic ACL view)**
- **rule (IPv6 advanced ACL view)**
- **rule (IPv6 basic ACL view)**

1.1.4 acl name

Syntax

acl [**ipv6**] **name** *acl-name*

View

System view

定義済みユーザロール

network-admin

パラメータ

ipv6: IPv6 ACL を指定します。

acl-name: ACL 名を指定します。設定範囲は 1～63 です。大文字、小文字は区別しません。最初の文字は英字を使用する必要があります。ACL はすでに作成されている必要があります。

説明

acl name コマンドは ACL 名がある ACL の ACL view に移行します。

例

ACL 名が flow のデフォルトの標準 IPv4 ACL の ACL view に移行します。

<Switch> system-view

[Switch] acl name flow

[Switch-acl-basic-2001-flow]

ACL 名が flow のデフォルトの標準 IPv6 ACL の ACL view に移行します。

<Switch> system-view

[Switch] acl ipv6 name flow

[Switch-acl6-basic-2001-flow]

関連コマンド

acl

1.1.5 description

Syntax

description *text*

undo description

デフォルト

設定なし

View

IPv4 basic/advanced ACL view

IPv6 basic/advanced ACL view

Layer 2 ACL view

定義済みユーザロール

network-admin

パラメータ

text: ACL の説明を設定します。設定範囲は 1～127 です。大文字、小文字は区別します。

説明

description コマンドは ACL の説明を設定します。

undo description コマンドは ACL の説明を削除します。

例

標準 IPv4 ACL 2000 の説明を設定します。

<Switch> system-view

[Switch] acl basic 2000

[Switch-acl-ipv4-basic-2000] description This is an IPv4 basic ACL.

関連コマンド

display acl

1.1.6 display acl

Syntax

display acl [**ipv6** | **mac**] { *acl-number* | **all** | **name** *acl-name* }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ipv6: IPv6 ACL を指定します。

mac: L2 ACL を指定します。

acl-number: ACL の番号を指定します。以下に設定範囲を示します。

- 2000～2999：標準 ACL です。

- 3000～3999：拡張 ACL です。
- 4000～4999：L2 ACL です。**mac** の指定が必要です。

all: すべての ACL を指定します。

name *acl-name*: ACL 名を指定します。設定範囲は 1～63 です。大文字、小文字は区別しません。最初の文字は英字を使用する必要があります。

説明

display acl コマンドは ACL の設定と一致する統計情報を表示します。

ACL ルールの順番が設定されたとき、このコマンドは **config** あるいは **auto** で表示します。

IPv4 ACL を指定する場合、**ipv6** パラメータあるいは **mac** パラメータを指定しないでください。

例

標準 IPv4 ACL 2001 の設定と一致する統計情報を表示します。

<Switch> display acl 2001

```
Basic IPv4 ACL 2001, 1 rules, 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.
```

表 1-1 コマンド出力

フィールド	説明
Basic ACL 2001	ACLのカテゴリと番号です。フィールドの情報は標準IPv4 ACL 2001です。
1 rule	ACLは2つのルールがあることを示します。
match-order is auto	ACLの比較順序が**auto**です。深さ優先順序に従ってACLルールを比較します。比較順序が**config**である場合は表示されません。
This is an IPv4 basic ACL.	ACLの説明です。
ACL's step is 5	ルールのステップ数が5です。
start ID is 0	ルールIDの開始番号が0です。
rule 5 permit source 1.1.1.1 0	ルール5の内容です。IPアドレス1.1.1.1からのパケットを許可します。

フィールド	説明
5 times matched	ルールに5回一致しています。統計情報はソフトウェアで実行されたACLに一致した回数です。 ルールに一致していない場合、フィールドは表示されません。
rule 5 comment This rule is used on GigabitEthernet 1/0/1.	ACLルール5の説明です。

1.1.7 display packet-filter

Syntax

display packet-filter { **interface** [*interface-type interface-number*] [**inbound** | **outbound**] | **interface** *vlan-interface vlan-interface-number* [**inbound** | **outbound**] [**slot** *slot-number*] }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface [*interface-type interface-number*]: インタフェースのタイプと番号を指定します。VLAN インタフェースはサポートしていません。インタフェースを指定しない場合、パケットフィルタリングの VLAN インタフェースを除くすべての ACL の情報を表示します。

interface vlan-interface *vlan-interface-number*: VLAN インタフェースの番号を指定します。

inbound: インタフェースで受信されたパケットを指定します。

outbound: インタフェースで送信されたパケットを指定します。

slot *slot-number*: IRF スタックメンバ装置を指定します。*slot-number* は IRF スタックメンバ装置の ID を示します。指定しない場合、IRF スタックユニットのマスタ装置のパケットフィルタリングの ACL 情報を表示します。

説明

display packet-filter コマンドはパケットフィルタリングを行うために ACL がインタフェースに正常に適用されたかどうかを表示します。

inbound パラメータと **outbound** パラメータのいずれも設定しない場合、受信パケットと送信パケットの両方でパケットフィルタリングを行う ACL が適用された状態を表示します。

例

GigabitEthernet 1/0/1 で受信されたパケットフィルタリングの ACL の情報を示します。

<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, Hardware-count (Failed)
  IPv4 ACL 2004, Hardware-count (Failed)
  IPv4 default action: Deny
```

表 1-2 コマンド出力

フィールド	説明
Interface	ACLが適用されるインタフェースです。
Inbound policy	受信トラフィックのフィルタリングに使用されるACLです。
Outbound policy	送信トラフィックのフィルタリングに使用されるACLです。
IPv4 ACL 2001	標準IPv4 ACL 2001が正常に適用されています。
IPv6 ACL 2002 (Failed)	標準IPv6 ACL 2002が適用されていません。
Hardware-count	正常にACLルールに一致した回数をカウントするようにします。
Hardware-count (Failed)	ACLルールに一致した回数をカウントすることに失敗しました。
IPv4 default action	パケットフィルタリングのIPv4 ACLに一致しないデフォルトアクションです。 • **Deny**—デフォルトアクション**deny**がパケットフィルタリングに正常に適用されました。 • **Deny (Failed)**—パケットフィルタリングのデフォルトアクション**deny**が適用されていません。アクションは**permit**のみです。 • **Permit**—デフォルトアクション**permit**がパケットフィルタリングに正常に適用されました。

フィールド	説明
IPv6 default action	パケットフィルタリングのIPv6 ACLに一致しないデフォルトアクションです。 • **Deny**—デフォルトアクション**deny**がパケットフィルタリングに正常に適用されました。 • **Deny (Failed)**—パケットフィルタリングのデフォルトアクション**deny**が適用されていません。アクションは**permit**のみです。 • **Permit**—デフォルトアクション**permit**がパケットフィルタリングに正常に適用されました。
MAC default action	パケットフィルタリングのL2 ACLに一致しないデフォルトアクションです。 • **Deny**—デフォルトアクション**deny**がパケットフィルタリングに正常に適用されました。 • **Deny (Failed)**—パケットフィルタリングのデフォルトアクション**deny**が適用されていません。アクションは**permit**のみです。 • **Permit**—デフォルトアクション**permit**がパケットフィルタリングに正常に適用されました。

1.1.8 display packet-filter statistics

Syntax

display packet-filter statistics interface *interface-type interface-number* { **inbound** | **outbound** } [[**ipv6** | **mac**] { *acl-number* | **name** *acl-name* }] [**brief**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: タイプと番号を指定したインタフェースの統計情報を表示します。

inbound: インタフェースで受信されたパケットの統計情報を表示します。

outbound: インタフェースで送信されたパケットの統計情報を表示します。

ipv6: IPv6 ACL を指定します。

mac: L2 ACL を指定します。

acl-number: ACL の番号を指定します。以下に設定範囲を示します。

- 2000～2999：標準 ACL です。
- 3000～3999：拡張 ACL です。
- 4000～4999：L2 ACL です。**mac** の指定が必要です。

name *acl-name*: ACL 名を指定します。設定範囲は 1～63 です。大文字、小文字は区別しません。最初の文字は英字を使用する必要があります。

brief: 統計情報の概要を表示します。

説明

display packet-filter statistics コマンドはパケットフィルタリングの ACL に一致する統計情報を表示します。

acl-number パラメータ、**name** *acl-name* パラメータ、**ipv6** パラメータ、**mac** パラメータが指定されていない場合、パケットフィルタリングのすべての ACL に一致する統計情報を表示します。

IPv4 ACL を指定する場合、**ipv6** パラメータあるいは **mac** パラメータを指定しないでください。

例

GigabitEthernet 1/0/1 でパケットフィルタリングのすべての ACL に一致する統計情報を表示します。

<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

  IPv4 ACL 2002 (Failed)

  MAC ACL 4000
   From 2011-06-04 10:25:34 to 2011-06-04 10:35:57
   rule 0 permit

  IPv6 ACL 2000

  IPv4 default action: Deny
```

```
MAC default action: Deny
```

表 1-3 コマンド出力

フィールド	説明
Interface	ACLが適用されるインタフェースです。
Inbound policy	受信トラフィックのフィルタリングに使用されるACLです。
Outbound policy	送信トラフィックのフィルタリングに使用されるACLです。
IPv4 ACL 2001	標準IPv4 ACL 2001が正常に適用されています。
IPv4 ACL 2002 (Failed)	標準IPv4 ACL 2002が適用されていません。
Hardware-count	正常にACLルールに一致した回数をカウントするようにします。
Hardware-count (Failed)	ACLルールに一致した回数をカウントすることに失敗しました。
From 2011-06-04 10:25:21 to 2011-06-04 10:35:57	統計情報の開始時間と終了時間です。
2 packets	2つのパケットがルールに一致します。 パケットがルールに一致しない場合、表示されません。
No resource	ルールのカウントに必要なリソースが十分ではありません。パケットフィルタリングの統計情報では、ルールに一致させるためのリソースが十分でない場合、表示されます。
rule 5 permit source 1.1.1.1 0 (Failed)	ルール5の適用に失敗しました。
Totally 2 packets permitted, 0 packets denied	ACLによって許可、拒否されたパケット数です。
Totally 100% permitted, 0% denied	すべてのパケットに対する許可、拒否されたパケットの割合です。
IPv4 default action	パケットフィルタリングのIPv4 ACLに一致しないデフォルトアクションです。 • **Deny**—デフォルトアクション**deny**がパケットフィルタリングに正常に適用されました。 • **Deny (Failed)**—パケットフィルタリングのデフォルトアクション**deny**が適用されていません。アクションは**permit**のみです。 • **Permit**—デフォルトアクション**permit**がパケットフィルタリングに正常に適用されました。

フィールド	説明
IPv6 default action	パケットフィルタリングのIPv6 ACLに一致しないデフォルトアクションです。 • **Deny**—デフォルトアクション**deny**がパケットフィルタリングに正常に適用されました。 • **Deny (Failed)**—パケットフィルタリングのデフォルトアクション**deny**が適用されていません。アクションは**permit**のみです。 • **Permit**—デフォルトアクション**permit**がパケットフィルタリングに正常に適用されました。
MAC default action	パケットフィルタリングのL2 ACLに一致しないデフォルトアクションです。 • **Deny**—デフォルトアクション**deny**がパケットフィルタリングに正常に適用されました。 • **Deny (Failed)**—パケットフィルタリングのデフォルトアクション**deny**が適用されていません。アクションは**permit**のみです。 • **Permit**—デフォルトアクション**permit**がパケットフィルタリングに正常に適用されました。
Totally 7 packets	デフォルトアクションが7つのパケットで実行されました。

関連コマンド

reset packet-filter statistics

1.1.9 display packet-filter statistics sum

Syntax

display packet-filter statistics sum { **inbound** | **outbound** } [**ipv6** | **mac**] { *acl-number* | **name** *acl-name* } [**brief**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

inbound: インタフェースで受信されたパケットの統計情報の累積を表示します。

outbound: インタフェースで送信されたパケットの統計情報の累積を表示します。

ipv6: IPv6 ACL を指定します。

mac: L2 ACL を指定します。

acl-number: ACL の番号を指定します。以下に設定範囲を示します。

- 2000～2999：標準 ACL です。
- 3000～3999：拡張 ACL です。
- 4000～4999：L2 ACL です。**mac** の指定が必要です。

name *acl-name*: ACL 名を指定します。設定範囲は 1～63 です。大文字、小文字は区別しません。最初の文字は英字を使用する必要があります。

brief: 統計情報の概要を表示します。

説明

display packet-filter statistics コマンドはパケットフィルタリングの ACL に一致する統計情報の累積を表示します。

IPv4 ACL を指定する場合、**ipv6** パラメータあるいは **mac** パラメータを指定しないでください。

例

受信パケットのパケットフィルタリングの標準 IPv4 ACL 2001 に一致する統計情報の累積を表示します。

<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
```

受信パケットのパケットフィルタリングの標準 IPv4 ACL 2000 に一致する統計情報の累積の概要を表示します。

<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
```

表 1-4 コマンド出力

フィールド	説明
Sum	パケットフィルタリングのACLに一致する累積統計情報です。
Inbound policy	受信トラフィックのフィルタリングに使用されるACLの統計情報の累積です。
Outbound policy	送信トラフィックのフィルタリングに使用されるACLの統計情報の累積です。
IPv4 ACL 2001	標準IPv4 ACL 2001の統計情報の累積です。
2 packets	2つのパケットがルールに一致しました。 このフィールドはルールに一致しない場合、表示されません。
Totally 2 packets permitted, 0 packets denied	ACLによって許可、拒否されたパケット数です。
Totally 100% permitted, 0% denied	すべてのパケットに対する許可、拒否されたパケットの割合です。

関連コマンド

reset packet-filter statistics

1.1.10 display packet-filter verbose

Syntax

display packet-filter verbose interface *interface-type interface-number* { **inbound** | **outbound** } [[**ipv6** | **mac**] { *acl-number* | **name** *acl-name* }] [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: タイプと番号を指定したインタフェースを指定します。Ethernet インタフェースは **slot** パラメータが無効です。

inbound: インタフェースで受信されたパケットを指定します。

outbound: インタフェースで送信されたパケットを指定します。

ipv6: IPv6 ACL を指定します。

mac: L2 ACL を指定します。

acl-number: ACL の番号を指定します。以下に設定範囲を示します。

- 2000～2999：標準 ACL です。
- 3000～3999：拡張 ACL です。
- 4000～4999：L2 ACL です。**mac** の指定が必要です。

name *acl-name*: ACL 名を指定します。設定範囲は 1～63 です。大文字、小文字は区別しません。最初の文字は英字を使用する必要があります。

slot *slot-number*: IRF スタックメンバ装置を指定します。*slot-number* は IRF スタックメンバ装置の ID を示します。指定しない場合、IRF スタックユニットのマスタのパケットフィルタリングの ACL の詳細情報を表示します。

説明

display packet-filter verbose コマンドはパケットフィルタリングの ACL の詳細情報を表示します。

acl-number パラメータ、**name** *acl-name* パラメータ、**ipv6** パラメータ、**mac** パラメータが指定されていない場合、パケットフィルタリングのすべての ACL に一致する詳細情報を表示します。

IPv4 ACL を指定する場合、**ipv6** パラメータあるいは **mac** パラメータを指定しないでください。

例

GigabitEthernet 1/0/1 でパケットフィルタリングのすべての ACL の詳細情報を表示します。

<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)

  IPv4 ACL 2002 (Failed)

  IPv6 ACL 2000
   rule 0 permit

  MAC ACL 4000

  IPv4 default action: Deny

  IPv6 default action: Deny
```

```
MAC default action: Deny
```

表 1-5 コマンド出力

フィールド	説明
Interface	ACLが適用されるインタフェースです。
Inbound policy	受信トラフィックのフィルタリングに使用されるACLです。
Outbound policy	送信トラフィックのフィルタリングに使用されるACLです。
IPv4 ACL 2001	標準IPv4 ACL 2001が正常に適用されています。
IPv4 ACL 2002 (Failed)	標準IPv4 ACL 2002が適用されていません。
Hardware-count	正常にACLルールに一致した回数をカウントするようにします。
Hardware-count (Failed)	ACLルールに一致した回数をカウントすることに失敗しました。
rule 5 permit source 1.1.1.1 0 (Failed)	ルール5の適用に失敗しました。
IPv4 default action	パケットフィルタリングのIPv4 ACLに一致しないデフォルトアクションです。 • **Deny**—デフォルトアクション**deny**がパケットフィルタリングに正常に適用されました。 • **Deny (Failed)**—パケットフィルタリングのデフォルトアクション**deny**が適用されていません。アクションは**permit**のみです。 • **Permit**—デフォルトアクション**permit**がパケットフィルタリングに正常に適用されました。
IPv6 default action	パケットフィルタリングのIPv6 ACLに一致しないデフォルトアクションです。 • **Deny**—デフォルトアクション**deny**がパケットフィルタリングに正常に適用されました。 • **Deny (Failed)**—パケットフィルタリングのデフォルトアクション**deny**が適用されていません。アクションは**permit**のみです。 • **Permit**—デフォルトアクション**permit**がパケットフィルタリングに正常に適用されました。

フィールド	説明
MAC default action	パケットフィルタリングのL2 ACLに一致しないデフォルトアクションです。 • **Deny**—デフォルトアクション**deny**がパケットフィルタリングに正常に適用されました。 • **Deny (Failed)**—パケットフィルタリングのデフォルトアクション**deny**が適用されていません。アクションは**permit**のみです。 • **Permit**—デフォルトアクション**permit**がパケットフィルタリングに正常に適用されました。

1.1.11 display qos-acl resource

Syntax

display qos-acl resource [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

slot *slot-number*: IRF スタックメンバ装置を指定します。*slot-number* は IRF スタックメンバ装置の ID を示します。指定しない場合、IRF スタックユニットのすべてのメンバ装置の QoS と ACL のリソースの使用状況を表示します。

説明

display qos-acl resource コマンドは QoS と ACL のリソースの使用状況を表示します。

QoS および ACL リソースが十分でない場合、以下の機能を使用することができません。機能を使用する場合、QoS および ACL リソースを十分に確保してください。

- パケットフィルタリング
- 装置のログイン
- 802.1X
- MAC アドレス認証

例

QoS と ACL のリソースの使用状況を表示します。

<Switch> display qos-acl resource

```
Interfaces: GE1/0/1 to GE1/0/24, XGE1/0/25 to XGE1/0/28 (slot 1)
------------------------------------------------------------------------
 Type           Total     Reserved   Configured Remaining  Usage
------------------------------------------------------------------------
 TTI ACL        1024      0          1          1023       0%
 PCL ACL        1536      11         0          1525       0%
 PCL Counter    2704      11         0          2693       0%
 IPCL Meter     1792      0          0          1792       0%
 EPCL Meter     512       0          0          512        0%
```

表 1-6 コマンド出力

フィールド	説明
Interfaces	リソースのインタフェース範囲です。
Type	リソースタイプです。 • **TTI ACL**–インタフェースで使用されるACLのリソースです。QinQ、VLANマッピング、mac-vlanなどで使用されます。 • **PCL ACL**–ポリシーで使用されるACLのリソースです。プロトコルパケット、ACLを参照するアプリケーションモジュールによって使用されるリソースが含まれます。 • PCL Counter–ポリシーで使用されるアカウンティングリソースです。 • IPCL Meter–inboundのQoSポリシーで使用されるトラフィックポリシングリソースです。 • EPCL Meter—outboundのQoSポリシーで使用されるトラフィックポリシングリソースです。
Total	リソースの総数です。
Reserved	予約されたリソース数です。
Configured	適用されたリソース数です。
Remaining	適用可能なリソース数です。
Usage	リソースの総数に対する設定されたリソースと予約済みリソース数の割合です。 割合が整数でない場合、整数部分のみ表示します。たとえば、正確な割合が50.8%である場合、50%と表示されます。

1.1.12 packet-filter

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** }

デフォルト

設定なし

View

Layer 2 Ethernet interface view

VLAN interface view

定義済みユーザロール

network-admin

パラメータ

ipv6: IPv6 ACL を指定します。

mac: L2 ACL を指定します。

acl-number: ACL の番号を指定します。以下に設定範囲を示します。

- 2000～2999：標準 ACL です。
- 3000～3999：拡張 ACL です。
- 4000～4999：L2 ACL です。**mac** の指定が必要です。

name *acl-name*: ACL 名を指定します。設定範囲は 1～63 です。大文字、小文字は区別しません。最初の文字は英字を使用する必要があります。

inbound: インタフェースで受信されるパケットをフィルタします。

outbound: インタフェースで送信されるパケットをフィルタします。

hardware-count: ハードウェアで実行される ACL ルールに一致した回数をカウントするようにします。指定しない場合、ACL ルールに一致する回数はカウントしません。

説明

packet-filter コマンドはパケットをフィルタするため、インタフェースに ACL を適用します。

undo packet-filter コマンドはインタフェースから ACL を削除します。

IPv4 ACL を指定する場合、**ipv6** パラメータあるいは **mac** パラメータを指定しないでください。

hardware-count パラメータを使用した場合、ACL のすべてのルールをカウントします。**rule** コマンドの **counting** パラメータはルールに一致する回数をカウントするようにします。

インタフェースの同一方向に対して、最大 3 つの ACL（1 つの標準 IPv4 ACL、1 つの標準 IPv4 ACL、1 つの L2 ACL）を適用することができます。

VLAN インタフェースでフィルタリングを設定した場合、別の VLAN インタフェースに転送される場合にのみフィルタされます。

メモ：

VLAN インタフェースには同じ方向のパケットフィルタを設定できません。設定がある場合は、先に元の設定を削除してください。
同じ方向のパケットフィルタを設定してエラーが表示された場合は、display packet-filter verbose コマンドで正常に適用されていない ACL を確認できます。

例

GigabitEthernet 1/0/1 に受信トラフィックをフィルタするため、標準 IPv4 ACL 2001 を適用し、ハードウェアで実行された ACL ルールに一致する回数をカウントするようにします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] packet-filter 2001 inbound hardware-count

関連コマンド

- **display packet-filter**
- **display packet-filter statistics**
- **display packet-filter verbose**

1.1.13 packet-filter filter

Syntax

packet-filter filter [**route** | **all**]

undo packet-filter filter

デフォルト

全てのパケット

View

VLAN interface view

定義済みユーザロール

network-admin

パラメータ

route: レイヤ 3 で VLAN インタフェースが転送したパケットをフィルタします。

all: レイヤ 3 で VLAN インタフェースが転送したパケットとレイヤ 2 で VLAN インタフェースに関連付けられた物理ポートが転送したパケットを含む、すべてのパケットをフィルタします。

説明

packet-filter filter コマンドは VLAN インタフェース上でパケットフィルタリングの適用範囲を指定します

undo packet-filter filter コマンドはデフォルトに戻します。

例

VLAN インタフェース 2 でパケットフィルタリングを設定して、レイヤ 3 で転送されるパケットをフィルタします。

<Switch> system-view

[Switch] interface vlan-interface 2

[Switch-Vlan-interface2] packet-filter filter route

1.1.14 reset acl counter

Syntax

reset acl [**ipv6** | **mac**] **counter** { *acl-number* | **all** | **name** *acl-name* }

View

User view

定義済みユーザロール

network-admin

パラメータ

ipv6: IPv6 ACL を指定します。

mac: L2 ACL を指定します。

acl-number: ACL の番号を指定します。以下に設定範囲を示します。

- 2000～2999：標準 ACL です。
- 3000～3999：拡張 ACL です。
- 4000～4999：L2 ACL です。**mac** の指定が必要です。

all: すべての ACL の統計情報を削除します。

name *acl-name*: ACL 名を指定します。設定範囲は 1～63 です。大文字、小文字は区別しません。

説明

reset acl counter コマンドは ACL の統計情報を削除します。

例

標準 IPv4 ACL 2001 の統計情報を削除します。

<Switch> reset acl counter 2001

関連コマンド

display acl

1.1.15 reset packet-filter statistics

Syntax

reset packet-filter statistics interface [*interface-type interface-number*] { **inbound** | **outbound** } [[**ipv6** | **mac**] { *acl-number* | **name** *acl-name* }]

View

User view

定義済みユーザロール

network-admin

パラメータ

interface [*interface-type interface-number*]: インタフェースのタイプと番号を指定します。指定しない場合、すべてのインタフェースのパケットフィルタリングの統計情報を削除します。

inbound: インタフェースで受信されたパケットを指定します。

outbound: インタフェースで送信されたパケットを指定します。

ipv6: IPv6 ACL を指定します。

mac: L2 ACL を指定します。

acl-number: ACL の番号を指定します。以下に設定範囲を示します。

- 2000～2999：標準 ACL です。
- 3000～3999：拡張 ACL です。
- 4000～4999：L2 ACL です。**mac** の指定が必要です。

name *acl-name*: ACL 名を指定します。設定範囲は 1～63 です。大文字、小文字は区別しません。最初の文字は英字を使用する必要があります。

説明

reset packet-filter statistics コマンドはパケットフィルタリングの ACL に一致する統計情報を削除します。この統計情報は累積された統計情報を含みます。

acl-number パラメータ、**name** *acl-name* パラメータ、**ipv6** パラメータ、**mac** パラメータが指定されていない場合、パケットフィルタリングのすべての ACL に一致する統計情報を削除します。

IPv4 ACL を指定する場合、**ipv6** パラメータあるいは **mac** パラメータを指定しないでください。

例

GigabitEthernet 1/0/1 でパケットフィルタリングの標準 IPv4 ACL 2001 の統計情報を削除します。

<Switch> reset packet-filter statistics interface gigabitethernet 1/0/1 inbound 2001

関連コマンド

- **display packet-filter statistics**
- **display packet-filter statistics sum**

1.1.16 rule (IPv4 advanced ACL view)

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 port1* [*port2*] | { **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 port1* [*port2*] | **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 port1* [*port2*] | { **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 port1* [*port2*] | **time-range** *time-range-name*] *

デフォルト

設定なし

View

IPv4 advanced ACL view

定義済みユーザロール

network-admin

パラメータ

rule-id: ルール ID を指定します。設定範囲は 0～65534 です。ACL ルールを作成するとき、ルール ID を指定しない場合、システムは自動でルール ID を割り当てます。0 から始まり現在のもっとも大きいルール ID より大きなステップの最小倍数をルールに割り当てます。たとえば、ステップが 5 のときに、現在のもっとも大きいルール ID が 28 の場合、ルールに 30 の番号を割り当てます。

deny: 一致するパケットを拒否します。

permit: 一致するパケットを許可します。

protocol: プロトコル番号あるいはプロトコル名を指定します。

- プロトコル番号の設定範囲は 0～255 です。
- プロトコル名は **gre** (47)、**icmp** (1)、**igmp** (2)、**ip**、**ipinip** (4)、**ospf** (89)、**tcp** (6)、**udp** (17)を指定できます。**ip** はすべてのプロトコルを指定します。表 1-7 にプロトコルの値に関わらず指定できるパラメータを示します。

表 1-7 拡張 IPv4 ACL ルールの一致基準と他のルールの情報

パラメータ	機能	説明
source { *source-address source-wildcard* | **any** }	送信元アドレスを定義します。	*source-address*と*source-wildcard*はドットで区切られた10進数表記の送信元IPアドレスとワイルドカードマスクを示します。すべてが0のワイルドカードはホストアドレスを示します。**any**は、任意の送信元IPアドレスを示します。
destination { *dest-address dest-wildcard* | **any** }	宛先アドレスを定義します。	*dest-address*と*dest-wildcard*はドットで区切られた10進数表記の宛先IPアドレスとワイルドカードマスクを示します。すべてが0のワイルドカードはホストアドレスを示します。**any**は、任意の宛先IPアドレスを示します。
counting	拡張IPv4 ACLルールが一致した回数をカウントします。	**counting**は指定したルールに一致した回数をカウントし、**packet-filter**コマンドの**hardware-count**はACLのすべてのルールをカウントします。**counting**が指定されない場合、ルールはカウントしません。

パラメータ	機能	説明
precedence *precedence*	IPプレシーデンスの値を指定します。	プレシーデンスの値あるいはプレシーデンスの名前を指定します。番号の設定範囲は0～7です。名前は**routine** (0)、**priority** (1)、**immediate** (2)、**flash** (3)、**flash-override** (4)、**critical** (5)、**internet** (6)、**network** (7)が指定できます。
tos *tos*	ToSプレシーデンスを指定します。	プレシーデンスの値あるいはプレシーデンスの名前を指定します。番号の設定範囲は0～15です。名前は**max-reliability** (2)、**max-throughput** (4)、**min-delay** (8)、**min-monetary-cost** (1)、**normal** (0)が指定できます。
dscp *dscp*	DSCPプライオリティを指定します。	*dscp*プライオリティの値あるいはプライオリティの名前を指定します。番号の設定範囲は0～63です。名前は**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)、**ef** (46)が指定できます。
fragment	最初のフラグメントではないフラグメントを指定します。	指定しない場合、ルールはすべてのフラグメントと非フラグメントを適用します。
logging	パケットに一致するログを指定します。	この機能はACLがloggingをサポートするモジュール（たとえばパケットフィルタリング）が必要です。
time-range *time-range-name*	ルールのタイムレンジを指定します。	*time-range-name*の設定範囲は1～32文字です。大文字、小文字を区別しません。最初の文字は英字を使用する必要があります。タイムレンジが設定されていない場合、システムはルールを作成しますが、タイムレンジを設定した後、タイムレンジを使用したルールが適用されます。タイムレンジの詳細は、オペレーションマニュアルのセクション8 *ACL and QoS*”*タイムレンジ*”を参照してください。

*protocol*が**tcp** (6)あるいは**udp** (7)である場合、設定するパラメータを表 1-8に示します。

表 1-8 拡張 IPv4 ACL ルールの TCP/UDP 指定パラメータ

パラメータ	機能	説明
source-port *operator port1* [*port2*]	1つまたは複数のTCP/UDPの送信元ポート番号を指定します。	*operator*は**lt** (lower than)、**gt** (greater than)、**eq** (equal to)、**neq** (not equal to)、**range** (inclusive range)が指定できます。*port1*、*port2*はTCPあるいはUDPポート番号です。設定範囲は0～65535です。*port2*は*operator*が範囲であるときのみ必要です。 TCPポート番号は以下の名前で指定できます。**chargen** (19)、**bgp** (179)、**cmd** (514)、**daytime** (13)、**discard** (9)、**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)、**www** (80) UDPポート番号は以下の名前で指定できます **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)、**xdmcp** (177)
destination-port *operator port1* [*port2*]	1つまたは複数のTCP/UDPの宛先ポート番号を指定します。	
{ **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } *	ACK、FIN、PSH、RST、SYN、URGを含む1つまたは複数のTCPフラグを指定します。	TCP用のパラメータです。各値は0(フラグビットがセットされていません)または1(フラグビットがセットされています)が指定できます。ルールのTCPフラグはANDの関係です。たとえば、ack 0 psh 1が設定されたルールはACKフラグが設定されておらず、PSHフラグが設定されているパケットに一致します。
established	TCP接続の確立状態を示すフラグを指定します。	TCP用のパラメータです。ルールはACKあるいはRSTフラグがセットされているTCP接続パケットに一致します。

protocol が **icmp** (1)である場合、設定するパラメータを表 1-9 に示します。

表 1-9 拡張 IPv4 ACL ルールの ICMP 指定パラメータ

パラメータ	機能	説明
icmp-type { **icmp-type** *icmp-code* | *icmp-message* }	ICMPメッセージタイプとコードを指定します。	*icmp-type*の設定範囲は0～255です。*icmp-code*の設定範囲は0～255です。*icmp-message*はメッセージの名前を指定します。サポートされるICMPメッセージ名と対応するタイプとコードの値を表 1-10に示します。

表 1-10 拡張 IPv4 ACL ルールでサポートされる ICMP メッセージ名

ICMP メッセージ名	ICMP メッセージタイプ	ICMP メッセージコード
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
port-unreachable	3	3
protocol-unreachable	3	2
reassembly-timeout	11	1
source-quench	4	0
source-route-failed	3	5

ICMP メッセージ名	ICMP メッセージタイプ	ICMP メッセージコード
timestamp-reply	14	0
timestamp-request	13	0
ttl-exceeded	11	0

説明

rule コマンドは拡張 IPv4 ACL のルールを作成あるいは修正します。

undo rule コマンドは拡張 IPv4 ACL ルールを削除あるいはルールから属性を削除します。

ACL で各ルールの **permit** あるいは **deny** は固有にする必要があります。別のルールと同一の **deny** あるいは **permit** がある ACL のルールを作成あるいは修正する場合、ルールは作成あるいは修正することができません。

一致の順番が **config** であるときのみ ACL ルールを修正することができます。

標準 IPv4 ACL、拡張 IPv4 ACL のルールとルールの ID を表示する場合、**display acl all** コマンドを使用します。

すべてのパラメータを指定しない場合、**undo rule** *rule-id* コマンドはすべてのルールを削除します。パラメータを指定した場合、**undo rule** *rule-id* コマンドは指定した属性を削除します。

undo rule { **deny** | **permit** }コマンドはルール全体を削除するためにのみ使用します。コマンドのルールのすべての属性を指定する必要があります。

例

アドレス 129.9.0.0/16 から 202.38.160.0/24 の宛先ポート 80 の TCP パケットを許可する拡張 IPv4 ACL ルールを作成します。

<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

192.168.1.0/24 宛の ICMP パケットを除くすべての IP パケットを許可する拡張 IPv4 ACL ルールを作成します。

<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

FTP の送受信パケットを許可する拡張 IPv4 ACL ルールを作成します。

<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

SNMP と SNMP trap の送受信パケットを許可する拡張 IPv4 ACL ルールを作成します。

<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

関連コマンド

- **acl**
- **acl logging interval**
- **display acl**
- **step**
- **time-range**

1.1.17 rule (IPv4 basic ACL view)

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*] *

デフォルト

設定なし

View

IPv4 basic ACL view

定義済みユーザロール

network-admin

パラメータ

rule-id: ルール ID を指定します。設定範囲は 0～65534 です。ACL ルールを作成するとき、ルール ID を指定しない場合、システムは自動でルール ID を割り当てます。0 から始まり現在のもっとも大きいルール ID より大きなステップの最小倍数をルールに割り当てます。たとえば、ステップが 5 のときに、現在のもっとも大きいルール ID が 28 の場合、ルールに 30 の番号を割り当てます。

deny: 一致するパケットを拒否します。

permit: 一致するパケットを許可します。

counting: 標準 IPv4 ACL ルールが一致した回数をカウントします。指定しない場合、ルールをカウントしません。

fragment: 最初のフラグメントではないフラグメントを指定します。指定しない場合、ルールはすべてのフラグメントと非フラグメントを適用します。

logging: パケットに一致するログを指定します。この機能は ACL が logging をサポートするモジュール（たとえばパケットフィルタリング）が必要です。

source { *source-address source-wildcard* | **any** }: 送信元アドレスを定義します。*source-address* と *source-wildcard* はドットで区切られた 10 進数表記の送信元 IP アドレスとワイルドカードマスクを示します。すべてが 0 のワイルドカードはホストアドレスを示します。**any** は、任意の送信元 IP アドレスを示します。

time-range *time-range-name*: ルールのタイムレンジを指定します。*time-range-name* の設定範囲は 1～32 文字です。大文字、小文字を区別しません。最初の文字は英字を使用する必要があります。タイムレンジが設定されていない場合、システムはルールを作成しますが、タイムレンジを設定した後、タイムレンジを使用したルールが適用されます。タイムレンジの詳細は、オペレーションマニュアルのセクション 8 *ACL and QoS*”*タイムレンジ*”を参照してください。

説明

rule コマンドは標準 IPv4 ACL のルールを作成あるいは修正します。

undo rule コマンドは標準 IPv4 ACL ルールを削除あるいはルールから属性を削除します。

ACL で各ルールの **permit** あるいは **deny** は固有にする必要があります。別のルールと同一の **deny** あるいは **permit** がある ACL のルールを作成あるいは修正する場合、ルールは作成あるいは修正することができません。

一致の順番が **config** であるときのみ ACL ルールを修正することができます。

counting パラメータを指定した場合、指定したルールに一致した回数をカウントし、**packet-filter** コマンドの **hardware-count** パラメータは ACL のすべてのルールをカウントします。

標準 IPv4 ACL、拡張 IPv4 ACL のルールとルールの ID を表示する場合、**display acl all** コマンドを使用します。

すべてのパラメータを指定しない場合、**undo rule** *rule-id* コマンドはすべてのルールを削除します。パラメータを指定した場合、**undo rule** *rule-id* コマンドは指定した属性を削除します。

undo rule { **deny** | **permit** }コマンドはルール全体を削除するためにのみ使用します。コマンドのルールのすべての属性を指定する必要があります。

例

アドレス 10.0.0.0/8、172.17.0.0/16、192.168.1.0/24 を除く送信元 IP セグメントからのパケットを拒否する標準 IPv4 ACL ルールを作成します。

<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

関連コマンド

- **acl**
- **acl logging interval**
- **display acl**
- **step**
- **time-range**

1.1.18 rule (IPv6 advanced ACL view)

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 port1* [*port2*] | **dscp** *dscp* | **flow-label** *flow-label-value* | **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 port1* [*port2*] | **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** | **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 port1* [*port2*] | **time-range** *time-range-name*] *

デフォルト

設定なし

View

IPv6 advanced ACL view

定義済みユーザロール

network-admin

パラメータ

rule-id: ルール ID を指定します。設定範囲は 0～65534 です。ACL ルールを作成するとき、ルール ID を指定しない場合、システムは自動でルール ID を割り当てます。0 から始まり現在のもっとも大きいルール ID より大きなステップの最小倍数をルールに割り当てます。たとえば、ステップが 5 のときに、現在のもっとも大きいルール ID が 28 の場合、ルールに 30 の番号を割り当てます。

deny: 一致するパケットを拒否します。

permit: 一致するパケットを許可します。

protocol: プロトコル番号あるいはプロトコル名を指定します。

- プロトコル番号の設定範囲は 0～255 です。
- プロトコル名は **gre** (47)、**icmpv6** (58)、**ipv6**、**ipv6-ah** (51)、**ipv6-esp** (50)、**ospf** (89)、**tcp** (6)、**udp** (17)があります。**ipv6** はすべてのプロトコルを指定します。

表 1-11 にプロトコルの値に関わらず指定できるパラメータを示します。

表 1-11 拡張 IPv6 ACL ルールの一致基準と他のルールの情報

パラメータ	機能	説明
source { *source-address source-prefix* | *source-address*/*source-prefix* | **any** }	送信元IPv6アドレスを指定します。	*dest-address*と*dest-prefix*は送信元IPv6アドレスとプレフィックス長を示します。プレフィックス長の範囲は1～128です。 **any**は、任意の送信元IPv6アドレスを示します。

パラメータ	機能	説明
destination { *dest-address* *dest-prefix* | *dest-address*/*dest-prefix* | **any** }	宛先IPv6アドレスを指定します。	*dest-address*と*dest-prefix*は宛先IPv6アドレスとプレフィックス長を示します。プレフィックス長の範囲は1～128です。 inboundフィルタの場合は、アドレスの先頭1バイトと末尾2バイトをフィルタします。 outboundフィルタの場合は、アドレスの先頭1バイトのみをフィルタします。 **any**は、任意の宛先IPv6アドレスを示します。
counting	拡張IPv6 ACLルールが一致した回数をカウントします。	**counting**は指定したルールに一致した回数をカウントし、**packet-filter ipv6**コマンドの**hardware-count**はACLのすべてのルールをカウントします。**counting**が指定されない場合、ルールはカウントしません。
dscp *dscp*	DSCPプライオリティを指定します。	*dscp*プライオリティの値あるいはプライオリティの名前を指定します。番号の設定範囲は0～63です。名前は**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)、**ef** (46). が指定できます。
flow-label *flow-label-value*	Pv6パケットヘッダのフローラベルを指定します。	*flow-label-value*の設定範囲は0～1048575です。
fragment	最初のフラグメントではないフラグメントを指定します。	指定しない場合、ルールはすべてのフラグメントと非フラグメントを適用します。
logging	パケットに一致するログを指定します。	この機能はACLがloggingをサポートするモジュール（たとえばパケットフィルタリング）が必要です。
routing [**type** *routing-type*]	IPv6ルーティングヘッダタイプを指定します。	*routing-type*: IPv6ルーティングヘッダタイプの値です。設定範囲は0～255です。 *routing-type*を指定する場合、ルールはIPv6ルーティングヘッダの指定されたタイプを適用します。そうでなければ、IPv6ルーティングヘッダのすべてのタイプを適用します。

パラメータ	機能	説明
time-range *time-range-name*	ルールのタイムレンジを指定します。	*time-range-name*の設定範囲は1～32文字です。大文字、小文字を区別しません。最初の文字は英字を使用する必要があります。タイムレンジが設定されていない場合、システムはルールを作成しますが、タイムレンジを設定した後、タイムレンジを使用したルールが適用されます。タイムレンジの詳細は、オペレーションマニュアルのセクション8 *ACL and QoS*”*タイムレンジ*”を参照してください。

protocol が **tcp** (6)あるいは **udp** (17)である場合、設定するパラメータを表 1-12 に示します。

表 1-12 拡張 IPv6 ACL ルールの TCP/UDP 指定パラメータ

パラメータ	機能	説明
source-port *operator port1* [*port2*]	1つまたは複数のTCP/UDPの送信元ポート番号を指定します。	*operator*は**lt** (lower than)、**gt** (greater than)、**eq** (equal to)、**neq** (not equal to)、**range** (inclusive range)が指定できます。*port1*、*port2*はTCPあるいはUDPポート番号です。設定範囲は0～65535です。*port2*は*operator*が範囲であるときのみ必要です。 TCPポート番号は以下の名前で指定できます。**chargen** (19)、**bgp** (179)、**cmd** (514)、**daytime** (13)、**discard** (9)、**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)、**www** (80) UDPポート番号は以下の名前で指定できます。**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)、**xdmcp** (177)
destination-port *operator port1* [*port2*]	1つまたは複数のTCP/UDPの宛先ポート番号を指定します。	

パラメータ	機能	説明
{ **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } *	ACK、FIN、PSH、RST、SYN、URGを含む1つまたは複数のTCPフラグを指定します。	TCPを特定するパラメータです。各値は0(フラグビットがセットされていません)または1(フラグビットがセットされています)が指定できます。ルールのTCPフラグはANDの関係です。たとえば、**ack** 0 **psh** 1 が設定されたルールはACKフラグが設定されておらず、PSHフラグが設定されているパケットに一致します。
established	TCP接続の確立状態を示すフラグを指定します。	TCP用のパラメータです。ルールはACKあるいはRSTフラグがセットされているTCP接続パケットに一致します。

protocol が **icmpv6** (58)である場合、設定するパラメータを表 1-13 に示します。

表 1-13 拡張 IPv6 ACL ルールの ICMPv6 指定パラメータ

パラメータ	機能	説明
icmp6-type { *icmp6-type icmp6-code* | *icmp6-message* }	ICMPv6メッセージタイプとコードを指定します。	*icmp6-type*の設定範囲は0～255です。*icmp6-code*の設定範囲は0～255です。*icmp6-message*はメッセージの名前を指定します。サポートされるICMPメッセージ名と対応するタイプとコードの値を表 1-14 に示します。

表 1-14 拡張 IPv6 ACL ルールでサポートされる ICMPv6 メッセージ名

ICMPv6 メッセージ名	ICMPv6 メッセージタイプ	ICMPv6 メッセージコード
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

ICMPv6 メッセージ名	ICMPv6 メッセージタイプ	ICMPv6 メッセージコード
neighbor-solicitation	135	0
network-unreachable	1	0
packet-too-big	2	0
port-unreachable	1	4
redirect	137	0
router-advertisement	134	0
router-solicitation	133	0
unknown-ipv6-opt	4	2
unknown-next-hdr	4	1

説明

rule コマンドは拡張 IPv6 ACL のルールを作成あるいは修正します。

undo rule コマンドは拡張 IPv6 ACL ルールを削除あるいはルールから属性を削除します。

ACL が QoS トラフィック分類あるいはパケットフィルタリング用である場合、**flow-label** パラメータを指定できません。

ACL がパケットフィルタリング用である場合、**fragment** パラメータを指定できません。

ACL で各ルールの **permit** あるいは **deny** は固有にする必要があります。別のルールと同一の **deny** あるいは **permit** がある ACL のルールを作成あるいは修正する場合、ルールは作成あるいは修正することができません。

一致の順番が **config** であるときのみ ACL ルールを修正することができます。

標準 IPv6 ACL、拡張 IPv6 ACL のルールとルールの ID を表示する場合、**display acl ipv6 all** コマンドを使用します。

すべてのパラメータを指定しない場合、**undo rule** *rule-id* コマンドはすべてのルールを削除します。パラメータを指定した場合、**undo rule** *rule-id* コマンドは指定した属性を削除します。

undo rule { **deny** | **permit** }コマンドはルール全体を削除するためにのみ使用します。コマンドのルールのすべての属性を指定する必要があります。

🕮 ポイント：

IPv6 アドレスのフィルタについて、destination の場合は、フィルタできるアドレスに条件があります。
条件については表 1-11 の destination の説明を参照ください。
具体的な設定例は以下を参照ください。

例

送信元アドレス 2030:5060::/64、宛先アドレス FE**::/8 の宛先ポート 80 の TCP パケットを許可する拡張 IPv6 ACL ルールを作成します。

#この IPv6 ACL ルールを inbound/outbound で指定した場合は、宛先アドレスに関しては、先頭が FE のアドレスがフィルタ対象となります。

<Switch> system-view

[Switch] acl ipv6 advanced 3000

[Switch-acl-ipv6-adv-3000] rule permit tcp source 2030:5060::/64 destination fe00::/8 destination-port eq 80

FE**::8F5C/128 宛の ICMPv6 パケットを除くすべての IPv6 パケットを許可する拡張 IPv6 ACL ルールを作成します。

#この IPv6 ACL ルールを inbound で指定した場合は、宛先アドレスの先頭が FE で、かつ末尾が BF5C のアドレスがフィルタ対象となります。

#この IPv6 ACL ルールを outbound で指定した場合は、宛先アドレスの先頭が FE のアドレスがフィルタ対象となります。

<Switch> system-view

[Switch] acl ipv6 advanced 3001

[Switch-acl-ipv6-adv-3001] rule deny icmpv6 destination fe00::bf5c 128

[Switch-acl-ipv6-adv-3001] rule permit ipv6

FTP の送受信パケットを許可する拡張 IPv6 ACL ルールを作成します。

<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

SNMP と SNMP trap の送受信パケットを許可する拡張 IPv6 ACL ルールを作成します。

<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

関連コマンド

- **acl**
- **acl logging interval**
- **display acl**
- **step**
- **time-range**

1.1.19 rule (IPv6 basic ACL view)

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*] *

デフォルト

設定なし

View

IPv6 basic ACL view

定義済みユーザロール

network-admin

パラメータ

rule-id: ルール ID を指定します。設定範囲は 0～65534 です。ACL ルールを作成するとき、ルール ID を指定しない場合、システムは自動でルール ID を割り当てます。0 から始まり現在のもっとも大きいルール ID より大きなステップの最小倍数をルールに割り当てます。たとえば、ステップが 5 のときに、現在のもっとも大きいルール ID が 28 の場合、ルールに 30 の番号を割り当てます。

deny: 一致するパケットを拒否します。

permit: 一致するパケットを許可します。

counting: 標準 IPv6 ACL ルールが一致した回数をカウントします。**counting** が指定されない場合、ルールはカウントしません。

fragment: 最初のフラグメントではないフラグメントを指定します。指定しない場合、ルールはすべてのフラグメントと非フラグメントを適用します。

logging: パケットに一致するログを指定します。この機能は ACL が logging をサポートするモジュール（たとえばパケットフィルタリング）が必要です。

routing [**type** *routing-type*]: 指定したタイプあるいはすべてのルーティングヘッダのルールを指定します。*routing-type* はルーティングヘッダのタイプの値を指定します。設定範囲は 0～255 です。指定しない場合、すべてのタイプのルーティングヘッダのルールを適用します。

source { *source-address source-prefix* | *source-address*/*source-prefix* | **any** }: 送信元 IPv6 アドレスを指定します。*source-address* と *source-prefix* は送信元 IPv6 アドレスとプレフィックス長を示します。プレフィックス長の範囲は 1～128 です。**any** は、任意の送信元 IPv6 アドレスを示します。

time-range *time-range-name*: ルールのタイムレンジを指定します。*time-range-name* の設定範囲は 1～32 文字です。大文字、小文字を区別しません。最初の文字は英字を使用する必要があります。タイムレンジが設定されていない場合、システムはルールを作成しますが、タイムレンジを設定した後、タイムレンジを使用したルールが適用されます。タイムレンジの詳細は、オペレーションマニュアルのセクション 8 *ACL and QoS*”*タイムレンジ*”を参照してください。

説明

rule コマンドは標準 IPv6 ACL のルールを作成あるいは修正します。

undo rule コマンドは標準 IPv6 ACL ルールを削除あるいはルールから属性を削除します。

ACL で各ルールの **permit** あるいは **deny** は固有にする必要があります。別のルールと同一の **deny** あるいは **permit** がある ACL のルールを作成あるいは修正する場合、ルールは作成あるいは修正することができません。

一致の順番が **config** であるときのみ ACL ルールを修正することができます。

counting パラメータを指定した場合、指定したルールに一致した回数をカウントし、**packet-filter ipv6** コマンドの **hardware-count** パラメータは ACL のすべてのルールをカウントします。

標準 IPv6 ACL、拡張 IPv6 ACL のルールとルールの ID を表示する場合、**display acl ipv6 all** コマンドを使用します。

すべてのパラメータを指定しない場合、**undo rule** *rule-id* コマンドはすべてのルールを削除します。パラメータを指定した場合、**undo rule** *rule-id* コマンドは指定した属性を削除します。

undo rule { **deny** | **permit** }コマンドはルール全体を削除するためにのみ使用します。コマンドのルールのすべての属性を指定する必要があります。

例

アドレス 1001::/16, 3124:1123::/32 あるいは FE80:5060:1001::/48 を除く送信元 IP セグメントからのパケットを拒否する標準 IPv6 ACL ルールを作成します。

<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

関連コマンド

- **acl**
- **acl logging interval**
- **display acl**
- **step**
- **time-range**

1.1.20 rule (Layer 2 ACL view)

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*] *

デフォルト

設定なし

View

Layer 2 ACL view

定義済みユーザロール

network-admin

パラメータ

rule-id: ルール ID を指定します。設定範囲は 0～65534 です。ACL ルールを作成するとき、ルール ID を指定しない場合、システムは自動でルール ID を割り当てます。0 から始まり現在のもっとも大きいルール ID より大きなステップの最小倍数をルールに割り当てます。たとえば、ステップが 5 のときに、現在のもっとも大きいルール ID が 28 の場合、ルールに 30 の番号を割り当てます。

deny: 一致するパケットを拒否します。

permit: 一致するパケットを許可します。

cos *dot1p*: 802.1p プライオリティを定義します。

- プライオリティの設定範囲は 0～7 です。
- **best-effort** (0)、**background** (1)、**spare** (2)、**excellent-effort** (3)、**controlled-load** (4)、**video** (5)、**voice** (6)、**network-management** (7)の用語で定義することができます。

counting: L2 ACL ルールが一致した回数をカウントします。**counting** が指定しない場合、ルールはカウントしません。

dest-mac *dest-address dest-mask*: 宛先 MAC アドレス範囲を定義します。*dest-address* と *dest-mask* は宛先 MAC アドレスとマスクを示します。マスクの形式は H-H-H です。

lsap *lsap-type lsap-type-mask*: LLC カプセル化の DSAP と SSAP フィールドを定義します。*lsap-type* は 16 進数表記でカプセル化フォーマットを示します。*lsap-type* の設定範囲は 0～ffff です。*lsap-type-mask* は 16 進数表記で LSAP マスクを示します。*lsap-type-mask* の設定範囲は 0～ffff です。

type *protocol-type protocol-type-mask*: L2 の 1 つ以上のプロトコルを定義します。*protocol-type* は 16 進数表記で Ethernet_II と Ethernet_SNAP のプロトコルタイプを示します。*protocol-type* の設定範囲は 0～ffff です。*protocol-type-mask* は 16 進数表記でプロトコルタイプのマスクを示します。*protocol-type-mask* の設定範囲は 0～ffff です。

source-mac *source-address source-mask*: 送信元 MAC アドレス範囲を定義します。*source-address* は送信元 MAC アドレスを示します。*sour-mask* はマスクを示します。マスクの形式は H-H-H です。

time-range *time-range-name*: ルールのタイムレンジを指定します。*time-range-name* の設定範囲は 1～32 文字です。大文字、小文字を区別しません。最初の文字は英字を使用する必要があります。タイムレンジが設定されていない場合、システムはルールを作成しますが、タイムレンジを設定した後、タイムレンジを使用したルールが適用されます。タイムレンジの詳細は、オペレーションマニュアルのセクション 8 *ACL and QoS*”*タイムレンジ*”を参照してください。

説明

rule コマンドは L2 ACL のルールを作成あるいは修正します。

undo rule コマンドは L2 ACL ルールを削除あるいはルールから属性を削除します。

ACL で各ルールの **permit** あるいは **deny** は固有にする必要があります。別のルールと同一の **deny** あるいは **permit** がある ACL のルールを作成あるいは修正する場合、ルールは作成あるいは修正することができません。

一致の順番が **config** であるときのみ ACL ルールを修正することができます。

counting パラメータを指定した場合、指定したルールに一致した回数をカウントし、**packet-filter** コマンドの **hardware-count** パラメータは ACL のすべてのルールをカウントします。

L2 ACL のルールとルールの ID を表示する場合、**display acl all** コマンドを使用します。

すべてのパラメータを指定しない場合、**undo rule** *rule-id* コマンドはすべてのルールを削除します。パラメータを指定した場合、**undo rule** *rule-id* コマンドは指定した属性を削除します。

undo rule { **deny** | **permit** }コマンドはルール全体を削除するためにのみ使用します。コマンドのルールのすべての属性を指定する必要があります。

例

L2 ACL 4000 のルールを作成します。ARP パケットを許可し、RARP パケットを拒否します。

<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

関連コマンド

- **acl**
- **display acl**
- **step**
- **time-range**

1.1.21 rule comment

Syntax

rule *rule-id* **comment** *text*

undo rule *rule-id* **comment**

デフォルト

設定なし

View

IPv4 basic/advanced ACL view

IPv6 basic/advanced ACL view

Layer 2 ACL view

定義済みユーザロール

network-admin

パラメータ

rule-id: ACL のルール ID を指定します。設定範囲は 0～65534 です。ACL のルールはすでに作成されている必要があります。

text: ACL のルールの説明を指定します。設定範囲は 1～127 文字です。大文字、小文字を区別します。

説明

rule comment コマンドは ACL のルールの説明を設定します。

undo rule comment コマンドは ACL のルールの説明を削除します。

ルールに説明がない場合、ルールに説明を追加します。すでにルールに説明がある場合、ルールの説明を修正します。

例

標準 IPv4 ACL 2000 を作成し、ルールの説明を追加します。

<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.

関連コマンド

display acl

1.1.22 step

Syntax

step *step-value*

undo step

デフォルト

5

View

IPv4 basic/advanced ACL view

IPv6 basic/advanced ACL view

Layer 2 ACL view

定義済みユーザロール

network-admin

パラメータ

step-value: ACL ルールのステップ数を指定します。設定範囲は 1～20 です。

説明

step コマンドは ACL ルールに自動的に番号を割り振るためのステップ数を設定します。

undo step コマンドはデフォルトに戻します。

ルールの番号づけステップはシステムが自動的にルール番号の増分を設定します。たとえば、デフォルトの ACL の番号づけステップは 5 です。ルールを作成するとき、ID を割り当てない場合、ルールの番号は 0、5、10、15、...と番号づけられます。番号づけのステップを広くする場合、2 つのルールの間に多くのルールを挿入することができます。ステップを変更したときはいつでも、ルールは 0 から再ナンバリングが行われます。たとえば、5 つのルールの番号 5、10、13、15、20 がつけられている場合、ステップを 5 から 2 に変更すると、ルールの番号は 0、2、4、6、8 に再ナンバリングされます。

例

標準 IPv4 ACL 2000 のステップ数を 2 に設定します。

<Switch> system-view

[Switch] acl basic 2000

[Switch-acl-ipv4-basic-2000] step 2

関連コマンド

display acl

目次

このセクションのページは **8-x-x** です。

2 章 QoS ポリシー..... 2-1
2.1 トラフィッククラス設定コマンド..... 2-1
2.1.1 description..... 2-1
2.1.2 display traffic classifier..... 2-1
2.1.3 if-match..... 2-3
2.1.4 traffic classifier..... 2-8
2.2 トラフィック動作設定コマンド..... 2-9
2.2.1 accounting..... 2-9
2.2.2 car..... 2-10
2.2.3 display traffic behavior..... 2-12
2.2.4 filter..... 2-13
2.2.5 nest top-most..... 2-14
2.2.6 redirect..... 2-15
2.2.7 remark dot1p..... 2-16
2.2.8 remark dscp..... 2-18
2.2.9 remark local-precedence..... 2-19
2.2.10 remark service-vlan-id..... 2-20
2.2.11 traffic behavior..... 2-21
2.3 QoS ポリシー設定コマンド..... 2-22
2.3.1 classifier behavior..... 2-22
2.3.2 display qos policy..... 2-23
2.3.3 display qos policy global..... 2-24
2.3.4 display qos policy interface..... 2-26
2.3.5 display qos policy user-profile..... 2-30
2.3.6 display qos vlan-policy..... 2-32
2.3.7 qos apply policy (interface view)..... 2-33
2.3.8 qos apply policy (user profile view)..... 2-35
2.3.9 qos apply policy global..... 2-36
2.3.10 qos policy..... 2-36
2.3.11 qos vlan-policy..... 2-37
2.3.12 reset qos policy global..... 2-38
2.3.13 reset qos vlan-policy..... 2-39

2章 QoS ポリシー

2.1 トラフィッククラス設定コマンド

2.1.1 description

Syntax

description *text*

undo description

デフォルト

設定なし

View

Traffic class view

定義済みユーザロール

network-admin

パラメータ

text: 説明を指定します。設定範囲は 1～127 文字です。大文字と小文字を区別します。

説明

description コマンドはトラフィッククラスの説明を設定します。

undo description コマンドはデフォルトに戻します。

このコマンドを複数回実行すると、最新の設定が有効になります。

例

トラフィッククラス **class1** の **classifier** として説明を設定します。

<Switch> system-view

[Switch] traffic classifier class1

[Switch-classifier-class1] description classifier

2.1.2 display traffic classifier

Syntax

display traffic classifier user-defined [*classifier-name*] [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

user-defined: ユーザ定義のクラスを表示します。

classifier-name: トラフィッククラスを指定します。設定範囲は 1～31 文字です。指定しない場合、すべてのトラフィッククラスを表示します。

slot *slot-number*: IRF スタックメンバ装置を指定します。*slot-number* は IRF スタックメンバ装置の ID を示します。指定しない場合、マスタ装置のトラフィッククラスを表示します。

説明

display traffic classifier コマンドはトラフィッククラスを表示します。

例

ユーザ定義のすべてのトラフィッククラスを表示します。

<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-
```

表 2-1 コマンド出力

フィールド	説明
Classifier	トラフィッククラス名と一致条件です。
Operator	トラフィッククラスが一致したときの動作です。動作がANDであるとき、トラフィッククラスはすべての一致条件に一致するパケットにマッチします。動作がORであるとき、トラフィッククラスはいずれかの一致条件に一致するパケットにマッチします。
Rule(s)	一致条件です。

2.1.3 if-match

Syntax

if-match *match-criteria*

undo if-match *match-criteria*

デフォルト

設定なし

View

Traffic class view

定義済みユーザロール

network-admin

パラメータ

match-criteria: 一致条件を指定します。表 2-2 に使用可能な一致条件を示します。

表 2-2 使用可能な一致条件

オプション	説明
acl [**ipv6**] { *acl-number* | **name** *acl-name* }	ACLでマッチするように指定します。 *acl-number*は、ACL番号でACLを指定します。 ● IPv4 ACLの設定範囲は2000～3999です。 ● IPv6 ACLの設定範囲は2000～3999です。 ● L2 ACLの設定範囲は4000～4999です。 *acl-name*は、ACL名でACLを指定します。設定範囲は1～63文字です。大文字、小文字を区別しません。文字列の最初は英字を指定します。混乱をさけるため**all**を使用してはいけません。
any	すべてのパケットにマッチするように指定します。
destination-mac *mac-address*	指定した宛先MACアドレスのパケットにマッチするよう指定します。
dscp *dscp-value*&<1-8>	DSCP値あるいはキーワードでマッチするように指定します。*dscp-value*は、設定範囲が0～63のDSCP値のリストです。&<1-8>を使用して最大8つまでDSCP値を設定できます。*dscp-value*のキーワードを表 2-3に示します。
ip-precedence *ip-precedence-value*&<1-8>	パケットのIPプレシーデンスにマッチするよう指定します。*ip-precedence-value*は、設定範囲が0～7のIPプレシーデンス値のリストです。&<1-8>を使用して最大8つのIPプレシーデンス値を指定できます。
protocol *protocol-name*	指定したプロトコルのパケットにマッチするように指定します。*protocol-name*はIP、IPv6が指定できます。
service-dot1p *dot1p-value*&<1-8>	外部VLANタグの802.1pプライオリティにマッチするように指定します。*dot1p-value*は、設定範囲が0～7の802.1pプライオリティ値のリストです。&<1-8>を使用して最大8つの802.1pプライオリティ値を指定できます。
service-vlan-id *vlan-id-list*	外部VLANタグのVLAN IDのパケットにマッチするように指定します。*vlan-id-list*は*vlan-id-list* = { *vlan-id* | *vlan-id1* **to** *vlan-id2* }&<1-10>でVALN IDの設定範囲が1～4094でVLAN IDを最大10個までのリストです。*vlan-id1*～vlan-id2は、VALN IDの設定範囲を指定します。*vlan-id1*は、*vlan-id2*よりも小さくなければなりません。&<1-10>を使用して最大10のVALN IDあるいはVLAN IDの範囲を指定できます。
source-mac *mac-address*	指定した送信元MACアドレスのパケットにマッチするよう指定します。

表 2-3 DSCP のキーワードと値

キーワード	DSCP 値（バイナリ）	DSCP 値（10 進数）
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
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

説明

if-match コマンドは一致条件を定義します。

undo if-match コマンドは一致条件を削除します。

複数の一致条件の **if-match** コマンドを作成する場合、クラスの演算子を OR に設定し、複数の **if-match** コマンドを使用して設定してください。

1 つの **if-match** コマンドで複数の条件を設定する場合、以下の制限とガイドラインに従ってください。

- 1 つの **if-match** コマンドで以下の一致条件を使用して最大 8 つまで指定することができます。
  - 802.1p プライオリティ
  - DSCP
  - IP プレシーデンス
  - VLAN ID
- 指定した値の 1 つが一致した場合、**if-match** コマンドに一致します。
- 1 つの **if-match** コマンドに設定された複数の条件を削除する場合、**undo if-match** コマンドで指定する値は **if-match** コマンドで指定された値と同一にする必要があります。設定した順番は異なっていても構いません。

ACL ベースの条件を設定する場合、以下の制限とガイドラインに従ってください。

- **if-match** コマンドに参照される ACL が存在しない場合、トラフィッククラスはハードウェアに適用することができません。
- 一致条件として同じ ACL を使用する **if-match** コマンドを 2 つ追加できます。1 つのコマンドで、名前で ACL を指定します。もう一方のコマンドで、番号で ACL を指定します。
- ACL ルールは分類のみ使用できます。permit/deny アクションに使用した場合、無視されます。パケットに一致するアクションはトラフィック動作で定義されます。

クラスの一致条件を定義するため論理積 AND、論理和 OR の両方を使用することができます。たとえば、以下のようにトラフィッククラス classA の 3 つの一致条件の関係を定義することができます。

traffic classifier classB operator and

if-match *match-criteria*1

if-match *match-criteria* 2

traffic classifier classA operator or

if-match *match-criteria* 3

例

宛先 MAC アドレスが 0050-ba27-bed3 のパケットのマッチングを行うように、トラフィッククラス class1 に一致条件を定義します。

<Switch> system-view

[Switch] traffic classifier class1

[Switch-classifier-class1] if-match destination-mac 0050-ba27-bed3

送信元 MAC アドレスが 0050-ba27-bed2 のパケットのマッチングを行うように、トラフィッククラス class2 に一致条件を定義します。

<Switch> system-view

[Switch] traffic classifier class2

[Switch-classifier-class2] if-match source-mac 0050-ba27-bed2

外部 VLAN タグの 802.1p プライオリティが 5 のパケットのマッチングを行うように、トラフィッククラス class1 の一致条件を定義します。

<Switch> system-view

[Switch] traffic classifier class1

[Switch-classifier-class1] if-match service-dot1p 5

拡張 ACL 3101 のマッチングを行うように、トラフィッククラス class1 に一致条件を定義します。

<Switch> system-view

[Switch] traffic classifier class1

[Switch-classifier-class1] if-match acl 3101

ACL 名が flow の ACL のマッチングを行うように、トラフィッククラス class1 に一致条件を定義します。

<Switch> system-view

[Switch] traffic classifier class1

[Switch-classifier-class1] if-match acl name flow

拡張 IPv6 ACL 3101 のマッチングを行うように、トラフィッククラス class1 に一致条件を定義します。

<Switch> system-view

[Switch] traffic classifier class1

[Switch-classifier-class1] if-match acl ipv6 3101

ACL 名が flow の拡張 IPv6 ACL のマッチングを行うように、トラフィッククラス class1 に一致条件を定義します。

<Switch> system-view

[Switch] traffic classifier class1

[Switch-classifier-class1] if-match acl ipv6 name flow

すべてのパケットのマッチングを行うように、トラフィッククラス class1 に一致条件を定義します。

<Switch> system-view

[Switch] traffic classifier class1

[Switch-classifier-class1] if-match any

DSCP が 1、6、9 のパケットのマッチングを行うように、トラフィッククラス class1 に一致条件を定義します。

<Switch> system-view

[Switch] traffic classifier class1

[Switch-classifier-class1] if-match dscp 1 6 9

IP プレシーデンスが 1、6 のパケットのマッチングを行うように、トラフィッククラス class1 に一致条件を定義します。

<Switch> system-view

[Switch] traffic classifier class1

[Switch-classifier-class1] if-match ip-precedence 1 6

IP パケットのマッチングを行うように、トラフィッククラス class1 に一致条件を定義します。

<Switch> system-view

[Switch] traffic classifier class1

[Switch-classifier-class1] if-match protocol ip

外部 VLAN タグの VLAN ID が 2、7、10 のパケットのマッチングを行うように、トラフィッククラス class1 に一致条件を定義します。

<Switch> system-view

[Switch] traffic classifier class1

[Switch-classifier-class1] if-match service-vlan-id 2 7 10

2.1.4 traffic classifier

Syntax

traffic classifier *classifier-name* [**operator** { **and** | **or** }]

undo traffic classifier *classifier-name*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

classifier-name: トラフィッククラスを指定します。設定範囲は 1～31 文字です。

operator: トラフィッククラスの論理積 AND あるいは論理和 OR を指定するオペレータを設定します。デフォルトは論理積 AND です。

and: 論理積 AND を指定します。トラフィッククラスはすべての条件に一致したパケットのみマッチングします。

or: 論理和 OR を指定します。トラフィッククラスはいずれかの条件に一致したパケットのみマッチングします。

説明

traffic classifier コマンドはトラフィッククラスを作成し、traffic class view に移行します。

undo traffic classifier コマンドはトラフィッククラスを削除します。

例

トラフィッククラス class1 を作成します。

<Switch> system-view

[Switch] traffic classifier class1

[Switch-classifier-class1]

関連コマンド

display traffic classifier

2.2 トラフィック動作設定コマンド

2.2.1 accounting

Syntax

accounting { **byte** | **packet** }

undo accounting

デフォルト

設定なし

View

Traffic behavior view

定義済みユーザロール

network-admin

パラメータ

byte: トラフィックをバイトでカウントします。

packet: トラフィックをパケットでカウントします。

説明

accounting コマンドはトラフィック動作にトラフィックのアカウンティングアクションを設定します。

undo accounting コマンドはトラフィック動作からトラフィックのアカウンティングアクションを削除します。

QoS ポリシーがグローバルで設定されている場合、QoS ポリシーのアカウンティングアクションは適用されません。

例

トラフィックをバイトでカウントするトラフィック動作 database のトラフィックのアカウンティングアクションを設定します。

<Switch> system-view

[Switch] traffic behavior database

[Switch-behavior-database] accounting byte

2.2.2 car

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

デフォルト

設定なし

View

Traffic behavior view

定義済みユーザロール

network-admin

パラメータ

cir *committed-information-rate*: 平均トラフィックレートを指定する CIR（認定情報レート）を kbps 単位で指定します。設定範囲は 8～160000000 です。8 の整数倍で設定します。

cbs *committed-burst-size*: CBS（認定バーストサイズ）を byte 単位で指定します。設定範囲は 512～256000000 です。512 の整数倍で設定します。デフォルトは 512 と CIR の

積で、512 の整数倍にする必要があります。62.5 と CIR の積が 512 の整数倍でない場合、積より大きい値で、512 にもっとも近い値になります。256000000 バイトを超えることはできません。超えた場合、256000000 バイトとなります。

ebs *excess-burst-size*: EBS（最大許容バーストサイズ）をバイト単位で指定します。設定範囲は 0～256000000 です。512 の整数倍で設定します。PIR が設定されている場合、デフォルトは 62.5 と PIR の積です。512 の整数倍で設定します。積が 512 の整数倍でない場合、積より大きい値で、512 の整数倍にもっとも近い値となります。デフォルトは 256000000 より大きい場合、256000000 となります。

pir *peak-information-rate*: PIR（最大情報速度）を kbps 単位で指定します。設定範囲は 8～160000000 です。8 の整数倍で設定します。

green *action*: CIR に対応するパケットに対して実施されるアクションを指定します。デフォルトはパケットを転送します。

red *action*: CIR および PIR のどちらにも対応しないパケットに対して実施されるアクションを指定します。デフォルトはパケットを廃棄します。

yellow *action*: PIR に対応し、CIR に対応しないパケットに対して実施されるアクションを指定します。デフォルトはパケットを転送します。

action: パケットに対して実施されるアクションを指定します。

- **discard**: パケットを廃棄します。
- **pass**: パケットを転送します。
- **remark-dot1p-pass** *new-cos*: 802.1p のパケットに *new-cos* を追加し、パケット転送を許可します。設定範囲は 0～7 です。
- **remark-dscp-pass** *new-dscp*: DSCP のパケットに *new-dscp* を追加し、パケット転送を許可します。設定範囲は 0～63 です。
- **remark-lp-pass** *new-local-precedence*: ローカル優先順位のパケットに *new-local-precedence* を追加し、パケット転送を許可します。設定範囲は 0～7 です。

説明

car コマンドはトラフィック動作に CAR アクションを設定します。

undo car コマンドはトラフィック動作から CAR アクションを削除します。

トラフィックポリシーで 2 つのレートを使用するには、**pir** *peak-information-rate* パラメータを指定し、**car** コマンドを設定してください。トラフィックポリシーで 1 つのレートを使用するには、**pir** *peak-information-rate* パラメータを指定しないで **car** コマンドを設定してください。

同一のトラフィック動作に **car** コマンドを複数設定した場合、最後に行った設定が適用されます。

例

トラフィック動作に CAR アクションを以下のように設定します。

- CIR を 200kbps、CBS を 51200 バイト、EBS を 0 に設定します。

- 一致するパケットの通過を許可し、DSCP プレシーデンス 0 で超過パケットをマーキングし、転送します。

<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

Syntax

display traffic behavior user-defined [*behavior-name*] [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

user-defined: ユーザ定義のトラフィック動作を表示します。

behavior-name: トラフィック動作を指定します。設定範囲は 1～31 文字です。大文字、小文字を区別します。指定しない場合、すべてのトラフィック動作を表示します。

slot *slot-number*: IRF スタックメンバ装置を指定します。*slot-number* は IRF スタックメンバ装置の ID を示します。指定しない場合、マスタ装置のトラフィック動作を表示します。

説明

display traffic behavior コマンドはトラフィック動作を表示します。

例

すべてのユーザ定義のトラフィック動作を表示します。

<Switch> display traffic behavior user-defined

```
User-defined behavior information:

  Behavior: 1 (ID 100)
    Marking:
      Remark dscp 3
    Committed Access Rate:
```

```
    CIR 200 (kbps), CBS 51200 (Bytes), EBS 512 (Bytes)
    Green action  : pass
    Yellow action : pass
    Red action    : discard

Behavior: 2 (ID 101)
  Accounting enable: Packet
  Filter enable: Permit
  Marking:
    Remark dscp 4
  Redirecting:
    Redirect to the CPU
```

表 2-4 コマンド出力

フィールド	説明
Behavior	トラフィック動作の名前と内容です。
Marking	プライオリティマーキングの情報です。
Remark dscp	DSCP値をパケットに設定するアクションです。
Committed Access Rate	CARアクションの情報です。
Green action	greenパケットを適用するアクションです。
Yellow action	yellowパケットを適用するアクションです。
Red action	redパケットを適用するアクションです。
Accounting enable	トラフィックアカウンティングアクションです。
Filter enable	トラフィックフィルタリングアクションです。
Redirecting	トラフィックリダイレクティングの情報です。
Mirroring	トラフィックミラーリングの情報です。
Pre	IPプレシーデンスです。

2.2.4 filter

Syntax

filter { **deny** | **permit** }

undo filter

デフォルト

設定なし

View

Traffic behavior view

定義済みユーザロール

network-admin

パラメータ

deny: パケットを廃棄します。

permit: パケットを転送します。

説明

filter コマンドはトラフィック動作にトラフィックフィルタリングを設定します。

undo filter コマンドはトラフィック動作からトラフィックフィルタリングを削除します。

例

トラフィック動作 database にパケットを廃棄するトラフィックフィルタリングを設定します。

<Switch> system-view

[Switch] traffic behavior database

[Switch-behavior-database] filter deny

2.2.5 nest top-most

Syntax

nest top-most vlan *vlan-id*

undo nest top-most

デフォルト

設定なし

View

Traffic behavior view

定義済みユーザロール

network-admin

パラメータ

vlan *vlan-id*: 追加される VLAN タグの ID を指定します。設定範囲は 1～4094 です。

説明

nest top-most コマンドはトラフィック動作に VLAN タグを追加するアクションを設定します。

undo nest top-most コマンドはデフォルトに戻します。

QoS ポリシーに外部 VLAN タグを追加するアクションが含まれる場合、インタフェースの入力トラフィックにのみ適用されます。

同一のトラフィック動作に **nest top-most** コマンドを複数回行った場合、最後に行った設定が適用されます。

例

トラフィック動作 b1 に VLAN タグ 123 を追加するアクションを設定します。

<Switch> system-view

[Switch] traffic behavior b1

[Switch-behavior-b1] nest top-most vlan 123

2.2.6 redirect

Syntax

redirect { **cpu** | **interface** *interface-type interface-number* }

undo redirect { **cpu** | **interface** *interface-type interface-number* }

デフォルト

設定なし

View

Traffic behavior view

定義済みユーザロール

network-admin

パラメータ

cpu: CPU にトラフィックをリダイレクトします。

interface *interface-type interface-number*: インタフェースにトラフィックをリダイレクトします。インタフェースのタイプと番号を指定します。

説明

redirect コマンドはトラフィック動作にトラフィックリダイレクティングアクションを設定します。

undo redirect コマンドはトラフィックリダイレクティングアクションを削除します。

同一のトラフィック動作に **redirect** コマンドを複数回行った場合、最後に行った設定が適用されます。

QoS ポリシーが入力トラフィックであるときのみ、トラフィックリダイレクティングアクションが適用されます。

アクセスポートにトラフィックをリダイレクトする場合、QoS ポリシーが適用されるインタフェースの PVID がアクセスポートの PVID と同一であることを確認してください。そうでない場合、アクセスポートはリダイレクトしたパケットを廃棄します。

トランクポートにトラフィックをリダイレクトする場合、QoS ポリシーが適用されるインタフェースの PVID がトランクポートで許可された VLAN リストにあることを確認してください。そうでない場合、トランクポートはリダイレクトしたパケットを廃棄します。

ユーザ定義に適用された QoS ポリシーがリダイレクトインタフェースアクションを含む場合、インタフェースとパケットの入力インタフェースが同一 VLAN であることを確認してください。

例

トラフィック動作 database で GigabitEthernet 1/0/1 にトラフィックをリダイレクトするように設定します。

<Switch> system-view

[Switch] traffic behavior database

[Switch-behavior-database] redirect interface gigabitethernet 1/0/1

関連コマンド

- **classifier behavior**
- **qos policy**
- **traffic behavior**

2.2.7 remark dot1p

Syntax

remark [**green** | **red** | **yellow**] **dot1p** *dot1p-value*

undo remark [**green** | **red** | **yellow**] **dot1p**

remark dot1p customer-dot1p-trust

undo remark dot1p

デフォルト

設定なし

View

Traffic behavior view

定義済みユーザロール

network-admin

パラメータ

green: green パケットを指定します。

red: red パケットを指定します。

yellow: yellow パケットを指定します。

dot1p-value: パケットに設定する 802.1p プライオリティを指定します。設定範囲は 0～7 です。

customer-dot1p-trust: インタフェースに QoS ポリシーが適用されたのち、内部 VLAN タグの 802.1p プライオリティを外部 VLAN タグにコピーします。

説明

remark dot1p コマンドはトラフィック動作に 802.1p プライオリティマーキングアクションを設定する、あるいは内部 VLAN タグから外部 VLAN タグにコピーするアクションを設定します。

undo remark dot1p コマンドはアクションを削除します。

remark dot1p *dot1p-value* コマンドと **remark dot1p customer-dot1p-trust** コマンドは同時に設定することができません。最後に行った設定が適用されます。

remark dot1p customer-dot1p-trust コマンドは 1 つのタグがつけられたパケットに適用されません。

例

トラフィック動作 database に 802.1p プライオリティを 2 に設定するアクションを設定します。

<Switch> system-view

[Switch] traffic behavior database

[Switch-behavior-database] remark dot1p 2

トラフィック動作に内部 VLAN タグから外部 VLAN タグにコピーするアクションを設定します。

<Switch> system-view

[Switch] traffic behavior database

[Switch-behavior-database] remark dot1p customer-dot1p-trust

2.2.8 remark dscp

Syntax

remark [**green** | **red** | **yellow**] **dscp** *dscp-value*

undo [**green** | **red** | **yellow**] **remark dscp**

デフォルト

設定なし

View

Traffic behavior view

定義済みユーザロール

network-admin

パラメータ

green: green パケットを指定します。

red: red パケットを指定します。

yellow: yellow パケットを指定します。

dscp-value: DSCP 値あるいは DSCP のキーワードを指定します。DSCP 値の設定範囲は 0～63 です。DSCP のキーワードを表 2-5 に示します。

表 2-5 DSCP のキーワードと値

キーワード	DSCP 値（バイナリ）	DSCP 値（10 進数）
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

キーワード	DSCP 値（バイナリ）	DSCP 値（10 進数）
af41	100010	34
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

説明

remark dscp コマンドはトラフィック動作に DSCP マーキングアクションを設定します。

undo remark dscp コマンドは DSCP マーキングアクションを削除します。

例

トラフィック動作の DSCP を 6 にするアクションを設定します。

<Switch> system-view

[Switch] traffic behavior database

[Switch-behavior-database] remark dscp 6

2.2.9 remark local-precedence

Syntax

remark local-precedence *local-precedence-value*

undo remark local-precedence

デフォルト

設定なし

View

Traffic behavior view

定義済みユーザロール

network-admin

パラメータ

local-precedence-value: パケットに設定するローカルプレシーデンスを指定します。設定範囲は 0～7 です。

説明

remark local-precedence コマンドはトラフィック動作にローカルプレシーデンスアクションを設定します。

undo remark local-precedence コマンドはアクションを削除します。

例

トラフィック動作にローカルプレシーデンスを 2 にするアクションを設定します。

<Switch> system-view

[Switch] traffic behavior database

[Switch-behavior-database] remark local-precedence 2

🕮 **メモ：**

1 つの traffic behavior view で local-precedence と dot1p のリマークは併用できません。

2.2.10 remark service-vlan-id

Syntax

remark service-vlan-id *vlan-id*

undo remark service-vlan-id

デフォルト

設定なし

View

Traffic behavior view

定義済みユーザロール

network-admin

パラメータ

vlan-id: 外部 VLAN ID を指定します。設定範囲は 1～4094 です。

説明

remark service-vlan-id コマンドはトラフィック動作に外部 VLAN マーキングアクションを設定します。

undo remark service-vlan-id コマンドはトラフィック動作からアクションを削除します。

例

トラフィック動作 b1 に外部 VLAN ID 222 をマーキングするアクションを設定します。

<Switch> system-view

[Switch] traffic behavior b1

[Switch-behavior-b1] remark service-vlan-id 222

2.2.11 traffic behavior

Syntax

traffic behavior *behavior-name*

undo traffic behavior *behavior-name*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

behavior-name: トラフィック動作を設定します。設定範囲は 1～31 です。

説明

traffic behavior コマンドはトラフィック動作を作成し、traffic behavior view に移行します。すでにトラフィック動作がある場合、その view に移行します。

undo traffic behavior コマンドはトラフィック動作を削除します。

例

トラフィック動作 behavior1 を作成します。

<Switch> system-view

[Switch] traffic behavior behavior1

[Switch-behavior-behavior1]

関連コマンド

display traffic behavior

2.3 QoSポリシー設定コマンド

2.3.1 classifier behavior

Syntax

classifier *classifier-name* **behavior** *behavior-name* [**insert-before** *before-classifier-name*]

undo classifier *classifier-name*

デフォルト

設定なし

View

QoS policy view

定義済みユーザロール

network-admin

パラメータ

classifier-name: トラフィッククラスを指定します。設定範囲は 1～31 文字です。大文字、小文字を区別します。

behavior-name: トラフィック動作を指定します。設定範囲は 1～31 文字です。大文字、小文字を区別します。

insert-before *before-classifier-name*: QoS ポリシーで設定済のトラフィッククラスの前に新しいトラフィッククラスを挿入します。**insert-before** *before-classifier-name* パラメータを指定しない場合、新しいトラフィッククラスは QoS ポリシーの最後に書き込まれます。

説明

classifier behavior コマンドはトラフィック動作を QoS ポリシーのトラフィッククラスに関連づけます。

undo classifier コマンドは QoS ポリシーからトラフィッククラスを削除します。

QoS ポリシーのトラフィッククラスは 1 つのトラフィック動作にのみ関連づけることができます。

指定したトラフィッククラスあるいはトラフィック動作が存在しない場合、システムは null のトラフィッククラスまたはトラフィック動作を作成します。

例

トラフィック動作 test を QoS ポリシーuser1 のトラフィッククラス database に関連づけます。

<Switch> system-view

[Switch] qos policy user1

[Switch-qospolicy-user1] classifier database behavior test

関連コマンド

qos policy

2.3.2 display qos policy

Syntax

display qos policy user-defined [*policy-name* [**classifier** *classifier-name*]] [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

user-defined: ユーザ定義の QoS ポリシーを表示します。

policy-name: QoS ポリシー名を指定します。設定範囲は 1～31 文字です。大文字、小文字を区別します。指定しない場合、すべてのユーザ定義の QoS ポリシーを表示します。

classifier *classifier-name*: トラフィッククラス名を指定します。設定範囲は 1～31 文字です。大文字、小文字を区別します。指定しない場合、すべてのトラフィッククラスを表示します。

slot *slot-number*: IRF スタックメンバ装置を指定します。*slot-number* は IRF スタックメンバ装置の ID を示します。指定しない場合、IRF スタックユニットのマスタ装置の QoS ポリシーを表示します。

説明

display qos policy コマンドは QoS ポリシーを表示します。

例

すべてのユーザ定義の QoS ポリシーを表示します。

<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-
```

コマンド出力は表 2-1、表 2-4 を参照してください。

2.3.3 display qos policy global

Syntax

display qos policy global [**slot** *slot-number*] [**inbound** | **outbound**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

inbound: 受信方向にグローバルで適用された QoS ポリシーを表示します。

outbound: 送信方向にグローバルで適用された QoS ポリシーを表示します。

slot *slot-number*: IRF スタックメンバ装置を指定します。*slot-number* は IRF スタックメンバ装置の ID を示します。指定しない場合、IRF スタックユニットのマスタ装置のグローバルに適用された QoS ポリシーを表示します。

説明

display qos policy global コマンドはグローバルで適用された QoS ポリシーを表示します。

方向を指定しない場合、**inbound** と **inbound** の両方のグローバルで適用された QoS ポリシーの情報を表示します。

例

グローバルで適用された QoS ポリシーを表示します。

<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-
```

表 2-6 コマンド出力

フィールド	説明
Direction	QoSポリシーが適用された方向（受信あるいは送信）です。
Green packets	greenパケットの統計情報です。
Yellow packets	yellowパケットの統計情報です。
Red packets	redパケットの統計情報です。

その他のコマンド出力は表 2-1、表 2-4 を参照してください。

2.3.4 display qos policy interface

Syntax

display qos policy interface [*interface-type interface-number*] [**inbound** | **outbound**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface-type interface-number: インタフェースのタイプと番号を指定します。

inbound: 受信トラフィックに適用された QoS ポリシーを表示します。

outbound: 送信トラフィックに適用された QoS ポリシーを表示します。

説明

display qos policy interface コマンドはインタフェースに適用された QoS ポリシーを表示します。

方向を指定しない場合、**inbound** と **inbound** の両方のトラフィックの QoS ポリシーを表示します。

例

GigabitEthernet 1/0/1 の受信方向のトラフィックに適用された QoS ポリシーを表示します。

<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-
```

すべてのインタフェースに適用された QoS ポリシーを表示します。

<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)
```

表 2-7 コマンド出力

フィールド	説明
Direction	インタフェースに適用されたQoSポリシーの方向です。
Matched	パケットに一致した数です。
Forwarded	統計収集期間以内に正常に転送された一致しているパケットの平均レートです。
Dropped	統計収集期間以内に廃棄された一致しているパケットの平均レートです。
Green packets	greenパケットのトラフィックの統計情報です。
Yellow packets	yellowパケットのトラフィックの統計情報です。
Red packets	redパケットのトラフィックの統計情報です。

その他のコマンド出力は表 2-1、表 2-4 を参照してください。

2.3.5 display qos policy user-profile

Syntax

display qos policy user-profile [**name** *profile-name*] [**user-id** *user-id*] [**slot** *slot-number*] [**inbound** | **outbound**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

name *profile-name:* ユーザプロファイル名を指定します。設定範囲は 1～31 文字です。大文字と小文字を区別します。有効な文字は、英字、数字、下線 (_)です。名前は英字で始まり、固有のものである必要があります。指定しない場合、すべてのユーザプロファイルに適用される QoS ポリシーを表示します。

user-id *user-id:* システム割り当ての 16 進数の ID (0~ffffffe) でオンラインユーザを指定します。指定しない場合、このコマンドはすべてのオンラインユーザのユーザプロファイルに適用される QoS ポリシーを表示します。

slot *slot-number*: メンバ ID によって IRF スタックメンバ装置を指定します。指定しない場合、すべてのメンバ装置のユーザプロファイルに適用される QoS ポリシーを表示します。

inbound: 受信トラフィックに適用された QoS ポリシーを指定します。

outbound: 送信トラフィックに適用された QoS ポリシーを指定します。

説明

display qos policy user-profile コマンドはユーザプロファイルに適用される QoS ポリシーを表示します。

方向を指定しない場合、受信と送信の両方の QoS ポリシーを表示します。

例

グローバルユーザのユーザプロファイル **abc** に適用される QoS ポリシーを表示します。

<Switch> display qos policy user-profile name abc user-id 30000000 inbound

```
User-Profile: abc
  User ID: 0x30000000(global)
```

```
  Direction: Inbound
  Policy: p1
   Classifier: default-class
     Matched : 0 (Packets) 0 (Bytes)
     Operator: AND
     Rule(s) :
      If-match any
     Behavior: be
      -none-
```

ローカルユーザのユーザプロファイル **abc** に適用される QoS ポリシーを表示します。

<Switch> display qos policy user-profile name abc user-id 30000001 inbound

```
User-Profile: abc
  slot 2:
    User ID: 0x30000001(local)
      Direction: Inbound
      Policy: p1
       Classifier: default-class
         Matched : 0 (Packets) 0 (Bytes)
         Operator: AND
         Rule(s) :
          If-match any
         Behavior: be
          -none-
```

表 2-8 コマンド出力

フィールド	説明
globa	アグリゲートインタフェースなどのグローバルインタフェースからオンラインになるグローバルユーザを示します。
local	物理インタフェースからオンラインになるローカルユーザを示します。
Matched	一致条件を満たすパケットの数です。
Direction	QoSポリシーが適用される方向です。
Green packets	greenパケットの統計情報です。
Yellow packets	Yellowパケットの統計情報です。
Red packets	redパケットの統計情報です。

他のフィールドの説明は表 2-1、表 2-4 を参照してください。

2.3.6 display qos vlan-policy

Syntax

display qos vlan-policy { **name** *policy-name* | **vlan** [*vlan-id*] } [**slot** *slot-number*] [**inbound** | **outbound**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

name *policy-name*: QoS ポリシー名を指定します。設定範囲は 1～31 文字です。大文字、小文字を区別します。

vlan *vlan-id*: VLAN の ID を指定します。設定範囲は 1～4094 です。

inbound: 受信トラフィックに適用された QoS ポリシーを表示します。

outbound: 送信トラフィックに適用された QoS ポリシーを表示します。

slot *slot-number*: IRF スタックメンバ装置を指定します。*slot-number* は IRF スタックメンバ装置の ID を示します。指定しない場合、IRF スタックユニットのマスタ装置の VLAN に適用された QoS ポリシーを表示します。

説明

display qos vlan-policy コマンドは VLAN に適用された QoS ポリシーを表示します。

方向を指定しない場合、**inbound** と **inbound** の両方の VLAN に適用された QoS ポリシーを表示します。

例

VLAN 2 に適用された QoS ポリシーを表示します。

<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-

表 2-9 コマンド出力

フィールド	説明
Direction	VLANに適用されたQoSポリシーの方向です。
Green packets	greenパケットの統計情報です。
Yellow packets	yellowパケットの統計情報です。
Red packets	redパケットの統計情報です。

その他のコマンド出力は表 2-1、表 2-4 を参照してください。

2.3.7 qos apply policy (interface view)

Syntax

qos apply policy *policy-name* { **inbound** | **outbound** }

undo qos apply policy *policy-name* { **inbound** | **outbound** }

デフォルト

設定なし

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

policy-name: QoS ポリシー名を指定します。設定範囲は 1〜31 文字です。大文字、小文字を区別します。

inbound: すべてのインタフェースの受信トラフィックに適用された QoS ポリシーを適用します。

outbound: すべてのインタフェースの送信トラフィックに適用された QoS ポリシーを適用します。**outbound** パラメータは control plane view でサポートしていません。

説明

qos apply policy コマンドはインタフェースに QoS ポリシーを適用します。

undo qos apply policy コマンドは QoS ポリシーを削除します。

🕮 **メモ：**

- **qos apply policy** コマンドと **packet-filter** コマンドを同じインタフェースで併用しないでください。
- behevior に redirect を指定した QoS ポリシーは outbound に設定できません。

例

GigabitEthernet 1/0/1 の送信トラフィックに適用された QoS ポリシーUSER1 を適用します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] qos apply policy USER1 outbound

2.3.8 qos apply policy (user profile view)

Syntax

qos apply policy *policy-name* { **inbound** | **outbound** }

undo qos apply policy *policy-name* { **inbound** | **outbound** }

デフォルト

設定なし

View

User profile view

定義済みユーザロール

network-admin

パラメータ

policy-name: QoS ポリシー名を指定します。設定範囲は 1～31 文字です。大文字、小文字を区別します。

inbound: 受信トラフィックに QoS ポリシーを適用します。

outbound: 送信トラフィックに QoS ポリシーを適用します。

説明

qos apply policy コマンドは QoS ポリシーをユーザプロファイルに適用します。

undo qos apply policy コマンドはユーザプロファイルに適用された QoS ポリシーを削除します。

ユーザプロファイルを削除すると、ユーザプロファイルに適用されている QoS ポリシーも削除されます。

ユーザプロファイルをアクティブにするには、ユーザプロファイルビューで適用される QoS ポリシーを空にすることはできません。ユーザプロファイルは、QoS ポリシー内の **car** アクションと **accounting** アクションだけをサポートします。

例

ユーザプロファイルユーザの受信トラフィックに QoS ポリシー**test** を適用します。

<Switch> system-view

[Switch] user-profile user

[Switch-user-profile-user] qos apply policy test outbound

2.3.9 qos apply policy global

Syntax

qos apply policy *policy-name* **global** { **inbound** | **outbound** }

undo qos apply policy *policy-name* **global** { **inbound** | **outbound** }

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

policy-name: QoS ポリシー名を指定します。設定範囲は 1～31 文字です。大文字、小文字を区別します。

inbound: すべてのインタフェースの受信パケットに適用された QoS ポリシーを適用します。

outbound: すべてのインタフェースの送信パケットに適用された QoS ポリシーを適用します。

説明

qos apply policy global コマンドはグローバルに QoS ポリシーを適用します。

undo qos apply policy global コマンドは QoS ポリシーを削除します。

グローバル QoS ポリシーは、QoS ポリシーが適用された方向に依存し、すべての受信トラフィックあるいはすべての送信トラフィックに適用します。

例

グローバルの受信トラフィックに適用された QoS ポリシーuser1 を適用します。

<Switch> system-view

[Switch] qos apply policy user1 global inbound

2.3.10 qos policy

Syntax

qos policy *policy-name*

undo qos policy *policy-name*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

policy-name: QoS ポリシー名を指定します。設定範囲は 1～31 文字です。大文字、小文字を区別します。

説明

qos policy コマンドは QoS ポリシーを作成し、QoS policy view に移行します。QoS ポリシーがすでに存在する場合、その view に移行します。

undo qos policy コマンドは QoS ポリシーを削除します。

undo qos policy コマンドでオブジェクトに適用されているポリシーを削除するには、最初にオブジェクトからポリシーを削除してください。

例

QoS ポリシーuser1 を作成します。

<Switch> system-view

[Switch] qos policy user1

[Switch-qospolicy-user1]

関連コマンド

- **classifier behavior**
- **qos apply policy**
- **qos apply policy global**
- **qos vlan-policy**

2.3.11 qos vlan-policy

Syntax

qos vlan-policy *policy-name* **vlan** *vlan-id-list* { **inbound** | **outbound** }

undo qos vlan-policy *policy-name* **vlan** *vlan-id-list* { **inbound** | **outbound** }

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

policy-name: QoS ポリシー名を指定します。設定範囲は 1～31 文字です。大文字、小文字を区別します。

vlan-id-list: VLAN を指定します。半角スペースで区切り 8 まで設定するか、VLAN の範囲で設定することができます。VLAN を範囲で指定する形式は *vlan-id1* **to** *vlan-id2* です。*vlan-id2* は *vlan-id1* より大きい値にしてください。設定範囲は 1～4094 です。

inbound: 指定された VLAN の受信パケットに QoS ポリシーを適用します。

outbound: 指定された VLAN の送信パケットに QoS ポリシーを適用します。

説明

qos vlan-policy コマンドは指定された VLAN に QoS ポリシーを適用します。

undo qos vlan-policy コマンドは指定された VLAN から QoS ポリシーを削除します。

例

VLAN 200、VLAN 300、VLAN 400、VLAN 500 の受信トラフィックに QoS ポリシーtest を適用します。

<Switch> system-view

[Switch] qos vlan-policy test vlan 200 300 400 500 inbound

2.3.12 reset qos policy global

Syntax

reset qos policy global [**inbound** | **outbound**]

View

User view

定義済みユーザロール

network-admin

パラメータ

inbound: 受信方向にグローバルで適用された QoS ポリシーの統計情報を削除します。

outbound: 送信方向にグローバルで適用された QoS ポリシーの統計情報を削除します。

説明

reset qos policy global コマンドはグローバルで適用された QoS ポリシーの統計情報を削除します。

方向を指定しない場合、**inbound** と **inbound** の両方のグローバルで適用された QoS ポリシーの統計情報を削除します。

例

受信方向にグローバルで適用された QoS ポリシーの統計情報を削除します。

<Switch> reset qos policy global inbound

2.3.13 reset qos vlan-policy

Syntax

reset qos vlan-policy [**vlan** *vlan-id*] [**inbound** | **outbound**]

View

User view

定義済みユーザロール

network-admin

パラメータ

vlan *vlan-id*: VLAN の ID を指定します。設定範囲は 1～4094 です。

inbound: 受信トラフィックに適用された QoS ポリシーの統計情報を削除します。

outbound: 送信トラフィックに適用された QoS ポリシーの統計情報を削除します。

説明

reset qos vlan-policy コマンドは VLAN に適用された QoS ポリシーの統計情報を削除します。

方向を指定しない場合、**inbound** と **inbound** の両方で適用された QoS ポリシーの統計情報を削除します。

例

VLAN 2 に適用された QoS ポリシーの統計情報を削除します。

<Switch> reset qos vlan-policy vlan 2

目次

このセクションのページは **8-x-x** です。

3章 プライオリティマッピング 3-1
3.1 プライオリティマッピング設定コマンド 3-1
3.1.1 display qos map-table 3-1
3.1.2 import 3-2
3.1.3 qos map-table 3-3
3.2 ポートプライオリティ設定コマンド 3-4
3.2.1 qos priority 3-4
3.3 プライオリティトラステッドモード設定コマンド 3-4
3.3.1 display qos trust interface 3-4
3.3.2 qos trust 3-5

3章 プライオリティマッピング

3.1 プライオリティマッピング設定コマンド

3.1.1 display qos map-table

Syntax

display qos map-table [**dot1p-lp** | **dscp-dot1p** | **dscp-dscp**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

装置は表 3-1 に示すプライオリティマッピングを適用します。

表 3-1 プライオリティマッピング

プライオリティマッピング	説明
dot1p-lp	802.1p-localプライオリティマッピングです。
dscp-dot1p	DSCP-802.1pプライオリティマッピングです。
dscp-dscp	DSCP-DSCPプライオリティマッピングです。

説明

display qos map-table コマンドはプライオリティマッピングの設定を表示します。

プライオリティマップを指定しない場合、すべてのプライオリティマッピングの設定を表示します。

例

802.1p-local プライオリティマッピングの設定を表示します。

<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
```

表 3-2 コマンド出力

フィールド	説明
MAP-TABLE NAME	プライオリティマッピングの名前です。
TYPE	プライオリティマッピングのタイプです。
IMPORT	プライオリティマッピングの入力値です。
EXPORT	プライオリティマッピングの出力値です。

3.1.2 import

Syntax

import *import-value-list* **export** *export-value*

undo import { *import-value-list* | **all** }

デフォルト

デフォルトのプライオリティマッピングが使用されます。詳細はオペレーションマニュアルのセクション 8 *ACL and QoS*”*プライオリティマッピング*”を参照してください。

View

Priority map view

定義済みユーザロール

network-admin

パラメータ

import-value-list: 入力値のリストを指定します。

export-value: 出力値を指定します。

all: プライオリティマッピングのすべてのマッピングをデフォルトに戻します。

説明

import コマンドはプライオリティマッピングのマッピングを設定します。

undo import コマンドはプライオリティマッピングの指定した、あるいはすべてのマッピングをデフォルトに戻します。

例

802.1p-local プライオリティマッピングテーブルを設定し、802.1p のプライオリティ 4 およびプライオリティ 5 を、ローカルプレシーデンス 1 にマッピングします。

<Switch> system-view

[Switch] qos map-table dot1p-lp

[Switch-maptbl-dot1p-lp] import 4 5 export 1

関連コマンド

display qos map-table

3.1.3 qos map-table

Syntax

qos map-table { **dot1p-lp** | **dscp-dot1p** | **dscp-dscp** }

View

System view

定義済みユーザロール

network-admin

パラメータ

パラメータの説明は表 3-1 を参照してください。

説明

qos map-table コマンドは指定した priority map view に移行します。

例

802.1p-local priority map view に移行します。

<Switch> system-view

[Switch] qos map-table dot1p-lp

[Switch-maptbl-dot1p-lp]

関連コマンド

- **display qos map-table**
- **import**

3.2 ポートプライオリティ設定コマンド

3.2.1 qos priority

Syntax

qos priority *priority-value*

undo qos priority

デフォルト

0

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

priority-value: ポートプライオリティの値を指定します。設定範囲は 0～7 です。

説明

qos priority コマンドはインタフェースのポートプライオリティを変更します。

undo qos priority コマンドはデフォルトに戻します。

例

GigabitEthernet 1/0/1 のポートプライオリティを 2 に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] qos priority 2

関連コマンド

display qos trust interface

3.3 プライオリティトラステッドモード設定コマンド

3.3.1 display qos trust interface

Syntax

display qos trust interface [*interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface-type interface-number: インタフェースのタイプと番号を指定します。指定しない場合、すべてのインタフェースのプライオリティのトラステッドモードとポートプライオリティの情報を表示します。

説明

display qos trust interface コマンドはインタフェースのプライオリティのトラステッドモードとポートプライオリティの情報を表示します。

例

GigabitEthernet 1/0/1のプライオリティのトラステッドモードとポートプライオリティの情報を表示します。

<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
```

表 3-3 コマンド出力

フィールド	説明
Interface	インタフェースのタイプと番号です。
Port priority	インタフェースのポートプライオリティのセットです。
Port priority trust type	インタフェースのプライオリティトラステッドモードです。**dot1p**、**dscp**、**none**があります。トラステッドモードが**none**の場合、プライオリティマッピングにポートプライオリティが使用されます。

3.3.2 qos trust

Syntax

qos trust { **dot1p** | **dscp** }

undo qos trust

デフォルト

インタフェースはパケットのプライオリティを信用しません。802.1p プライオリティとしてポートプライオリティを使用します。

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

dot1p: プライオリティマッピングの受信パケットの 802.1p プライオリティを使用します。

dscp: プライオリティマッピングの受信パケットの DSCP を使用します。

説明

qos trust コマンドはインタフェースのプライオリティトラステッドモードを設定します。

undo qos trust コマンドはデフォルトのプライオリティのトラステッドモードに戻します。

例

GigabitEthernet 1/0/1 のプライオリティトラステッドモードを 802.1p プライオリティに設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] qos trust dot1p

関連コマンド

display qos trust interface

目次

このセクションのページは **8-x-x** です。

4章 トラフィックポリシング、GTS、ラインレート 4-1
4.1 GTS 設定コマンド 4-1
4.1.1 display qos gts interface 4-1
4.1.2 qos gts 4-2
4.2 ラインレート設定コマンド 4-3
4.2.1 display qos lr interface 4-3
4.2.2 qos lr 4-4

4章 トラフィックポリシング、GTS、ラインレート

4.1 GTS設定コマンド

4.1.1 display qos gts interface

Syntax

display qos gts interface [*interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface-type interface-number: インタフェースのタイプと番号を指定します。指定しない場合、すべてのインタフェースの GTS の設定を表示します。

説明

display qos gts interface コマンドはインタフェースの GTS（generic traffic shaping）を表示します。

例

すべてのインタフェースの GTS を表示します。

<Switch> display qos gts interface

```
Interface: GigabitEthernet1/0/1
 Rule: If-match acl 2001
  CIR 512 (kbps), CBS 51200 (Bytes)
```

表 4-1 コマンド出力

フィールド	説明
Interface	インタフェースのタイプと番号です。
Rule	一致条件です。
CIR	平均トラフィックレートを指定するCIRです。単位はkbpsです。

フィールド	説明
CBS	時間内に許可されるバーストトラフィック量を指定する CBSです。単位はバイトです。

4.1.2 qos gts

Syntax

qos gts queue *queue-id* **cir** *committed-information-rate* [**cbs** *committed-burst-size*]

undo qos gts queue *queue-id*

デフォルト

設定なし

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

queue *queue-id*: キューの ID を指定します。設定範囲は 0～7 です。

cir *committed-information-rate*: 平均トラフィックレートを指定する CIR を kbps 単位で指定します。GE インタフェースの設定範囲は 8～1048576 です。10GE インタフェースの設定範囲は 8～10485760 です。値は 8 の整数倍にする必要があります。

cbs *committed-burst-size*: CBS をバイト単位で指定します。設定範囲は 512～16777216 です。512 の整数倍にする必要があります。デフォルトは 62.5 と CIR の積で、512 の整数倍にする必要があります。512 と CIR の積が 512 の整数倍でない場合、積より大きい値で、512 にもっとも近い値になります。デフォルトは 16777216 より大きい場合、16777216 となります。

説明

qos gts コマンドはインタフェースの GTS のパラメータを設定します。

undo qos gts コマンドはインタフェースの GTS のパラメータを削除します。

例

CIR を 6400kbps、CBS を 51200 バイトに制限するように、GigabitEthernet 1/0/1 のキュー1 のパケットに GTS のパラメータを設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] qos gts queue 1 cir 6400 cbs 51200

4.2 ラインレート設定コマンド

4.2.1 display qos lr interface

Syntax

display qos lr interface [*interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface-type interface-number: インタフェースのタイプと番号を指定します。指定しない場合、すべてのインタフェースのラインレートの設定を表示します。

説明

display qos lr interface コマンドはインタフェースのラインレート（レートリミット）の設定を表示します。

例

すべてのインタフェースのラインレートの設定を表示します。

<Switch> display qos lr interface

```
Interface: GigabitEthernet1/0/1
 Direction: Inbound
  CIR 2000 (kbps), CBS 20480 (Bytes)
```

表 4-2 コマンド出力

フィールド	説明
Interface	インタフェースのタイプと番号です。
Direction	ラインレートの設定が適用される方向です。inbound、outbound があります。
CIR	平均トラフィックレートを指定するCIRです。単位はkbpsです。
CBS	時間内に許可されるバーストトラフィック量を指定するCBSです。単位はバイトです。

4.2.2 qos lr

Syntax

qos lr { **inbound** | **outbound** } **cir** *committed-information-rate* [**cbs** *committed-burst-size*]

undo qos lr { **inbound** | **outbound** }

デフォルト

設定なし

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

inbound: インタフェースで受信パケットのレートを制限します。

outbound: インタフェースで送信パケットのレートを制限します。

cir *committed-information-rate*: 平均トラフィックレートを指定する CIR を kbps 単位で指定します。GE インタフェースの設定範囲は 8～1048576 です。10GE インタフェースの設定範囲は 8～10485760 です。値は 8 の整数倍にする必要があります。

cbs *committed-burst-size*: CBS をバイト単位で指定します。設定範囲は 512～134217728 です。512 の整数倍にする必要があります。デフォルトは 62.5 と CIR の積で、512 の整数倍にする必要があります。512 と CIR の積が 512 の整数倍でない場合、積より大きい値で 512 にもっとも近い値になります。デフォルトは 134217728 より大きい場合、134217728 となります。

説明

qos lr コマンドはインタフェースのパケットのレートを制限します。

undo qos lr コマンドはパケットのラインレートを削除します。

例

GigabitEthernet 1/0/1 の送信パケットのレートを、CIR が 256kbps、CBS が 51200 バイトに制限します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] qos lr outbound cir 256 cbs 51200

目次

このセクションのページは **8-x-x** です。

5 章 輻輳制御 5-1
5.1 Common 設定コマンド 5-1
5.1.1 display qos queue interface 5-1
5.2 SP 設定コマンド 5-2
5.2.1 display qos queue sp interface 5-2
5.2.2 qos sp 5-3
5.3 WRR 設定コマンド 5-4
5.3.1 display qos queue wrr interface 5-4
5.3.2 qos wrr 5-5
5.3.3 qos wrr group sp 5-6
5.3.4 qos wrr weight 5-7
5.4 キューベースアカウンティング設定コマンド 5-8
5.4.1 display qos queue-statistics interface outbound 5-8

5章 輻輳制御

5.1 Common設定コマンド

5.1.1 display qos queue interface

Syntax

display qos queue interface [*interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface-type interface-number: インタフェースのタイプと番号を指定します。指定しない場合、すべてのインタフェースのキューイングの設定を表示します。

説明

display qos queue interface コマンドはインタフェースのキューイングの設定を表示します。

例

すべてのインタフェースのキューイングの設定を表示します。

<Switch> display qos queue interface

```
Interface: GigabitEthernet1/0/1
Output queue: Strict Priority queuing
Interface: GigabitEthernet1/0/2
 Output queue: Strict Priority queuing
Interface: GigabitEthernet1/0/3
 Output queue: Strict Priority queuing
Interface: GigabitEthernet1/0/4
 Output queue: Strict Priority queuing
Interface: GigabitEthernet1/0/5
 Output queue: Strict Priority queuing
Interface: GigabitEthernet1/0/6
 Output queue: Strict Priority queuing
```

表 5-1 コマンド出力

フィールド	説明
Interface	インタフェースのタイプと番号です。
Output queue	現在の出力キューのタイプです。
Group	キューを保持するグループの番号です。
Weight	キューのパケットカウントスケジューリングの重みづけです。N/AはSPスケジュールのアルゴリズムを使用していることを示します。

5.2 SP設定コマンド

5.2.1 display qos queue sp interface

Syntax

display qos queue sp interface [*interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface-type interface-number: インタフェースのタイプと番号を指定します。指定しない場合、すべてのインタフェースの SP キューイングの設定を表示します。

説明

display qos queue sp interface コマンドはインタフェースの SP キューイングの設定を表示します。

例

GigabitEthernet 1/0/1 の SP キューイングの設定を表示します。

<Switch> display qos queue sp interface gigabitethernet 1/0/1

```
Interface: GigabitEthernet1/0/1
 Output queue: Strict Priority queuing
```

表 5-2 コマンド出力

フィールド	説明
Interface	インタフェースのタイプと番号です。
Output queue	現在の出力キューのタイプです。

5.2.2 qos sp

Syntax

qos sp

undo qos sp

デフォルト

パケット単位の WRR キューイング

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

説明

qos sp コマンドはインタフェースで SP キューイングを設定します。

undo qos sp コマンドはデフォルトに戻します。

例

GigabitEthernet 1/0/1 で SP キューイングを設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] qos sp

関連コマンド

display qos queue sp interface

5.3 WRR設定コマンド

5.3.1 display qos queue wrr interface

Syntax

display qos queue wrr interface [*interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface-type interface-number: インタフェースのタイプと番号を指定します。指定しない場合、すべてのインタフェースの WRR キューイングの設定を表示します。

説明

display qos queue wrr interface コマンドはインタフェースの WRR キューイングの設定を表示します。

例

GigabitEthernet 1/0/1 の WRR キューイングの設定を表示します。

<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
```

表 5-3 コマンド出力

フィールド	説明
Interface	インタフェースのタイプと番号です。

フィールド	説明
Output queue	現在の出力キューのタイプです。
Group	キューに割り当てられたグループの番号です。
Weight	パケット単位のキューのスケジュールの重みづけです。**N/A** はSPキューのスケジュールのアルゴリズムを使用していることを示します。

5.3.2 qos wrr

Syntax

qos wrr weight

undo qos wrr weight

デフォルト

パケット単位の WRR キューイング

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

weight: パケット単位でキューに帯域幅を割り当てます。

説明

qos wrr コマンドはパケット単位の WRR キューイングを有効にします。

undo qos wrr コマンドはデフォルトに戻します。

インタフェースのキューの WRR キューイングのパラメータを設定する前に、**qos wrr** コマンドで WRR キューイングを有効にしてください。

例

GigabitEthernet 1/0/1 でパケット単位の WRR キューイングを有効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] qos wrr weight

関連コマンド

display qos queue wrr interface

5.3.3 qos wrr group sp

Syntax

qos wrr *queue-id* **group sp**

undo qos wrr *queue-id*

デフォルト

WRR が有効なインタフェースのすべてのキューは WRR グループ 1 にあります。

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

queue-id: キューID を指定します。設定範囲あるいは表 5-4 に示すキーワードで指定します。設定範囲は 0～7 です。

表 5-4 キューID の番号とキーワードの関係

番号	キーワード
0	be
1	af1
2	af2
3	af3
4	af4
5	ef
6	cs6
7	cs7

説明

qos wrr group sp コマンドは SP グループにキューを割り当てます。

undo qos wrr group sp コマンドは SP グループからキューを削除します。

qos wrr group sp コマンドは WRR が有効なインタフェースでのみ有効です。SP グループのキューは SP によってスケジューリングされます。SP グループは WRR グループよりスケジューリングのプライオリティが高くなります。

インタフェースで **qos wrr group sp** コマンドを設定する前に、**qos wrr** コマンドで WRR キューイングを有効にしてください。

キューがインタフェースのトラフィックの負荷でもっとも低いプライオリティを持つ場合、SP グループのキューはスケジューリングされません。

例

GigabitEthernet 1/0/1 で WRR キューイングを有効にし、キュー0 を SP グループに割り当てます。

<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

関連コマンド

- **display qos queue wrr interface**
- **qos wrr**

5.3.4 qos wrr weight

Syntax

qos wrr *queue-id* **group 1 weight** *schedule-value*

undo qos wrr *queue-id*

デフォルト

WRR が有効なすべてのキューは WRR グループ 1 にあります。キュー0～キュー7 の重みは、それぞれ 1、2、3、4、5、9、13、15 です。

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

queue-id: キューID を指定します。設定範囲あるいは表 5-4 に示すキーワードで指定します。設定範囲は 0～7 です。

group 1: WRR グループ 1を指定します。現在のソフトウェアバージョンでは 1 つの WRR グループのみサポートしています。

weight: パケット単位でキューに帯域幅を割り当てます。

schedule-value: WRR キューイングのキューにスケジュールされた重みを指定します。設定範囲は 1～15 です。

説明

qos wrr weight コマンドはインタフェースのキューに WRR キューイングパラメータを設定します。

undo qos wrr コマンドはインタフェースのキューの WRR キューイングパラメータを削除します。

インタフェースのキューの WRR キューイングのパラメータを設定する前に、**qos wrr** コマンドで WRR キューイングを有効にしてください。

例

GigabitEthernet 1/0/1 でパケット単位の WRR キューイングを有効にし、キュー0、キュー1 を WRR グループ 1 に割り当てます。キュー0 の重みは 10 に設定します。

<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

関連コマンド

- **display qos queue wrr interface**
- **qos wrr**

5.4 キューベースアカウンティング設定コマンド

5.4.1 display qos queue-statistics interface outbound

Syntax

display qos queue-statistics interface [*interface-type interface-number*] **outbound**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface-type interface-number: インタフェースのタイプと番号を指定します。指定しない場合、すべてのインタフェースのキューベースの出力トラフィックの統計情報を表示します。

説明

display qos queue-statistics interface outbound コマンドはインタフェースでキューベースの出力トラフィックの統計情報を表示します。

例

GigabitEthernet 1/0/1 でキューベースの出力トラフィックの統計情報を表示します。

<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
```

表 5-5 コマンド出力

フィールド	説明
Interface	キューベースのトラフィックの統計情報が表示されるインタフェースです。
Direction	収集された統計情報のトラフィック方向です。
Forwarded	転送されたトラフィックの統計情報です。パケット、バイトがあります。
Dropped	廃棄されたトラフィックの統計情報です。パケット、バイトがあります。
Current queue length	現在のキューの長さです。

関連コマンド

reset counters interface (Interface Command Reference)

目次

このセクションのページは **8-x-x** です。

6 章 データバッファ 6-1
6.1 データバッファ設定コマンド 6-1
6.1.1 buffer apply 6-1
6.1.2 buffer queue guaranteed 6-1
6.1.3 buffer shared 6-2
6.1.4 buffer total-shared 6-3
6.1.5 burst-mode enable 6-4
6.1.6 display buffer 6-6

6章 データバッファ

6.1 データバッファ設定コマンド

6.1.1 buffer apply

Syntax

buffer apply

undo buffer apply

Views

System view

定義済みユーザロール

network-admin

説明

buffer apply 手動で設定したデータバッファを適用します。

undo buffer apply を使用して、デフォルトに戻します。

データバッファ設定を有効にするには、このコマンドを実行する必要があります。

手動で設定したデータバッファ設定を適用した後に、設定を直接変更することはできません。変更するには、**undo buffer apply** を実行し、再設定して、再適用する必要があります。

例

手動で設定したデータバッファ設定を適用します。

```
<Switch> system-view
[Switch] buffer apply
```

6.1.2 buffer queue guaranteed

Syntax

buffer egress [**slot** *slot-number*] { **cell** | **packet** } **queue** *queue-id* **guaranteed ratio** *ratio*

undo buffer egress [**slot** *slot-number*] { **cell** | **packet** } **queue** *queue-id* **guaranteed**

デフォルト

キューのセルリソースは、全セルリソースの 12%です。

キューのパケットリソースは、全パケットリソースの 12%です。

Views

System view

定義済みユーザロール

network-admin

パラメータ

egress: 出力バッファを指定します。

slot *slot-number*: IRF スタックメンバ ID (スロット番号) で メンバ デバイスを指定します。IRF スタックメンバ デバイスを指定しない場合、このコマンドはすべての IRF スタックメンバ デバイスに適用されます。

cell: セルリソースを指定します。

queue-id: 0~7 の範囲でキューID を指定します。

ratio *ratio*:固定領域の比率(パーセント)を指定します。ratio の値の範囲は 1～100 です。

説明

buffer queue guaranteed コマンドで、キューの固定領域比率を設定します。

undo buffer queue guaranteed でデフォルトに戻ります。

デフォルトでは、すべてのキューが固定領域を均等に共有します。キューの固定領域比率を設定できます。他のキューは残りの部分を均等に共有します。

キューの固定領域は、他のキューでは使用できません。したがって、キューの最小保証バッファとも呼ばれます。すべてのキューに設定された固定領域比率の合計が、合計固定領域比率を超えることはできません。そうでない場合、 設定 は失敗します。

例

キュー0 を、セルリソースの 20%の固定領域スペースを使用するように設定します。

```
<Switch> system-view
[Switch] buffer egress cell queue 0 guaranteed ratio 20
```

6.1.3 buffer shared

Syntax

buffer egress [**slot** *slot-number*] { **cell** | **packet** } [**queue** *queue-id*] **shared ratio** *ratio*

undo buffer egress [**slot** *slot-number*] { **cell** | **packet** } [**queue** *queue-id*] **shared**

デフォルト

The maximum packet resource ratio for a port is 10% of the total packet resources.

The maximum cell resource ratio for a port is 10% of the total cell resources.

Views

System view

定義済みユーザロール

network-admin

パラメータ

egress: 出力バッファを指定します。

slot *slot-number*: IRF スタックメンバ ID (スロット番号) で メンバ デバイスを指定します。IRF スタックメンバ デバイスを指定しない場合、このコマンドはすべての IRF スタックメンバ デバイスに適用されます。

cell: セルリソースを指定します。

packet: パケットリソースを指定します。

queue-id: 0~7 の範囲でキューID を指定します。

ratio *ratio*:固定領域の比率(パーセント)を指定します。ratio の値の範囲は 1～100 です。

説明

buffer shared コマンドで、各ポートまたはキューの最大共有領域比率を設定します。

undo buffer shared コマンドで、デフォルトに戻ります。

デフォルトでは、すべてのポートまたはキューが共有領域を均等に共有します。各ポートまたはキューの共有領域の比率を設定できます。未構成のキューは、デフォルト設定を使用します。各ポートまたはキューの共有領域スペースは、最終的に、 設定 と送受信されるパケットの数に基づいてチップによって決定されます。

例

#キュー 0 の、出力バッファセルリソースの共有領域を最大 10%に設定します。

```
<Switch> system-view
[Switch] buffer egress cell queue 0 shared ratio 10
```

6.1.4 buffer total-shared

Syntax

buffer egress [**slot** *slot-number*] { **cell** | **packet** } **total-shared ratio** *ratio*

undo buffer egress [**slot** *slot-number*] { **cell** | **packet** } **total-shared**

デフォルト

セルリソースは 52%で、パケットリソースは 50%です。

Views

System view

定義済みユーザロール

network-admin

パラメータ

egress: 出力バッファを指定します。

slot *slot-number*: IRF スタックメンバ ID (スロット番号) で メンバ デバイスを指定します。IRF スタックメンバ デバイスを指定しない場合、このコマンドはすべての IRF スタックメンバ デバイスに適用されます。

cell: セルリソースを指定します。

packet: パケットリソースを指定します。

ratio *ratio*:固定領域の比率(パーセント)を指定します。ratio の値の範囲は 1～100 です。

説明

buffer total-shared コマンドで、共有エリアの比率の合計を設定します。

undo buffer total-shared コマンドで、デフォルトに戻ります。

共有領域の比率を設定すると、残りのバッファ領域は自動的に固定領域に割り当てられます。

例

#出力バッファのセルリソース共有領域を 50%に 設定します。

```
<Switch> system-view
```

6.1.5 burst-mode enable

Syntax

burst-mode enable

undo burst-mode enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

burst-mode enable コマンドはバースト機能を有効にします。

undo burst-mode enable コマンドはバースト機能を無効にします。

バースト機能は、以下の状況下においてパケットの損失を削減することに有益です。

- ブロードキャストトラフィックあるいはマルチキャストトラフィックが集中し、トラフィックのバーストを引き起こします。
- 装置の高速インタフェースから低速インタフェースにトラフィックが転送されます。
- 複数の同一レートのインタフェースから同一レートでインタフェースにトラフィックが転送されます。

バースト機能が無効の場合、セルリソースとパケットリソースは表 6-1 に示すような割合で割り当てられます。

表 6-1 パケットバッファの割り当て（バースト機能が無効の場合）

リソースタイプ	キューの専用（固定）エリアの割合	ポートあるいはキューごとに使用できる共有エリアの割合の最大	共有エリア全体の割合
セル	12%	10%	50%
パケット	12%	10%	52%

バースト機能が有効の場合、セルリソースとパケットリソースは表 6-2 に示すような割合で割り当てられます。

表 6-2 パケットバッファの割り当て（バースト機能が有効の場合）

リソースタイプ	キューの専用（固定）エリアの割合	ポートあるいはキューごとに使用できる共有エリアの割合の最大	共有エリア全体の割合
セル	12%	90%	72%
パケット	12%	90%	74%

例

バースト機能を有効にします。

<Switch> system-view

[Switch] burst-mode enable

6.1.6 display buffer

Syntax

display buffer [**slot** *slot-number*][**queue** [*queue-id*]]

Views

Any view

定義済みユーザロール

network-admin

network-operator

パラメータ

slot *slot-number*: IRF スタックメンバ ID (スロット番号) で メンバ デバイスを指定します。IRF スタックメンバ デバイスを指定しない場合、このコマンドはすべての IRF スタックメンバ デバイスのバッファサイズ設定を表示します。

queue *queue-id*: 0~7 の範囲の番号でキューを指定します。キューを指定すると、指定したキューの固定領域比率と共有領域比率が表示されます。**queue** キーワードを queue-id 引数なしで指定すると、各キューの固定領域比率と共有領域比率が表示されます。**queue** キーワードを指定しない場合、このコマンドは総共有領域比率を表示します。

説明

display buffer コマンドで、バッファサイズの設定を表示します。

例

#バッファサイズの設定を表示します。

```
<Switch> display buffer
Slot  Type    Eg(Total-shared , Shared)
1     packet  50 , 10
1     cell    52 , 10


         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
```

キューの固定領域比率と共有領域比率を表示します。

```
<Switch> display buffer queue
Slot  Queue       Type    Eg(Guaranteed , Shared)
1     0-7         packet  12 , --
1     0-7         cell    12 , --


         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
```

表 6-3 コマンド出力

Field	Description
Type	リソースタイプ:パケットまたはセル。
Queue	0~7の範囲のキューID。
Eg	出力バッファ。
(Total-shared , Shared)	**Total-shared** inは、総共有面積率を示します。 **Shared** は、ポートの共有面積率を示します。
(Guaranteed , Shared)	**Guaranteed**は、キューの固定領域比率を示します。 **Shared** は、キューの共有領域比率を示します。 デバイスが リソース タイプをサポートしていない場合、このフィールドには2つのハイフン (--) が表示されます。

目次

このセクションのページは **8-x-x** です。

7 章 タイムレンジ 7-1
7.1 タイムレンジ設定コマンド 7-1
7.1.1 display time-range 7-1
7.1.2 time-range 7-2

7章 タイムレンジ

7.1 タイムレンジ設定コマンド

7.1.1 display time-range

Syntax

display time-range { *time-range-name* | **all** }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

time-range-name: タイムレンジの名前を指定します。設定範囲は 1～32 文字です。大文字、小文字を区別しません。文字列の最初は英字を指定します。

all: 既存のすべてのタイムレンジの設定と状態を表示します。

説明

display time-range コマンドはタイムレンジの設定と状態を表示します。

例

タイムレンジ 14 の設定と状態を表示します。

<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
```

表 7-1 コマンド出力

フィールド	説明
Current time	現在のシステム時間です。

フィールド	説明
Time-range	タイムレンジの設定と状態です。タイムレンジ名、状態（activeあるいはinactive）、開始時間、終了時間が含まれます。

7.1.2 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*]

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

time-range-name: タイムレンジの名前を指定します。設定範囲は 1～32 文字です。大文字、小文字を区別しません。文字列の最初は英字を指定します。混乱をさけるため **all** を使用してはいけません。

start-time **to** *end-time*: 周期的なタイムレンジを指定します。*start-time* と *end-time* の形式は hh:mm です。24 時間時計です。*start-time* の設定範囲は 00:00～23:59 です。*end-time* の設定範囲は 00:00～24:00 です。*end-time* は *start-time* よりも大きい値にする必要があります。

days: 周期的なタイムレンジの日時あるいは曜日を指定します。複数の値を指定する場合、スペースで区切ります。値は重複することができません。値は以下のいずれかを指定することができます。

- 0～6：それぞれ日曜日、月曜日、火曜日、水曜日、木曜日、金曜日、土曜日の設定範囲を指定します。
- **Sun**、**Mon**、**Tue**、**Wed**、**Thu**、**Fri**、**Sat**：曜日を指定します。
- **working-day**：月曜日～金曜日の営業日を指定します。
- **off-day**：土曜日、日曜日の非営業日を指定します。
- **daily**：一週間の日付を指定します。

from *time1 date1*: 絶対的なタイムレンジの開始時間と開始日を指定します。*time1* は時間を指定します。形式は hh:mm です。24 時間時計です。設定範囲は 00:00～23:59 です。*date1* は日付を指定します。形式は MM/DD/YYYY あるいは YYYY/MM/DD です。MM は 1～12 の月、*DD* は各月の日付、*YYYY* は 1970～2100 の年です。このパラメータを指定しない場合、開始時間と開始日はシステムで有効なもっとも早い時間の 01/01/1970 00:00 AM となります。

to *time2 date2*: 絶対的なタイムレンジの終了時間と終了日を指定します。*time2* は時間を指定します。形式は hh:mm です。24 時間時計です。設定範囲は 00:00～24:00 です。*date2* は日付を指定します。形式は MM/DD/YYYY あるいは YYYY/MM/DD です。MM は 1～12 の月、*DD* は各月の日付、*YYYY* は 1970～2100 の年です。このパラメータを指定しない場合、終了時間と終了日はシステムで有効なもっとも遅い時間の 12/31/2100 24:00 PM となります。

説明

time-range コマンドはタイムレンジを作成あるいは修正します。

undo time-range コマンドはタイムレンジあるいはタイムレンジのパラメータを削除します。

タイムレンジ名が既に存在する場合、タイムレンジのパラメータを追加します。

タイムレンジの複数のパラメータを作成することができます。各時間のパラメータは以下の形式の 1 つを指定することができます。

- *start-time* **to** *end-time days* の形式の周期的なパラメータを指定します。周期的なパラメータは日付あるいは曜日を周期的に繰り返します。
- *from time1 date1* **to** *time2 date2* の形式の絶対的なパラメータを指定します。一度限りで繰り返しません。
- *start-time* **to** *end-time days* **from** *time1 date1* **to** *time2 date2* の形式の組み合わせを指定します。指定した期間内で日付あるいは曜日を周期的に繰り返します。たとえば、2015 年 1 月 1 日～12 月 31 日の月曜日の 8:00～12:00 の営業時間のタイムレンジ test を指定する場合、**time-range test 08:00 to 12:00 mon from 00:00 01/01/2015 to 23:59 12/31/2015** コマンドを使用します。

周期的なパラメータを最大 32、絶対的なパラメータを最大 12 の、最大 1024 のタイムレンジを作成することができます。タイムレンジのアクティブな期間を以下のように計算します。

1) すべての周期的なタイムレンジを組み合わせます。
2) すべての絶対的なタイムレンジを組み合わせます。
3) タイムレンジのアクティブな期間として 2 つの記述の AND を行います。

例

周期的なタイムレンジ t1 を作成し、営業時間の 8:00～18:00 をアクティブな期間に設定します。

<Switch> system-view

[Switch] time-range t1 08:00 to 18:00 working-day

絶対的なタイムレンジ t2 を作成し、2011 年のすべてをアクティブな期間に設定します。

<Switch> system-view

[Switch] time-range t2 from 00:00 1/1/2011 to 24:00 12/31/2011

組み合わせのタイムレンジ t3 を作成し、2011 年の土曜日と日曜日の 8:00～12:00 をアクティブな期間に設定します。

<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

組み合わせのタイムレンジ t4 を作成し、2011 年の 1 月～6 月の月曜日の 10:00～12:00 と水曜日の 14:00～16:00 をアクティブな期間に設定します。

<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

関連コマンド

display time-range

QX-S5100G シリーズ Ethernet スイッチ

コマンドマニュアル

9. セキュリティ

本マニュアルは以下に示す章で構成されています。

01-AAA
02-802.1X
03-MAC アドレス認証
04-Web 認証
05-ポートセキュリティ
06-User profile
07-パスワード管理
08-公開鍵
09-PKI
10-SSH
11-SSL
12-TCP フラグメントアタックプロテクション
13-IP ソースガード
14-ARP アタックプロテクション
15-uRPF

目次

このセクションのページは **9-x-x** です。

1 章 AAA 1-1
1.1 AAA 設定コマンド 1-1
1.1.1 aaa session-limit 1-1
1.1.2 accounting default 1-2
1.1.3 accounting lan-access 1-3
1.1.4 accounting login 1-4
1.1.5 accounting start-fail 1-6
1.1.6 accounting update-fail 1-7
1.1.7 authentication default 1-7
1.1.8 authentication lan-access 1-9
1.1.9 authentication login 1-10
1.1.10 authorization command 1-11
1.1.11 authorization default 1-13
1.1.12 authorization lan-access 1-14
1.1.13 authorization login 1-15
1.1.14 display domain 1-17
1.1.15 domain 1-21
1.1.16 domain default enable 1-22
1.1.17 state (ISP domain view) 1-23
1.2 ローカルユーザ設定コマンド 1-24
1.2.1 access-limit 1-24
1.2.2 authorization-attribute (local user view/user group view) 1-25
1.2.3 bind-attribute 1-27
1.2.4 display local-user 1-29
1.2.5 display user-group 1-32
1.2.6 group 1-34
1.2.7 local-user 1-35
1.2.8 password 1-36
1.2.9 service-type 1-38
1.2.10 state (local user view) 1-39
1.2.11 user-group 1-40
1.3 RADIUS 設定コマンド 1-41
1.3.1 accounting-on enable 1-41
1.3.2 data-flow-format (RADIUS scheme view) 1-42
1.3.3 display radius scheme 1-44
1.3.4 display radius statistics 1-48

1.3.5 display stop-accounting-buffer (for RADIUS) 1-49
1.3.6 key (RADIUS scheme view) 1-51
1.3.7 nas-ip (RADIUS scheme view) 1-52
1.3.8 primary accounting (RADIUS scheme view) 1-54
1.3.9 primary authentication (RADIUS scheme view) 1-55
1.3.10 radius dscp 1-57
1.3.11 radius nas-ip 1-58
1.3.12 radius scheme 1-59
1.3.13 reauthentication server-select 1-60
1.3.14 reset radius statistics 1-61
1.3.15 reset stop-accounting-buffer (for RADIUS) 1-62
1.3.16 retry 1-63
1.3.17 retry realtime-accounting 1-64
1.3.18 retry stop-accounting (RADIUS scheme view) 1-65
1.3.19 secondary accounting (RADIUS scheme view) 1-66
1.3.20 secondary authentication (RADIUS scheme view) 1-68
1.3.21 snmp-agent trap enable radius 1-70
1.3.22 state primary 1-72
1.3.23 state secondary 1-73
1.3.24 stop-accounting-buffer enable (RADIUS scheme view) 1-74
1.3.25 timer quiet (RADIUS scheme view) 1-75
1.3.26 timer realtime-accounting (RADIUS scheme view) 1-76
1.3.27 timer response-timeout (RADIUS scheme view) 1-77
1.3.28 user-name-format (RADIUS scheme view) 1-79

1章 AAA

1.1 AAA設定コマンド

1.1.1 aaa session-limit

Syntax

aaa session-limit { **ftp** | **http** | **https | ssh** | **telnet** } *max-sessions*

undo aaa session-limit { **ftp** | **http** | **https | ssh** | **telnet** }

デフォルト

32

View

System view

定義済みユーザロール

network-admin

パラメータ

ftp: FTP ユーザを指定します。

http: HTTP ユーザを指定します。

https: HTTPS ユーザを指定します。

ssh: SSH ユーザを指定します。

telnet: Telnet ユーザを指定します。

max-sessions: 装置に同時に接続可能な最大接続数を指定します。FTP、SSH、Telnet の設定範囲は 1～32 です。HTTP、HTTPS の設定範囲は 1～64 です。

説明

aaa session-limit コマンドは装置に同時に接続可能な最大接続数を指定します。

undo aaa session-limit コマンドはデフォルトに戻します。

ユーザタイプの最大同時接続数が上限に到達したのち、システムは後続のユーザタイプの接続を拒否します。

例

FTP ユーザの最大同時接続数を 4 に設定します。

<Switch> system-view

[Switch] aaa session-limit ftp 4

1.1.2 accounting default

Syntax

accounting default { **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo accounting default

デフォルト

local

View

ISP domain view

定義済みユーザロール

network-admin

パラメータ

local: ローカルアカウンティングを実行します。

none: アカウンティングを実行しません。

radius-scheme *radius-scheme-name*: RADIUS スキーム名を指定します。設定範囲は 1～32 です。大文字、小文字を区別しません。

説明

accounting default コマンドは ISP ドメインのデフォルトアカウンティング方式を指定します。

undo accounting default コマンドはデフォルトに戻します。

デフォルトアカウンティング方式は、この方式をサポートするすべてのユーザで使用されます。特定のアカウンティング方式は設定されません。

ローカルアカウンティングは、ローカルユーザ接続の数を監視し、制御するためにのみ使用されます。アカウンティング機能が一般的に提供する統計機能を提供していません。

1 つのプライマリデフォルトアカウンティング方式と複数のバックアップのアカウンティング方式を指定することができます。

プライマリアカウンティングが無効であるとき、装置は、順番にバックアップのアカウンティング方式を使用します。たとえば、**accounting default radius-scheme** *radius-scheme-name* **local none** コマンドはプライマリデフォルト RADIUS アカウンティング方式と 2 つのバックアップの方式（ローカルアカウンティング方式とアカウンティングがない方式）を指定します。装置はデフォルトで RADIUS アカウンティング方式を実行し、RADIUS サーバが無効であるときローカルアカウンティング方式を実行しま

す。RADIUS アカウンティング方式とローカルアカウンティング方式の両方が無効であるとき、装置はアカウンティング方式を実行しません。

例

ISP ドメイン test のデフォルトアカウンティング方式を設定します。プライマリを RADIUS スキーム rd、バックアップをローカルとして設定します。

<Switch> system-view

[Switch] domain test

[Switch-isp-test] accounting default radius-scheme rd local

関連コマンド

- **local-user**
- **radius scheme**

1.1.3 accounting lan-access

Syntax

accounting lan-access { **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo accounting lan-access

デフォルト

LAN ユーザのアカウンティング方式はデフォルトアカウンティング方式を使用します。

View

ISP domain view

定義済みユーザロール

network-admin

パラメータ

local: ローカルアカウンティングを実行します。

none: アカウンティングを実行しません。

radius-scheme *radius-scheme-name*: RADIUS スキームを指定します。設定範囲は 1～32 です。大文字、小文字を区別しません。

説明

accounting lan-access コマンドは LAN ユーザのアカウンティング方式を設定します。

undo accounting lan-access コマンドはデフォルトに戻します。

1 つのプライマリアカウンティング方式と複数のバックアップのアカウンティング方式を指定することができます。

プライマリアカウンティングが無効であるとき、装置は、順番にバックアップのアカウンティング方式を使用します。たとえば、**accounting lan-access radius-scheme** *radius-scheme-name* **local none** コマンドはプライマリ RADIUS アカウンティング方式と 2 つのバックアップ方式（ローカルアカウンティング方式とアカウンティングがない方式）を指定します。装置はデフォルトで RADIUS アカウンティング方式を実行し、RADIUS サーバが無効であるときローカルアカウンティング方式を実行します。RADIUS アカウンティング方式とローカルアカウンティング方式の両方が無効であるとき、装置はアカウンティング方式を実行しません。

例

ISP ドメイン test の LAN ユーザのローカルアカウンティング方式を設定します。

<Switch> system-view

[Switch] domain test

[Switch-isp-test] accounting lan-access local

LAN ユーザの ISP ドメイン test のアカウンティング方式を設定します。プライマリを RADIUS スキーム rd、バックアップをローカルに設定します。

<Switch> system-view

[Switch] domain test

[Switch-isp-test] accounting lan-access radius-scheme rd local

関連コマンド

- **accounting default**
- **local-user**
- **radius scheme**

1.1.4 accounting login

Syntax

accounting login { **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo accounting login

デフォルト

ログインユーザの ISP ドメインのアカウンティング方式はデフォルトアカウンティング方式を使用します。

View

ISP domain view

定義済みユーザロール

network-admin

パラメータ

local: ローカルアカウンティングを実行します。

none: アカウンティングを実行しません。

radius-scheme *radius-scheme-name*: RADIUS スキーム名を指定します。設定範囲は 1～32 です。大文字、小文字を区別しません。

説明

accounting login コマンドはログインユーザのアカウンティング方式を指定します。

undo accounting login コマンドはデフォルトに戻します。

FTP、SFTP ユーザのアカウンティングはサポートしていません。

1 つのプライマリアカウンティング方式と複数のバックアップのアカウンティング方式を指定することができます。

プライマリアカウンティングが無効であるとき、装置は、順番にバックアップのアカウンティング方式を使用します。たとえば、**accounting login radius-scheme** *radius-scheme-name* **local none** コマンドはプライマリデフォルト RADIUS アカウンティング方式と 2 つのバックアップ方式（ローカルアカウンティング方式とアカウンティングがない方式）を指定します。装置はデフォルトで RADIUS アカウンティング方式を実行し、RADIUS サーバが無効であるときローカルアカウンティング方式を実行します。RADIUS アカウンティング方式とローカルアカウンティング方式の両方が無効であるとき、装置はアカウンティング方式を実行しません。

例

ISP ドメイン test のログインユーザのローカルアカウンティングを設定します。

<Switch> system-view

[Switch] domain test

[Switch-isp-test] accounting login local

ログインユーザの ISP ドメイン test のアカウンティング方式を設定します。プライマリを RADIUS スキーム rd、バックアップをローカルに設定します。

<Switch> system-view

[Switch] domain test

[Switch-isp-test] accounting login radius-scheme rd local

関連コマンド

- **accounting default**
- **local-user**
- **radius scheme**

1.1.5 accounting start-fail

Syntax

accounting start-fail { **offline** | **online** }

undo accounting start-fail

デフォルト

online

View

ISP domain view

定義済みユーザロール

network-admin

パラメータ

offline: アカウンティング開始失敗したとき、ユーザをログオフします。

online: アカウンティング開始失敗したとき、ユーザをオンラインの状態で保持します。

説明

accounting start-fail コマンドはアカウンティング開始に失敗したユーザのアクセス制御を設定します。

undo accounting start-fail コマンドはデフォルトに戻します。

を使用します。

例

ISP ドメイン test で、アカウンティング開始に失敗したとき、ユーザをオンラインの状態で保持します。

<Switch> system-view

[Switch] domain test

[Switch-isp-test] accounting start-fail online

1.1.6 accounting update-fail

Syntax

accounting update-fail { [**max-times** *max-times*] **offline** | **online** }

undo accounting update-fail

デフォルト

online

View

ISP domain view

定義済みユーザロール

network-admin

パラメータ

max-times *max-times*: 各ユーザが連続してアカウンティングの更新に失敗可能な最大数を指定します。設定範囲は 1～255 です。デフォルトは 1 です。

offline: アカウンティングの更新に失敗したとき、ユーザをログオフします。

online: アカウンティングの更新に失敗したとき、ユーザをオンラインの状態で保持します。

説明

accounting update-fail コマンドはすべてのアカウンティングの更新に失敗したユーザのアクセス制御を設定します。

undo accounting update-fail デフォルトに戻すには、を使用します。

例

ISP ドメイン test で、アカウンティングの更新に失敗したとき、ユーザをオンラインの状態で保持します。

<Switch> system-view

[Switch] domain test

[Switch-isp-test] accounting update-fail online

1.1.7 authentication default

Syntax

authentication default { **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo authentication default

デフォルト

local

View

ISP domain view

定義済みユーザロール

network-admin

パラメータ

local: ローカル認証を実行します。

none: 認証を実行しません。

radius-scheme *radius-scheme-name*: RADIUS スキーム名を指定します。設定範囲は 1～32 です。大文字、小文字を区別しません。

説明

authentication default コマンドは ISP ドメインのデフォルト認証方式を指定します。

undo authentication default コマンドはデフォルトに戻します。

デフォルト認証方式は、この方式をサポートするすべてのユーザで使用されます。特定の認証方式は設定されません。

1 つのプライマリデフォルト認証方式と複数のバックアップの認証方式を指定することができます。

プライマリ認証が無効であるとき、装置は、順番にバックアップの認証方式を使用します。たとえば、**authentication default radius-scheme** *radius-scheme-name* **local none** コマンドはプライマリデフォルト RADIUS 認証方式と 2 つのバックアップの方式（ローカル認証方式と認証がない方式）を指定します。装置はデフォルトで RADIUS 認証方式を実行し、RADIUS サーバが無効であるときローカル認証方式を実行します。RADIUS 認証方式とローカル認証方式の両方が無効であるとき、装置は認証を実行しません。

例

ISP ドメイン test のデフォルト認証方式を設定します。プライマリを RADIUS スキーム rd、バックアップをローカルとして設定します。

<Switch> system-view

[Switch] domain test

[Switch-isp-test] authentication default radius-scheme rd local

関連コマンド

- **local-user**
- **radius scheme**

1.1.8 authentication lan-access

Syntax

authentication lan-access { **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo authentication lan-access

デフォルト

LAN ユーザの認証方式はデフォルト認証方式を使用します。

View

ISP domain view

定義済みユーザロール

network-admin

パラメータ

local: ローカル認証を実行します。

none: 認証を実行しません。

radius-scheme *radius-scheme-name*: RADIUS スキーム名を指定します。設定範囲は 1～32 です。大文字、小文字を区別しません。

説明

authentication lan-access コマンドは LAN ユーザの認証方式を設定します。

undo authentication lan-access コマンドはデフォルトに戻します。

1 つのプライマリ認証方式と複数のバックアップの認証方式を指定することができます。

プライマリ認証が無効であるとき、装置は、順番にバックアップの認証方式を使用します。たとえば、**authentication lan-access radius-scheme** *radius-scheme-name* **local none** コマンドはプライマリ RADIUS 認証方式と 2 つのバックアップ方式（ローカル認証方式と認証がない方式）を指定します。装置はデフォルトで RADIUS 認証方式を実行し、RADIUS サーバが無効であるときローカル認証方式を実行します。RADIUS 認証方式とローカル認証方式の両方が無効であるとき、装置は認証を実行しません。

例

ISP ドメイン test の LAN ユーザのローカル認証方式を設定します。

<Switch> system-view

[Switch] domain test

[Switch-isp-test] authentication lan-access local

LAN ユーザの ISP ドメイン test の認証方式を設定します。プライマリを RADIUS スキーム rd、バックアップをローカルに設定します。

<Switch> system-view

[Switch] domain test

[Switch-isp-test] authentication lan-access radius-scheme rd local

関連コマンド

- **authentication default**
- **local-user**
- **radius scheme**

1.1.9 authentication login

Syntax

authentication login { **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo authentication login

デフォルト

ログインユーザの ISP ドメインの認証方式はデフォルト認証方式を使用します。

View

ISP domain view

定義済みユーザロール

network-admin

パラメータ

local: ローカル認証を実行します。

none: 認証を実行しません。

radius-scheme *radius-scheme-name*: RADIUS スキーム名を指定します。設定範囲は 1～32 です。大文字、小文字を区別しません。

説明

authentication login コマンドはログインユーザの認証方式を指定します。

undo authentication login コマンドはデフォルトに戻します。

1 つのプライマリ認証方式と複数のバックアップの認証方式を指定することができます。

プライマリ認証が無効であるとき、装置は、順番にバックアップの認証方式を使用します。たとえば、**authentication login radius-scheme** *radius-scheme-name* **local none** コマンドはプライマリデフォルト RADIUS 認証方式と 2 つのバックアップ方式（ローカ

ル認証方式と認証がない方式）を指定します。装置はデフォルトで RADIUS 認証方式を実行し、RADIUS サーバが無効であるときローカル認証方式を実行します。RADIUS 認証方式とローカル認証方式の両方が無効であるとき、装置は認証を実行しません。

例

ISP ドメイン test のログインユーザのローカル認証を設定します。

<Switch> system-view

[Switch] domain test

[Switch-isp-test] authentication login local

ログインユーザの ISP ドメイン test の認証方式を設定します。プライマリを RADIUS スキーム rd、バックアップをローカルに設定します。

<Switch> system-view

[Switch] domain test

[Switch-isp-test] authentication login radius-scheme rd local

関連コマンド

- **authentication default**
- **local-user**
- **radius scheme**

1.1.10 authorization command

Syntax

authorization command { **local** [**none**] | **none** }

undo authorization command

デフォルト

ISP ドメインのコマンド許可（認可）方式はデフォルト許可方式を使用します。

View

ISP domain view

定義済みユーザロール

network-admin

パラメータ

local: ローカル許可を実行します。

none: 許可を実行しません。許可サーバは、入力されたコマンドがユーザロールで許可されているかどうかを確認しません。ユーザロールがコマンドを許可している場合、コマンドが正常に実行されます。

説明

authorization command コマンドはコマンドの許可方式を指定します。

undo authorization command コマンドはデフォルトに戻します。

入力された各コマンドが許可されているかどうか確認するため、コマンド許可は、許可サーバを使用しログインユーザが入力可能なコマンドのみを実行できるように制限します。

ローカルコマンド許可が設定されているとき、装置は入力された各コマンドとユーザの設定を比較します。ユーザの許可されたユーザロールによって許可されるときのみ、コマンドが実行されます。

実行できるコマンドは、ユーザロールのアクセス許可と許可サーバのコマンド許可の両方で管理されます。アクセス許可の管理は、許可されたユーザロールが入力されたコマンドにアクセスできるかどうかを管理しますが、ユーザロールがこれらのコマンドに許可を取得したかどうかを管理しません。コマンドがアクセス許可によって許可されるが、コマンド許可で許可されていない場合、コマンドは実行できません。

1 つのプライマリコマンド許可方式と複数のバックアップのコマンド許可方式を指定することができます。

デフォルト許可方式が無効であるとき、装置は、順番にバックアップの許可方式を使用します。たとえば、**authorization command local none** コマンドはプライマリデフォルトローカル許可方式と 1 つのバックアップ方式（認証がない方式）を指定します。装置はデフォルトでローカル許可方式を実行し、ローカル許可方式が無効であるとき装置は許可を実行しません。

例

ISP ドメイン test の LAN ユーザのローカルコマンド許可方式を設定します。

<Switch> system-view

[Switch] domain test

[Switch-isp-test] authorization command local

ログインユーザの ISP ドメイン test の認証方式を設定します。プライマリをローカル許可方式、バックアップをコマンド許可なしに設定します。

<Switch> system-view

[Switch] domain test

[Switch-isp-test] authorization command local none

関連コマンド

local-user

1.1.11 authorization default

Syntax

authorization default { **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo authorization default

デフォルト

local

View

ISP domain view

定義済みユーザロール

network-admin

パラメータ

local: ローカル許可を実行します。

none: 許可を実行しません。ユーザが認証にパスしたのち、以下のデフォルト許可情報を適用します。

- ログインユーザがネットワークにアクセスできません。
- ログインユーザはユーザロール Level-0 に割り当てられています。ログインユーザは Telnet、FTP、SFTP、端末ユーザです。端末ユーザはコンソールポートを使用して装置にアクセスできます。Level-0 のユーザロールの詳細は、オペレーションマニュアルのセクション 1 *はじめに* “*RBAC*”を参照してください。
- FTP、SFTP ユーザが作業ディレクトリとして設定した NAS のルートディレクトリを持っていますが、ユーザはルートディレクトリへのアクセス権限がありません。

radius-scheme *radius-scheme-name*: RADIUS スキーム名を指定します。設定範囲は 1～32 です。大文字、小文字を区別しません。

説明

authorization default コマンドは ISP ドメインのデフォルト許可方式を指定します。

undo authorization default コマンドはデフォルトに戻します。

デフォルト許可方式は、この方式をサポートするすべてのユーザで使用されます。特定の許可方式は設定されません。

ISP ドメインの認証方式と許可方式が同じ RADIUS スキームを使用するときのみ RADIUS 許可が適用されます。

1 つのプライマリデフォルト許可方式と複数のバックアップの許可方式を指定することができます。

プライマリ許可が無効であるとき、装置は、順番にバックアップの許可方式を使用します。たとえば、**authorization default radius-scheme** *radius-scheme-name* **local none** コマンドはプライマリデフォルト RADIUS 許可方式と 2 つのバックアップの方式（ローカル許可方式と許可がない方式）を指定します。装置はデフォルトで RADIUS 許可方式を実行し、RADIUS サーバが無効であるときローカル許可方式を実行します。RADIUS 許可方式とローカル許可方式の両方が無効であるとき、装置は許可を実行しません。

例

ISP ドメイン test のデフォルト許可方式を設定します。プライマリを RADIUS スキーム rd、バックアップをローカルとして設定します。

<Switch> system-view

[Switch] domain test

[Switch-isp-test] authorization default radius-scheme rd local

関連コマンド

- **local-user**
- **radius scheme**

1.1.12 authorization lan-access

Syntax

authorization lan-access { **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo authorization lan-access

デフォルト

LAN ユーザの許可方式はデフォルト許可方式を使用します。

View

ISP domain view

定義済みユーザロール

network-admin

パラメータ

local: ローカル許可を実行します。

none: 許可を実行しません。認証された LAN ユーザは直接ネットワークにアクセスします。

radius-scheme *radius-scheme-name*: RADIUS スキームを指定します。設定範囲は 1～32 です。大文字、小文字を区別しません。

説明

authorization lan-access コマンドは LAN ユーザの許可方式を設定します。

undo authorization lan-access コマンドはデフォルトに戻します。

ISP ドメインの認証方式と許可方式が同じ RADIUS スキームを使用するときのみ RADIUS 許可が適用されます。

1 つのプライマリ許可方式と複数のバックアップの許可方式を指定することができます。

プライマリ許可が無効であるとき、装置は、順番にバックアップの許可方式を使用します。たとえば、**authorization lan-access radius-scheme** *radius-scheme-name* **local none** コマンドはプライマリ RADIUS 許可方式と 2 つのバックアップ方式（ローカル許可方式と許可がない方式）を指定します。装置はデフォルトで RADIUS 許可方式を実行し、RADIUS サーバが無効であるときローカル許可方式を実行します。RADIUS 許可方式とローカル許可方式の両方が無効であるとき、装置は許可を実行しません。

例

ISP ドメイン test の LAN ユーザのローカル許可方式を設定します。

<Switch> system-view

[Switch] domain test

[Switch-isp-test] authorization lan-access local

LAN ユーザの ISP ドメイン test の許可方式を設定します。プライマリを RADIUS スキーム rd、バックアップをローカルに設定します。

<Switch> system-view

[Switch] domain test

[Switch-isp-test] authorization lan-access radius-scheme rd local

関連コマンド

- **authorization default**
- **local-user**
- **radius scheme**

1.1.13 authorization login

Syntax

authorization login { **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo authorization login

デフォルト

ログインユーザの ISP ドメインの許可方式はデフォルト許可方式を使用します。

View

ISP domain view

定義済みユーザロール

network-admin

パラメータ

local: ローカル許可を実行します。

none: 許可を実行しません。ユーザが認証にパスしたのち、以下のデフォルト許可情報を適用します。

- ログインユーザはユーザロール Level-0 に割り当てられています。ログインユーザは Telnet、FTP、SFTP、端末ユーザです。端末ユーザはコンソールポートを使用して装置にアクセスできます。Level-0 のユーザロールの詳細は、オペレーションマニュアルのセクション 1 *はじめに* “*RBAC*”を参照してください。
- FTP、SFTP ユーザが作業ディレクトリとして設定した NAS のルートディレクトリを持っていますが、ユーザはルートディレクトリへのアクセス権限がありません。

radius-scheme *radius-scheme-name*: RADIUS スキーム名を指定します。設定範囲は 1～32 です。大文字、小文字を区別しません。

説明

authorization login コマンドはログインユーザの許可方式を指定します。

undo authorization login コマンドはデフォルトに戻します。

ISP ドメインの認証方式と許可方式が同じ RADIUS スキームを使用するときのみ RADIUS 許可が適用されます。

1 つのプライマリ許可方式と複数のバックアップの許可方式を指定することができます。

プライマリ許可が無効であるとき、装置は、順番にバックアップの許可方式を使用します。たとえば、**authorization login radius-scheme** *radius-scheme-name* **local none** コマンドはプライマリデフォルト RADIUS 許可方式と 2 つのバックアップ方式（ローカル許可方式と許可がない方式）を指定します。装置はデフォルトで RADIUS 許可方式を実行し、RADIUS サーバが無効であるときローカル許可方式を実行します。RADIUS 許可方式とローカル許可方式の両方が無効であるとき、装置は許可を実行しません。

例

ISP ドメイン test のログインユーザのローカル許可を設定します。

<Switch> system-view

[Switch] domain test

[Switch-isp-test] authorization login local

ログインユーザの ISP ドメイン test の許可方式を設定します。プライマリを RADIUS スキーム rd、バックアップをローカルに設定します。

<Switch> system-view

[Switch] domain test

[Switch-isp-test] authorization login radius-scheme rd local

関連コマンド

- **authorization default**
- **local-user**
- **radius scheme**

1.1.14 display domain

Syntax

display domain [*isp-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

isp-name: ISP ドメイン名を指定します。設定範囲は 1～255 です。大文字、小文字を区別しません。ISP ドメインを指定しない場合、すべての ISP ドメインの設定を表示します。

説明

display domain コマンドは ISP ドメインの設定を表示します。

例

すべての ISP ドメインの設定を表示します。

<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
  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
    User profile: test
    ACL number: 3000
    User group: ugg
    URL: http://test
    IGMP access number: 4
    MLD access number: 4

Default domain name: system
```

表 1-1 コマンド出力

フィールド	説明
Domain	ISP ドメイン名です。
State	ISP ドメインの状態です。
Default authentication scheme	デフォルト認証方式です。

フィールド	説明
Default authorization scheme	デフォルト許可方式です。
Default accounting scheme	デフォルトアカウンティング方式です。
Login authentication scheme	ログインユーザの認証方式です。
Login authorization scheme	ログインユーザの許可方式です。
Login accounting scheme	ログインユーザのアカウンティング方式です。
Super authentication scheme	装置に再接続を行わず別のユーザロールを取得する認証方式です。
Command authorization scheme	コマンドライン許可方式です。
Command accounting scheme	コマンドラインアカウンティング方式です。
LAN access authentication scheme	LANユーザの認証方式です。
LAN access authorization scheme	LANユーザの許可方式です。
LAN access accounting scheme	LANユーザのアカウンティング方式です。
RADIUS	RADIUSスキームです。
HWTACACS	HWTACACSスキームです。 HWTACACSスキームはサポートしていません。
LDAP	LDAPスキームです。 LDAPスキームはサポートしていません。
Local	ローカルスキームです。
None	認証、許可、アカウンティングがありません。
Accounting start failure action	アカウンティング開始の失敗となるユーザのアクセス制御です。 • **Online**–ユーザがオンライン状態のままとなることを許可します。 • **Offline**–ユーザをログオフします。 このフィールドは現在のソフトウェアバージョンでサポートしていません。
Accounting update failure max-times	ドメインの各ユーザによって、許可されたアカウンティングアップデートが連続して失敗する最大数です。 このフィールドは現在のソフトウェアバージョンでサポートしていません。

フィールド	説明
Accounting update failure action	すべてのアカウンティングアップデート試行に失敗したユーザのアクセス制御です。 ● **Online**–ユーザがオンライン状態のままとなることを許可します。 ● **Offline**–ユーザをログオフします。 このフィールドは現在のソフトウェアバージョンでサポートしていません。
Accounting quota out policy	データ割り当てを使い果たしたユーザの制御です。 ● **Online**–ユーザがオンライン状態のままとなることを許可します。 ● **Offline**–ユーザをログオフします。 このフィールドは現在のソフトウェアバージョンでサポートしていません。
Service type	ISPドメインのサービスタイプです。HIS、STB、VoIPがあります。 このフィールドは現在のソフトウェアバージョンでサポートしていません。
Session time	接続失敗あるいは誤動作によって、ユーザがオフラインとなったため、オンライン時間がサーバに送信されました。 ● **Include idle time**–オンライン時間にアイドルカット期間が含まれます。 ● **Exclude idle time**–オンライン時間にアイドルカット期間が含まれません。
Dual-stack accounting method	dual-stackユーザのアカウンティング方式です。 ● **Merge**–アカウンティングのためIPv4データとIPv6データを併合します。 ● **Separate**–アカウンティングのためIPv6データからIPv4データを分離します。
Authorization attributes	ISPドメインのユーザの許可属性です。
Idle cut	アイドルカット機能の状態です。 **Disabled**と表示されている場合、アイドルカット機能が無効です。 このフィールドは現在のソフトウェアバージョンでサポートしていません。
User profile	許可ユーザプロファイル名です。
ACL number	ユーザの許可ACLです。
User group	ユーザの許可ユーザグループです。

フィールド	説明
URL	ユーザのリダイレクトURLです。
IGMP max access number	IPv4ユーザが同時に加入できるIGMPグループの最大数です。このフィールドは現在のソフトウェアバージョンでサポートしていません。
MLD max access number	IPv6ユーザが同時に加入できるMLDグループの最大数です。このフィールドは現在のソフトウェアバージョンでサポートしていません。

1.1.15 domain

Syntax

domain *isp-name*

undo domain *isp-name*

デフォルト

system

View

System view

定義済みユーザロール

network-admin

パラメータ

isp-name: ISP ドメイン名を指定します。設定範囲は 1～255 です。大文字、小文字を区別しません。

次の記号は使用できません。スラッシュ（/），バックスラッシュ、垂直バー（|）、コーテーションマーク（"）、コロン（:）、アスタリスク（*）、クエスチョンマーク（?）、小なり記号（<）、大なり記号（>）、アットマーク（@）

次のドメイン名は使用できません。(d)、(de)(def)、(defa)、(defau)、(defaul)、(default)、(i)、(if)、(if-)、(if-u)、(if-un)、(if-unk)、(if-unkn)、(if-unkno)、(if-unknow)、(if-unknown)

説明

domain コマンドは ISP ドメインを作成し、ISP domain view に移行します。ISP ドメインが既に存在する場合、その view に移行します。

undo domain コマンドは ISP ドメインを削除します。

作成されたとき、すべての ISP ドメインはアクティブ状態です。

システムには予約済み ISP ドメイン system があり、修正できますが削除することはできません。

デフォルト ISP ドメインは、削除することができません。**undo domain** コマンドを使用する前に、**undo domain default enable** コマンドを使用して、デフォルトでない ISP ドメインを変更してください。

ドメイン名を含むユーザ名は、異なるタイプのユーザの最大長を超過しないように短いユーザ名を使用してください。

例

ISP ドメイン test を作成し、ISP domain view に移行します。

<Switch> system-view

[Switch] domain test

[Switch-isp-test]

関連コマンド

- **display domain**
- **domain default enable**
- **state (ISP domain view)**

1.1.16 domain default enable

Syntax

domain default enable *isp-name*

undo domain default enable

デフォルト

system

View

System view

定義済みユーザロール

network-admin

パラメータ

isp-name: ISP ドメイン名を指定します。設定範囲は 1～255 です。大文字、小文字を区別しません。

説明

domain default enable コマンドはデフォルト ISP ドメインを指定します。ドメイン名が付加されないユーザは、デフォルトドメインであるとみなします。

undo domain default enable コマンドはデフォルトに戻します。

デフォルトの ISP ドメインは 1 つしかありません。

デフォルトの ISP ドメインは、削除することができません。**undo domain** コマンドを使用する前に、**undo domain default enable** コマンドを使用して、デフォルトでない ISP ドメインを変更してください。

例

ISP ドメイン test を作成し、デフォルト ISP ドメインとして設定します。

<Switch> system-view

[Switch] domain test

[Switch-isp-test] quit

[Switch] domain default enable test

関連コマンド

- **display domain**
- **domain**

1.1.17 state (ISP domain view)

Syntax

state { **active** | **block** }

undo state

デフォルト

active

View

ISP domain view

定義済みユーザロール

network-admin

パラメータ

active: ISP ドメインをアクティブ状態にし、ISP ドメイン内のユーザがネットワークサービスを要求できるようにします。

block: ISP ドメインをブロック状態にし、ISP ドメイン内のユーザがネットワークサービスを要求できないようにします。

説明

state コマンドは ISP ドメインの状態を設定します。

undo state コマンドはデフォルトに戻します。

ISP ドメインをブロック状態にすると、このドメイン内のオフラインのユーザは、ネットワークサービスを要求できなくなります。オンラインユーザには影響しません。

例

ISP ドメイン test をブロック状態にします。

<Switch> system-view

[Switch] domain test

[Switch-isp-test] state block

関連コマンド

display domain

1.2 ローカルユーザ設定コマンド

1.2.1 access-limit

Syntax

access-limit *max-user-number*

undo access-limit

デフォルト

ローカルユーザを使用して同時に接続するユーザ数に制限はありません。

View

Local user view

定義済みユーザロール

network-admin

パラメータ

max-user-number: 同時に接続するユーザの最大数です。設定範囲は 1～1024 です。

説明

access-limit コマンドはローカルユーザを使用して同時に接続するユーザの最大数を設定します。

undo access-limit コマンドはデフォルトに戻します。

ローカルユーザでローカルアカウンティングが設定されているときのみ適用されます。

FTP、SFTP ユーザはアカウンティングをサポートしていないため、FTP、SFTP ユーザには適用されません。

例

ローカルユーザ abc を使用して同時に接続するユーザの最大数 5 を設定します。

<Switch> system-view

[Switch] local-user abc

[Switch-luser-manage-abc] access-limit 5

関連コマンド

display local-user

1.2.2 authorization-attribute (local user view/user group view)

Syntax

authorization-attribute { **acl** *acl-number* | **idle-cut** *minutes* **user-profile** *profile-name* | **user-role** *role-name* | **vlan** *vlan-id* | **work-directory** *directory-name* } *

undo authorization-attribute { **acl** | **idle-cut** | **session-timeout** | **user-profile** | **user-role** *role-name* | **vlan** | **work-directory** } *

デフォルト

FTP、SFTPユーザは作業ディレクトリとしてNASのルートディレクトリを設定します。しかし、ユーザはルートディレクトリへのアクセス許可がありません。

network-admin あるいは level-15 のユーザによって作成されたローカルユーザは network-operator のユーザロールが割り当てられています。

View

Local user view

User group view

定義済みユーザロール

network-admin

パラメータ

acl *acl-number*: 許可 ACL を指定します。設定範囲は 2000～3999 です。認証をパスした後、ローカルユーザは ACL で指定されたネットワークリソースにアクセスすることができます。

idle-cut *minute*: アイドルタイムアウト時間を設定します。設定範囲は 1～120 分です。指定されるアイドル時間を超過したアイドル中のオンラインユーザはログアウトされます。

user-profile *profile-name*: 許可ユーザプロファイルを指定します。設定範囲は 1～31 です。大文字、小文字を区別します。ユーザプロファイル名は英字、数字、アンダーライン（_）のみ使用することができます。ユーザプロファイルは認証されたユーザの動作を制限します。

user-role *role-name*: 許可されたユーザロールを指定します。設定範囲は 1～63 です。ユーザに 64 のユーザロールを指定することができます。ユーザロールに関するコマンドの詳細は、コマンドマニュアルのセクション 1 *はじめに*“*RBAC*”を参照してください。このオプションは local user view でのみ有効で、user group view では無効です。

vlan *vlan-id*: 許可 VLAN を指定します。設定範囲は 1～4094 です。認証にパスし、VLAN が許可されたのち、ローカルユーザは VLAN のリソースのみアクセスすることができます。

work-directory *directory-name*: FTP、SFTP ユーザの作業ディレクトリを指定します。設定範囲は 1～255 です。大文字、小文字を区別しません。このディレクトリは既に存在している必要があります。デフォルトで FTP、SFTP ユーザは装置のルートディレクトリにアクセスすることができます。

説明

authorization-attribute コマンドはローカルユーザまたはユーザグループの許可属性を設定します。ローカルユーザ、またはローカルユーザのユーザグループが認証を通過すると、装置はユーザにそれらの属性を割り当てます。

undo authorization-attribute コマンドはデフォルトに戻します。

アプリケーション環境と目的に従って許可属性を設定してください。ユーザのサービスタイプに依存して許可属性をサポートします。

LAN ユーザの場合、許可属性は ACL、ユーザプロファイル、VLAN のみが適用できます。

Telnet、端末ユーザの場合、許可属性はアイドルカット、ユーザロール、作業ディレクトリが適用できます。

HTTP、HTTPS ユーザの場合、許可属性はユーザロールが適用できます。

SSH、FTP ユーザの場合、許可属性はユーザロール、アイドルカット、ユーザロール、作業ディレクトリが適用できます。

ローカルユーザのほかのタイプは適用されません。

ユーザグループで設定された許可属性は、グループのすべてのローカルユーザに影響します。設定と管理の効率を上げるためにローカルユーザをグループ化することができま

す。local user view に設定する許可属性は、user group view に設定する同属性より優先されます。

IRF スタックのマスタ/メンバ装置の切り替えが行われた後、FTP、SFTP ユーザがディレクトリにアクセスできるように、作業ディレクトリに slot 情報を指定しないでください。

ユーザが許可されたユーザロールのみ適用させるため、あらかじめ定義されたユーザロールを削除するために **undo authorization-attribute user-role** コマンドを使用してください。

例

ネットワークアクセスユーザ abc の許可される VLAN を VLAN 2 として設定します。

<Switch> system-view

[Switch] local-user abc class network

[Switch-luser-network-abc] authorization-attribute vlan 2

ユーザグループ abc の許可される VLAN を VLAN3 として設定します。

<Switch> system-view

[Switch] user-group abc

[Switch-ugroup-abc] authorization-attribute vlan 3

関連コマンド

- **display local-user**
- **display user-group**

1.2.3 bind-attribute

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** } *

デフォルト

設定なし

View

Local user view

定義済みユーザロール

network-admin

パラメータ

ip *ip-address*: ユーザの IP アドレスを指定します。このオプションは 802.1X ユーザのみ適用可能です。

location interface *interface-type interface-number*: ユーザのインタフェースを指定します。*interface-type* はインタフェースタイプ、*interface-number* はインタフェース番号を示します。認証にパスするため、ユーザはインタフェースを通してネットワークにアクセスする必要があります。このオプションは LAN ユーザのみ適用可能です。

mac *mac-address*: ユーザの MAC アドレスを指定します。形式は H-H-H です。このオプションは LAN ユーザのみ適用可能です。

vlan *vlan-id*: ユーザが所属する VLAN を指定します。設定範囲は 1～4094 です。このオプションは LAN ユーザのみ適用可能です。

説明

bind-attribute コマンドはローカルユーザのバインディング属性を設定します。

undo bind-attribute コマンドはローカルユーザのバインディング属性を削除します。

ユーザのローカル認証を実行するため、装置はユーザの属性と設定されたバインディング属性を一致させます。ユーザが属性に一致しない、あるいは必要な属性が不足している場合、ユーザは認証に失敗します。

バインディング属性のチェックはすべてのアクセスサービスに適用します。

アクセスサービスにもとづいたユーザのバインディング属性を設定してください。装置はユーザのパケットから取得したすべての属性を確認します。たとえば、802.1X 認証はパケット内のユーザの IP アドレスを含むため、802.1X ユーザの IP アドレスのバインディング属性を設定することができます。しかし MAC アドレス認証は IP アドレスを使用しないため、MAC アドレス認証ユーザの IP アドレスのバインディング属性を設定することはできません。

バインディングするインタフェースタイプはローカルユーザの要件に合わせる必要があります。ユーザのサービスタイプにもとづいてインタフェースの割り当てを設定してください。

- ユーザが 802.1X ユーザの場合、802.1X が有効なレイヤ 2 Ethernet インタフェースを指定してください。
- ユーザが MAC アドレス認証ユーザの場合、MAC アドレス認証が有効なレイヤ 2 Ethernet インタフェースを指定してください。

例

ネットワークアクセスユーザ abc に IP アドレス 3.3.3.3 を割り当てます。

```
<Switch> system-view
[Switch] local-user abc class network
[Switch-luser-network-abc] bind-attribute ip 3.3.3.3
```

関連コマンド

display local-user

1.2.4 display local-user

Syntax

display local-user [**class** { **manage** | **network** } | **idle-cut** { **disable** | **enable** } | **service-type** { **ftp** | **http** | **lan-access** | **ssh** | **telnet** | **terminal** } | **state** { **active** | **block** } | **user-name** *user-name* **class** { **manage** | **network** } | **vlan** *vlan-id*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

class: ローカルユーザタイプを指定します。

- **manage**: 装置管理ユーザを指定します。
- **network**: ネットワークアクセスユーザを指定します。

idle-cut { **disable** | **enable** }: アイドルカット機能が有効、または無効になっているローカルユーザを指定します。

service-type: サービスの指定タイプを使用するローカルユーザを指定します。

- **ftp**: FTP ユーザを指定します。
- **http**: HTTP ユーザを指定します。
- **lan-access**: 801.1x ユーザなど、イーサネット経由でネットワークにアクセスするユーザを指定します。
- **ssh**: SSH ユーザを指定します。
- **telnet**: Telnet ユーザを指定します。
- **terminal**: コンソールポートを使用してログインする端末ユーザを指定します。

state { **active** | **block** }: アクティブまたはブロック状態にあるローカルユーザを指定します。アクティブ状態のローカルユーザは、ネットワークサービスにアクセスできます。ブロック状態のローカルユーザは認証、許可、アカウンティングサービスに要求することができません。

user-name *user-name*: 指定されたユーザ名を使用したすべてのローカルユーザを指定します。設定範囲は 1～55 です。大文字、小文字を区別します。

- ドメイン名を含めることはできません。

- スラッシュ（/），バックスラッシュ、垂直バー（|）、アスタリスク（*）、クエスチョンマーク（?）、小なり記号（<）、大なり記号（>）、アットマーク（@）
- （a）、（al）、（all）は使用できません。

vlan *vlan-id*: VLAN のすべてのローカルユーザを指定します。設定範囲は 1～4094 です。

説明

display local-user コマンドはローカルユーザの設定、オンラインユーザの統計情報を表示します。

パラメータを指定しない場合、すべてのローカルユーザの情報を表示します。

例

すべてのローカルユーザの情報を表示します。

<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.
```

表 1-2 コマンド出力

フィールド	説明
State	ローカルユーザの状態（アクティブまたはブロック）です。
Service Type	ローカルユーザが使用可能なサービスタイプです。
Access limit	同時にログインできる接続数を制限しているかどうかを示します。
Max access number	ローカルユーザ名を使用して同時にログインする最大接続数です。
Current access number	ローカルユーザ名を使用して同時にログインしている現在の接続数です。
User Group	ローカルユーザのグループです。
Bind attributes	ローカルユーザのバインディング属性です。
IP address	ローカルユーザのIPアドレスです。
Location bound	ローカルユーザのバインディングポートです。
MAC address	ローカルユーザのMACアドレスです。
VLAN ID	ローカルユーザのバインディングVLANです。
Authorization attributes	ローカルユーザの許可属性です。
Idle timeout	ユーザのアイドルタイムアウト時間です。単位は分です。
Session-timeout	ユーザのセッションタイムアウト時間です。単位は分です。
Work directory	ユーザがアクセスできるFTP、SFTPのディレクトリです。
ACL Number	ローカルユーザの許可ACLです。
VLAN ID	ローカルユーザの許可VLANです。
User profile	ローカルユーザの許可ユーザプロファイルです。
User role list	ローカルユーザの許可ロールです。

フィールド	説明
URL	ローカルユーザのリダイレクトURLです。
Password control configurations	ローカルユーザで設定されるパスワード管理属性です。
Password aging	パスワードエージング時間です。
Password length	パスワードの最小パスワード長です。
Password composition	パスワードの構成のポリシーです。 • パスワードが含まれる文字タイプの最小数です。 • パスワードの各タイプの最小文字数です。
Password complexity	パスワードの複雑性のポリシーです。 • パスワードにユーザ名あるいはユーザ名の逆の順番を使用しているかどうかを表示します。 • パスワードに文字が3回以上連続して続いているかどうかを表示します。
Maximum login attempts	連続してログインに失敗した最大数です。
Action for exceeding login attempts	ログイン試行後に、ログインに失敗したユーザへの動作です。
Description	ネットワークアクセスユーザの説明です。
Validity period	ネットワークアクセスユーザの有効期間です。
Start date and time	ネットワークアクセスユーザが適用された日時です。
Expiration date and time	ネットワークアクセスユーザの有効期限が終了する日時です。

1.2.5 display user-group

Syntax

display user-group { **all** | **name** *group-name* }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all: すべてのユーザグループを指定します。

name *group-name*: ユーザグループ名を指定します。設定範囲は 1～32 です。大文字、小文字を区別しません。

説明

display user-group コマンドはユーザグループの設定を表示します。

例

すべてのユーザグループの設定を表示します。

<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
```

表 1-3 コマンド出力

フィールド	説明
User group	ユーザグループ名です。
Authorization attributes	ユーザグループの許可属性です。
Idle timeout	アイドルタイムアウト時間です。単位は分です。
Session-timeout	セッションタイムアウト時間です。単位は分です。
Work Directory	グループのユーザがアクセスできるFTP、SFTPのディレクトリです。
ACL Number	許可ACLです。
VLAN ID	許可VLANです。

フィールド	説明
User profile	許可ユーザプロファイルです。
URL	ユーザグループのリダイレクトURLです。
Password control configurations	設定されたユーザグループのパスワード管理属性です。
Password aging	パスワードエージング時間です。
Password length	パスワードの最小パスワード長です。
Password composition	パスワードの構成のポリシーです。 ● パスワードが含まれる文字タイプの最小数です。 ● パスワードの各タイプの最小文字数です。
Password complexity	パスワードの複雑性のポリシーです。 ● パスワードにユーザ名あるいはユーザ名の逆の順番を使用しているかどうかを表示します。 ● パスワードに文字が3回以上連続して続いているかどうかを表示します。
Maximum login attempts	連続してログインに失敗した同時接続最大数です。
Action for exceeding login attempts	ログイン試行後に、ログインに失敗したユーザへの動作です。

1.2.6 group

Syntax

group *group-name*

undo group

デフォルト

ローカルユーザは定義済みユーザグループ system に所属しています。

View

Local user view

定義済みユーザロール

network-admin

パラメータ

group-name: ユーザグループ名を指定します。設定範囲は 1～32 です。大文字、小文字を区別しません。

説明

group コマンドはユーザグループにローカルユーザを割り当てます。

undo group コマンドはデフォルトに戻します。

例

ユーザグループ abc に装置管理ユーザ 111 を割り当てます。

<Switch> system-view

[Switch] local-user 111 class manage

[Switch-luser-manage-111] group abc

関連コマンド

display local-user

1.2.7 local-user

Syntax

local-user *user-name* [**class** { **manage** | **network** }]

undo local-user { *user-name* **class** { **manage** | **network** } | **all** [**service-type** { **ftp** | **http** | **https | lan-access** | **ssh** | **telnet** | **terminal** } | **class** { **manage** | **network** }] }

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

user-name *user-name*: ローカルユーザ名を指定します。設定範囲は 1～55 です。大文字、小文字を区別します。

- ドメイン名を含めることはできません。
- スラッシュ（/），バックスラッシュ、垂直バー（|）、アスタリスク（*）、クエスチョンマーク（?）、小なり記号（<）、大なり記号（>）、アットマーク（@）
- （a）、（al）、（all）は使用できません。

class: ローカルユーザタイプを指定します。指定しない場合、装置管理ユーザを指定します。

- **manage**: 装置管理ユーザを指定します。装置管理ユーザは FTP、HTTP、Telnet、SSH、端末サービスを使用することができます。
- **network**: ネットワークのリソースにアクセスするネットワークアクセスユーザを指定します。ネットワークアクセスユーザは LAN アクセスサービスを使用することができます。

all: すべてのユーザを指定します。

service-type: サービスの指定タイプを使用するローカルユーザを指定します。

- **ftp**: FTP ユーザを指定します。
- **http**: HTTP ユーザを指定します。
- **https**: HTTPS ユーザを指定します。
- **lan-access**: 801.1x ユーザなど、イーサネット経由でネットワークにアクセスするユーザを指定します。
- **ssh**: SSH ユーザを指定します。
- **telnet**: Telnet ユーザを指定します。
- **terminal**: コンソールポートを使用してログインする端末ユーザを指定します。

説明

local-user コマンドはローカルユーザを追加し、local user view に移行します。

undo local-user コマンドはローカルユーザを削除します。

例

装置管理ユーザ user1 を追加し、local user view に移行します。

<Switch> system-view

[Switch] local-user user1 class manage

[Switch-luser-manage-user1]

ネットワークアクセスユーザ user2 を追加し、local user view に移行します。

<Switch> system-view

[Switch] local-user user2 class network

[Switch-luser-network-user2]

関連コマンド

- **display local-user**
- **service-type**

1.2.8 password

Syntax

ネットワークアクセスユーザ：

password { **cipher** | **simple** } *string*

undo password

装置管理ユーザ：

password [{ **hash** | **simple** } *string*]

undo password

デフォルト

ローカルユーザのパスワードは設定されていません。正しいユーザ名を入力し、属性の確認を行った後、認証にパスできます。

View

Local user view

定義済みユーザロール

network-admin

パラメータ

cipher: 暗号テキストのパスワードを設定します。

hash: ハッシュパスワードを設定します。

simple: プレーンテキストのパスワードを設定します。セキュリティのため、プレーンテキストで設定されたパスワードを含めたすべてのパスワードは、暗号化されて保存されます。

string: パスワードを指定します。大文字、小文字を区別します。

- 暗号テキストの設定範囲は 1～117 文字です。
- ハッシュテキストのパスワードは 1～110 文字です。
- プレーンテキストのパスワードは 1～63 文字です。

説明

password コマンドはローカルユーザのパスワードを設定します。

undo password コマンドはローカルユーザのパスワードを削除します。

パラメータを指定しない場合、インタラクティブモードに移行し、プレーンパスワードを設定するようにメッセージが表示されます。装置管理ユーザのみインタラクティブモードでのパスワードの設定がサポートされています。ユーザが正しいユーザ名を入力し、属性の確認にパスした場合、パスワードによるプロテクトの設定が行われていないユーザは認証をパスします。セキュリティのため、各ローカルユーザのパスワードを設定してください。

装置管理ユーザはプレーンテキストパスワードとハッシュパスワードをサポートします。ネットワークアクセスユーザはプレーンテキストパスワードと暗号テキストパスワードをサポートします。

例

装置管理ユーザ user1 のパスワード 123456TESTplat&!をプレーンテキストで設定します。

<Switch> system-view

[Switch] local-user user1 class manage

[Switch-luser-manage-user1] password simple 123456TESTplat&!

装置管理ユーザ test のパスワードをインタラクティブモードで設定します。

<Switch> system-view

[Switch] local-user test class manage

[Switch-luser-manage-test] password

```
Password:
Confirm :
```

ネットワークアクセスユーザ user2 のパスワード 123456TESTplat&!をプレーンテキストで設定します。

<Switch> system-view

[Switch] local-user user2 class network

[Switch-luser-network-user2] password simple 123456TESTuser&!

関連コマンド

display local-user

1.2.9 service-type

Syntax

service-type { **ftp** | **lan-access** | { **http** | **https** | **ssh** | **telnet** | **terminal** } * }

undo service-type { **ftp** | **lan-access** | { **http** | **https** | **ssh** | **telnet** | **terminal** } * }

デフォルト

ローカルユーザは許可されておらず、サービスを使用することができません。

View

Local user view

定義済みユーザロール

network-admin

パラメータ

ftp: ユーザが FTP サービスを使用することを許可します。許可されたディレクトリは **authorization-attribute work-directory** コマンドで変更することができます。

http: HTTP サービスを使用することを許可します。

https: HTTPS サービスを使用することを許可します。

lan-access: ユーザが LAN アクセスサービスを使用することを許可します。一般的にユーザは 802.1X ユーザのようなイーサネットユーザです。

ssh: ユーザが SSH サービスを使用することを許可します。

telnet: ユーザが Telnet サービスを使用することを許可します。

terminal: ユーザが端末サービスを使用し、コンソールポートからログインすることを許可します。

説明

service-type コマンドはローカルユーザが使用するサービスタイプを指定します。

undo service-type コマンドはローカルユーザが使用するサービスタイプを削除します。

複数のサービスタイプをユーザに割り当てることができます。

例

装置管理ユーザ user1 が Telnet、FTP サービスを使用することを許可します。

<Switch> system-view

[Switch] local-user user1 class manage

[Switch-luser-manage-user1] service-type telnet

[Switch-luser-manage-user1] service-type ftp

関連コマンド

display local-user

1.2.10 state (local user view)

Syntax

state { **active** | **block** }

undo state

デフォルト

active

View

Local user view

定義済みユーザロール

network-admin

パラメータ

active: 現在のローカルユーザをアクティブ状態にし、現在のローカルユーザがネットワークサービスを要求できるようにします。

block: 現在のローカルユーザをブロック状態にします。ブロックされたローカルユーザはネットワークサービスを要求できなくなります。

説明

state コマンドはローカルユーザの状態を設定します。

undo state コマンドはデフォルトに戻します。

例

装置管理ユーザ user1 をブロック状態にします。

<Switch> system-view

[Switch] local-user user1 class manage

[Switch-luser-manage-user1] state block

関連コマンド

display local-user

1.2.11 user-group

Syntax

user-group *group-name*

undo user-group *group-name*

デフォルト

システムユーザグループ system

View

System view

定義済みユーザロール

network-admin

パラメータ

group-name: ユーザグループ名を指定します。設定範囲は 1～32 です。大文字、小文字を区別しません。

説明

user-group コマンドはユーザグループを作成し、user group view に移行します。ユーザグループが既に存在する場合、その view に移行します。

undo user-group コマンドはユーザグループを削除します。

ユーザグループはローカルユーザのグループで構成され、ローカルユーザの属性を設定します。グループ内でローカルユーザのユーザ属性の一元管理を実装するために、ユーザグループでローカルユーザの属性を設定することができます。設定可能なユーザ属性は、許可属性です。

ローカルユーザが存在するユーザグループは削除できません。

デフォルトのシステムユーザグループ system は削除できませんが、設定を変更することはできます。

例

ユーザグループ abc を作成し、user group view に移行します。

<Switch> system-view

[Switch] user-group abc

[Switch-ugroup-abc]

関連コマンド

display user-group

1.3 RADIUS設定コマンド

1.3.1 accounting-on enable

Syntax

accounting-on enable [**interval** *interval* | **send** *send-times*] *

undo accounting-on enable

デフォルト

無効

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

interval *interval*: accounting-on パケットを再送する間隔を設定します。設定範囲は 1～15 秒です。デフォルトは 3 秒です。

send *send-times*: accounting-on パケットを送信する試行回数を指定します。設定範囲は 1～255 です。デフォルトは 50 です。

説明

accounting-on enable コマンドは accounting-on 機能を有効にします。

undo accounting-on enable コマンドは accounting-on 機能を無効にします。

accounting-on 機能は装置を再起動したのち、RADIUS サーバに accounting-on パケットを自動で送信します。accounting-on パケットを受信すると RADIUS サーバは装置に対してログインできるようにすべてのオンラインユーザをログアウトします。

次回の装置の再起動時に **accounting-on enable** コマンドを適用させるため、**save** コマンドを実行してください。**save** コマンドの詳細は、コマンドマニュアルのセクション 1 *はじめに* “*コンフィグレーションファイル管理*”を参照してください。

accounting-on enable コマンドのパラメータはコマンドを設定したのち、すぐに適用されます。

例

RADIUS スキーム radius1 で accounting-on 機能を有効にします。accounting-on パケットを再送する間隔を 5 秒に設定し、accounting-on パケットを送信する試行回数を 15 回に設定します。

<Switch> system-view

[Switch] radius scheme radius1

[Switch-radius-radius1] accounting-on enable interval 5 send 15

関連コマンド

display radius scheme

1.3.2 data-flow-format (RADIUS scheme view)

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** }

デフォルト

データフローの単位は **byte**、データパケットの単位は **one-packet** です。

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

data: データフローの単位を指定します。

byte: データフローの単位をバイトで指定します。

giga-byte: データフローの単位をギガバイトで指定します。

kilo-byte: データフローの単位をキロバイトで指定します。

mega-byte: データフローの単位をメガバイトで指定します。

packet: データパケットの単位をバイトで指定します。

giga-packet: データパケットの単位をギガバイトで指定します。

kilo-packet: データパケットの単位をキロバイトで指定します。

mega-packet: データパケットの単位をメガバイトで指定します。

one-packet: データパケットの単位を 1 パケットで指定します。

説明

data-flow-format コマンドはトラフィックの統計情報を送信する際に使用するデータフロー、またはパケットの単位を指定します。

undo data-flow-format コマンドはデフォルトに戻します。

トラフィックの統計情報を送信する際に使用するデータフロー、またはパケットの単位は RADIUS アカウンティングサーバの設定と同一にしてください。そうでなければアカウンティングは正しく実行できません。

例

RADIUS スキーム radius1 でデータフローの単位をキロバイト、パケットの単位をキロパケットに設定します。

<Switch> system-view

[Switch] radius scheme radius1

[Switch-radius-radius1] data-flow-format data kilo-byte packet kilo-packet

関連コマンド

display radius scheme

1.3.3 display radius scheme

Syntax

display radius scheme [*radius-scheme-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

radius-scheme-name: RADIUS スキーム名を指定します。設定範囲は 1～32 です。大文字、小文字を区別しません。RADIUS スキーム名を指定しない場合、すべての RADIUS スキームの設定が表示されます。

説明

display radius scheme コマンドは RADIUS スキームの設定を表示します。

例

すべての RADIUS スキームの設定を表示します。

<Switch> display radius scheme

```
Total 1 RADIUS schemes

------------------------------------------------------------------
RADIUS scheme name: radius1
  Index : 0
  Primary authentication server:
    IP   : 2.2.2.2                          Port: 1812
    VPN  : Not configured
    State: Active
    Test profile: 132
      Probe username: test
      Probe interval: 60 minutes
    Weight: 40
  Primary accounting server:
    IP   : 1.1.1.1                          Port: 1813
    VPN  : Not configured
    State: Active
    Weight: 40
  Second authentication server:
```

```
  IP   : 3.3.3.3                              Port: 1812
  VPN  : Not configured
  State: Block
  Test profile: Not configured
  Weight: 40
Second accounting server:
  IP   : 3.3.3.3                              Port: 1813
  VPN  : Not configured
  State: Block (Mandatory)
  Weight: 0
Accounting-On function                  : Enabled
  extended function                     : Enabled
  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(minutes)     : 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
------------------------------------------------------------------
```

表 1-4 コマンド出力

フィールド	説明
Index	RADIUSスキームのインデックス番号です。
Primary authentication server	プライマリ認証サーバの情報です。
Primary accounting server	プライマリアカウンティングサーバの情報です。
Second authentication server	セカンダリ認証サーバの情報です。

フィールド	説明
Second accounting server	セカンダリアカウンティングサーバの情報です。
IP	サーバのIPアドレスです。 サーバが設定されていない場合、**Not configured**と表示されます。
Port	サーバのサービスポート番号です。ポート番号が指定されていない場合、**Not configured**と表示されます。
VPN	サーバあるいはRADIUSスキームが所属しているVPNインスタンスです。サーバのVPNが指定されていない場合、このフィールドは**Not configured**と表示されます。 このフィールドは現在のソフトウェアバージョンでサポートしていません。
State	サーバの状態です。 ● **Active**–サーバはアクティブ状態です。 ● **Block**–サーバは自動でブロック状態に変更されました。 ● **Block (Mandatory)**–サーバを手動でブロック状態に設定しました。
Test profile	RADIUSサーバのステータス検出で使用されるテストプロファイルです。
Probe username	RADIUSサーバのステータス検出で使用されるユーザ名です。
Probe interval	サーバのステータス検出間隔です。単位は分です。
Weight	RADIUSサーバのWeightです。
Accounting-On function	accounting-on機能が有効にされているかどうかを示します。
extended function	拡張accounting-on機能が有効にされているかどうかを示します。
retransmission times	accounting-onパケット転送の試行回数です。
retransmission interval(seconds)	accounting-onパケットの再送間隔です。単位は秒です。
Timeout Interval(seconds)	RADIUSサーバ応答タイムアウト間隔です。単位は秒です。
Retransmission times	単一RADIUSサーバにRADIUSパケットを転送する最大試行回数です。
Retransmission Times for Accounting Update	アカウンティングの最大試行回数です。
Server Quiet Period(minutes)	サーバの停止間隔です。単位は分です。
Realtime Accounting Interval(minutes)	リアルタイムアカウンティングアップデートの間隔です。単位は分です。

フィールド	説明
Stop-accounting packets buffering	応答されなかったRADIUSストップアカウンティング要求のバッファが有効にされているかどうかを示します。
Retransmission times	単一のRADIUSサーバに送信するストップアカウンティング要求の最大試行回数です。
NAS IP Address	送信するRADIUSパケットの送信元IPアドレスです。
User Name Format	RADIUSサーバに送信されたユーザ名の形式です。以下の値が含まれます。 ● **with-domain**–ドメイン名を含みます。 ● **without-domain**–ドメイン名が除外されています。 ● **keep-original**–受信されたユーザ名をそのままユーザ名として転送します。
Data flow unit	データフローの単位です。
Packet unit	データパケットの単位です。
Attribute 15 check-mode	RADIUSがSSH、FTP、端末ユーザのログインサービス属性をチェックする方式です。 ● **Strict**–SSH、FTP、端末サービスのログインサービスの属性の値がそれぞれ50、51、52に一致するかどうかを確認します。 ● **Loose**–SSH、FTP、端末サービスの標準ログインサービスの属性が0に一致するか確認します。
Attribute 25	RADIUS属性25の中断状態です。 ● **Standard**–CARパラメータとして中断しません。 ● **CAR**–CARパラメータとして中断します。
Attribute Remanent-Volume unit	RADIUS Remanent_Volume属性のデータ単位です。
server-load-sharing	RADIUSサーバロードシェアリング機能の状態です。 ● **Disabled**–ロードシェアリング機能は無効です。装置はプライマリ、セカンダリサーバのロールに従って選択されたサーバにトラフィックを転送します。 ● **Enabled**–ロードシェアリング機能が有効です。ロードシェアリングのため、複数のサーバにトラフィックが分配されます。
Attribute 31 MAC format	RADIUS属性31のMACアドレス形式です。

1.3.4 display radius statistics

Syntax

display radius statistics

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display radius statistics コマンドは RADIUS パケットの統計情報を表示します。

例

RADIUS パケットの統計情報を表示します。

<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
```

表 1-5 コマンド出力

フィールド	説明
Auth.	認証パケットです。
Acct.	アカウンティングパケットです。

フィールド	説明
SessCtrl.	セッションコントロールパケットです。
Request Packet	パケット要求数です。
Retry Packet	パケット要求が再送された数です。
Timeout Packet	パケット要求がタイムアウトした数です。
Access Challenge	アクセスチャレンジを行ったパケット数です。
Account Start	スタートアカウンティング要求のパケット数です。
Account Update	アップデートアカウンティング要求のパケット数です。
Account Stop	ストップアカウンティング要求のパケット数です。
Terminate Request	強制的にユーザをログオフするためのパケット数です。
Set Policy	ユーザ許可情報をアップデートするパケット数です。
Packet With Response	応答が受信されたパケット数です。
Packet Without Response	応答が受信されていないパケット数です。
Access Rejects	アクセス拒否のパケット数です。
Dropped Packet	廃棄されたパケット数です。
Check Failures	チェックサムエラーのパケット数です。

関連コマンド

reset radius statistics

1.3.5 display stop-accounting-buffer (for RADIUS)

Syntax

display stop-accounting-buffer { **radius-scheme** *radius-scheme-name* | **session-id** *session-id* | **time-range** *start-time end-time* | **user-name** *user-name* }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

radius-scheme *radius-scheme-name*: RADIUS スキーム名を指定します。設定範囲は 1～32 です。大文字、小文字を区別しません。

session-id *session-id*: セッションの ID を指定します。設定範囲は 1～64 です。英字を含めることはできません。セッション ID は RADIUS スキームのオンラインユーザを固有に識別します。

time-range *start-time end-time*: タイムレンジを指定します。開始時刻と終了時刻の形式は hh:mm:ss-mm/dd/yyyy あるいは hh:mm:ss-yyyy/mm/dd です。

user-name *user-name*: ユーザ名を指定します。設定範囲は 1～255 文字です。ユーザ名は RADIUS スキームの **user-name-format** コマンドの設定によって、ユーザ名にドメイン名が含まれるかどうかを示します。

説明

display stop-accounting-buffer コマンドは応答が受け付けられずにバッファされた RADIUS ストップアカウンティング要求の情報を表示します。

例

ユーザ abc でバッファされた応答が受け付けられない RADIUS ストップアカウンティング要求の情報を表示します。

<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
```

表 1-6 コマンド出力

フィールド	説明
First sending time	ストップアカウンティング要求が最初に送信されてからの時間です。
Attempts	ストップアカウンティング要求を送信した試行回数です。

関連コマンド

- **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)

Syntax

key { **accounting** | **authentication** } { **cipher** | **simple** } *string*

undo key { **accounting** | **authentication** }

デフォルト

設定なし

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

accounting: セキュアな RADIUS アカウンティングの通信を行うために共有キーを設定します。

authentication: セキュアな RADIUS 認証の通信を行うために共有キーを設定します。

cipher: 暗号テキストの共有キーを設定します。

simple: プレーンテキストの共有キーを設定します。セキュリティのため、プレーンテキストで設定された共有キーを含めたすべての共有キーは、暗号化されて保存されます。

string: 共有キーを指定します。大文字、小文字を区別します。

- 暗号テキストの設定範囲は 1～117 文字です。
- プレーンテキストのパスワードは 1～64 文字です。

説明

key コマンドはセキュリティの高いセキュアな RADIUS 認証、アカウンティング通信を行うために共有キーを設定します。

undo key コマンドはセキュリティの高い RADIUS 認証、アカウンティング通信を行うための共有キーを削除します。

デフォルトに戻します。

このコマンドを使用して設定された共有キーはスキームのすべてのサーバに適用されます。

RADIUS サーバで設定された共有キーと一致していることを確認してください。

指定した RADIUS サーバの共有キーは **key** コマンドで指定された共有キーよりも優先されます。

例

RADIUS スキーム radius1 の共有キーok をプレーンテキストで設定します。

<Switch> system-view

[Switch] radius scheme radius1

[Switch-radius-radius1] key accounting simple ok

関連コマンド

display radius scheme

1.3.7 nas-ip (RADIUS scheme view)

Syntax

nas-ip { *ipv4-address* | **ipv6** *ipv6-address* }

undo nas-ip [**ipv6**]

デフォルト

サーバへ送信されるパケットの送信元 IP アドレスは、system view の **radius nas-ip** コマンドを使用して指定されます。

radius nas-ip コマンドが設定されていない場合、送信元インタフェースのプライマリ IP アドレスがパケットの送信元 IP アドレスとなります。

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

ipv4-address: 装置の IPv4 アドレスを指定します。0.0.0.0、255.255.255.255、クラス D アドレス、クラス E アドレス、ループバックアドレスを指定することはできません。

ipv6 *ipv6-address*: 装置の IPv6 アドレスを指定します。装置のユニキャストアドレスを指定します。ループバックアドレス、リンクローカルアドレスを指定することはできません。

説明

nas-ip コマンドはサーバへ送信される RADIUS パケットの送信元アドレスを設定します。

undo nas-ip コマンドはサーバへ送信される RADIUS パケットの送信元アドレスを削除します。

NAS が送信した RADIUS パケットの送信元 IP アドレスは RADIUS サーバに設定されている NAS の IP アドレスと一致する必要があります。RADIUS サーバは IP アドレスで NAS を識別します。RADIUS パケットを受信すると、RADIUS サーバは、パケットの送信元 IP アドレスが任意の管理 NAS の IP アドレスであるかどうかチェックします。

- パケットの送信元 IP アドレスが管理 NAS の IP アドレスと一致する場合、サーバはパケットを処理します。
- パケットの送信元 IP アドレスが管理 NAS の IP アドレスと一致しない場合、サーバはパケットを廃棄します。

サーバへ送信される RADIUS パケットの送信元アドレスとしてループバックインタフェースの IP アドレスを設定することを推奨します。

nas-ip コマンドと **radius nas-ip** コマンドの両方を使用する場合、以下のガイドラインに従います。

- RADIUS scheme view の **nas-ip** コマンドは、現在の RADIUS スキームにのみ適用されます。
- system view の **radius nas-ip** コマンドは、すべての RADIUS スキームに適用されます。
- RADIUS scheme view の **nas-ip** コマンドで設定されたコマンドは system view の **radius nas-ip** コマンドで設定されたコマンドよりも優先されます。

RADIUS スキームは、発信 RADIUS パケット用に送信元 IPv4 アドレス、送信元 IPv6 アドレスを 1 つだけ設定することができます。同じ RADIUS スキーム用に新しい送信元 IP アドレスを指定する場合、最後に指定されたコマンドが適用されます。

undo nas-ip コマンドで **ipv6** パラメータを指定しない場合、設定された RADIUS パケットの送信元 IPv4 アドレスを削除します。

例

RADIUS スキーム radius1 でサーバへ送信される RADIUS パケットの送信元アドレス 10.1.1.1 を設定します。

```
<Switch> system-view
[Switch] radius scheme radius1
[Switch-radius-radius1] nas-ip 10.1.1.1
```

関連コマンド

- **display radius scheme**
- **radius nas-ip**

1.3.8 primary accounting (RADIUS scheme view)

Syntax

primary accounting { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string*] *

undo primary accounting

デフォルト

設定なし

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

ipv4-address: プライマリ RADIUS アカウンティングサーバの IPv4 アドレスを指定します。

ipv6 *ipv6-address*: プライマリ RADIUS アカウンティングサーバの IPv6 アドレスを指定します。

port-number: プライマリ RADIUS アカウンティングサーバのサービスポート番号を UDP ポート番号で指定します。設定範囲は 1～65535 です。デフォルトは 1813 です。

key: セキュアなプライマリ RADIUS アカウンティングサーバの通信を行うために共有キーを設定します。

cipher: 暗号テキストを指定します。

simple: プレーンテキストを指定します。セキュリティのため、プレーンテキストで設定された共有キーを含めたすべての共有キーは、暗号化されて保存されます。

string: 共有キーを指定します。大文字、小文字を区別します。暗号テキストの設定範囲は 1～117 文字です。プレーンテキストの設定範囲は 1～64 文字です。

説明

primary accounting コマンドはプライマリ RADIUS アカウンティングサーバを指定します。

undo primary accounting コマンドはプライマリ RADIUS アカウンティングサーバの設定を削除します。

プライマリ RADIUS アカウンティングサーバのポート番号と共有キーの設定は、サーバで設定された値と同一にしてください。

スキームのプライマリとセカンダリの 2 つのアカウンティングサーバでホスト名、IP アドレス、ポート番号を同一にすることはできません。

primary accounting コマンドで設定された共有キーは **key accounting** コマンドで設定された共有キーよりも優先されます。

primary accounting コマンドを使用してスタートアカウンティング要求を送信するプライマリアカウンティングサーバを修正あるいは削除する場合、プライマリサーバとの通信はタイムアウトします。

装置はアカウンティングを行うため、もっとも高い優先度のアクティブなサーバと通信をしようとします。

もしアクティブな使用されているアカウンティングサーバを削除する場合、装置はユーザのリアルタイムアカウンティング要求とストップアカウンティング要求を送信しません。ストップアカウンティング要求を保持することはできません。装置は不正確なアカウンティングの結果を生成する可能性があります。

例

RADIUS スキーム radius1 に IP アドレス 10.110.1.2、UDP ポート番号 1813、プレーンテキスト共有キー123456TESTacct&!のプライマリアカウンティングサーバを指定します。

<Switch> system-view

[Switch] radius scheme radius1

[Switch-radius-radius1] primary accounting 10.110.1.2 1813 key simple 123456TESTacct&!

関連コマンド

- **display radius scheme**
- **key (RADIUS scheme view)**
- **secondary accounting (RADIUS scheme view)**

1.3.9 primary authentication (RADIUS scheme view)

Syntax

primary authentication { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string*] *

undo primary authentication

デフォルト

設定なし

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

ipv4-address: プライマリ RADIUS 認証サーバの IPv4 アドレスを指定します。

ipv6 *ipv6-address*: プライマリ RADIUS 認証サーバの IPv6 アドレスを指定します。

port-number: プライマリ RADIUS 認証サーバのサービスポート番号を UDP ポート番号で指定します。設定範囲は 1～65535 です。デフォルトは 1812 です。

key: プライマリ RADIUS 認証サーバとのセキュア通信のための共有鍵を指定します。

cipher: 暗号テキストを指定します。

simple: プレーンテキストを指定します。セキュリティのため、プレーンテキストで設定された共有キーを含めたすべての共有キーは、暗号化されて保存されます。

string: 共有キーを指定します。大文字、小文字を区別します。暗号テキストの設定範囲は 1～117 文字です。プレーンテキストの設定範囲は 1～64 文字です。

説明

primary authentication コマンドはプライマリ RADIUS 認証サーバを指定します。

undo primary authentication コマンドはプライマリ RADIUS 認証サーバの設定を削除します。

プライマリ RADIUS 認証サーバのポート番号と共有キーの設定は、サーバで設定された値と同一にしてください。

スキームのプライマリとセカンダリの 2 つの認証サーバでホスト名、IP アドレス、ポート番号を同一にすることはできません。

primary authentication コマンドで設定された共有キーは **key authentication** コマンドで設定された共有キーよりも優先されます。

primary authentication コマンドを使用して認証の処理中にプライマリ認証サーバを修正あるいは削除する場合、プライマリサーバとの通信はタイムアウトします。

装置は認証を行うため、もっとも高い優先度のアクティブなサーバと通信をしようとします。

例

RADIUS スキーム radius1 に IP アドレス 10.110.1.1、UDP ポート番号 1812、プレーンテキスト共有キー123456TESTauth&!のプライマリ認証サーバを指定します。

<Switch> system-view

[Switch] radius scheme radius1

[Switch-radius-radius1] primary authentication 10.110.1.1 1812 key simple 123456TESTauth&!

関連コマンド

- **display radius scheme**
- **key (RADIUS scheme view)**
- **secondary authentication (RADIUS scheme view)**

1.3.10 radius dscp

Syntax

radius [**ipv6**] **dscp** *dscp-value*

undo radius [**ipv6**] **dscp**

デフォルト

0

View

System view

定義済みユーザロール

network-admin

パラメータ

ipv6: IPv6 RADIUS パケットを指定します。指定しない場合、IPv4 RADIUS パケットの DSCP 値を設定します。

dscp-value: RADIUS パケットの DSCP 値を指定します。設定範囲は 0～63 です。値が大きいほど、優先度は高くなります。

説明

radius dscp コマンドは RADIUS パケットの DSCP 値を設定します。

undo radius dscp コマンドはデフォルトに戻します。

RADIUS パケットの優先度を変更するため、ToS フィールドの DSCP 値を設定します。

例

IPv4 RADIUS パケットの DSCP 値を 10 に設定します。

<Switch> system-view

[Switch] radius dscp 10

1.3.11 radius nas-ip

Syntax

radius nas-ip { *ipv4-address* | **ipv6** *ipv6-address* }

undo radius nas-ip { *ipv4-address* | **ipv6** *ipv6-address* }

デフォルト

サーバへ送信されるパケットの送信元 IP アドレスは、送信元インタフェースの IP アドレスがパケットの送信元 IP アドレスとなります。

View

System view

定義済みユーザロール

network-admin

パラメータ

ipv4-address: 装置の IPv4 アドレスを指定します。0.0.0.0、255.255.255.255、クラス D アドレス、クラス E アドレス、ループバックアドレスを指定することはできません。

ipv6 *ipv6-address*: 装置の IPv6 アドレスを指定します。装置のユニキャストアドレスを指定します。ループバックアドレス、リンクローカルアドレスを指定することはできません。

説明

radius nas-ip コマンドはサーバへ送信される RADIUS パケットの送信元アドレスを設定します。

undo radius nas-ip コマンドはサーバへ送信される RADIUS パケットの送信元アドレスを削除します。

NAS が送信した RADIUS パケットの送信元 IP アドレスは RADIUS サーバに設定されている NAS の IP アドレスと一致する必要があります。RADIUS サーバは IP アドレスで NAS を識別します。RADIUS パケットを受信すると、RADIUS サーバは、パケットの送信元 IP アドレスが任意の管理 NAS の IP アドレスであるかどうかチェックします。

- パケットの送信元 IP アドレスが管理 NAS の IP アドレスと一致する場合、サーバはパケットを処理します。
- パケットの送信元 IP アドレスが管理 NAS の IP アドレスと一致しない場合、サーバはパケットを廃棄します。

サーバへ送信される RADIUS パケットの送信元アドレスが指定されていない場合、サーバから戻ったパケットは物理ポートエラーとして装置に到着することができません。

nas-ip コマンドと **radius nas-ip** コマンドの両方を使用する場合、以下のガイドラインに従います。

- RADIUS scheme view の **nas-ip** コマンドは、現在の RADIUS スキームにのみ適用されます。
- system view の **radius nas-ip** コマンドは、すべての RADIUS スキームに適用されます。
- RADIUS scheme view の **nas-ip** コマンドで設定されたコマンドは system view の **radius nas-ip** コマンドで設定されたコマンドよりも優先されます。

新しい送信元 IPv4 アドレスあるいは IPv6 アドレスを指定する場合、最後に指定されたコマンドが適用されます。

例

サーバへ送信される RADIUS パケットの送信元アドレス 129.10.10.1 を設定します。

<Switch> system-view

[Switch] radius nas-ip 129.10.10.1

関連コマンド

nas-ip (RADIUS scheme view)

1.3.12 radius scheme

Syntax

radius scheme *radius-scheme-name*

undo radius scheme *radius-scheme-name*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

radius-scheme-name: RADIUS スキーム名を指定します。設定範囲は 1～32 です。大文字、小文字を区別しません。

説明

radius scheme コマンドは RADIUS スキームを作成し、RADIUS scheme view に移行します。

undo radius scheme コマンドは RADIUS スキームを削除します。

RADIUS スキームは、同時に 2 つ以上の ISP ドメインで使用されることがあります。

装置は最大 16 までの RADIUS スキームをサポートしています。

例

RADIUS スキーム radius1 を作成し、RADIUS scheme view に移行します。

<Switch> system-view

[Switch] radius scheme radius1

[Switch-radius-radius1]

関連コマンド

display radius scheme

1.3.13 reauthentication server-select

Syntax

reauthentication server-select { **inherit** | **reselect** }

undo reauthentication server-select

デフォルト

inherit

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

inherit: 認証を実行した RADIUS サーバを再認証に使用します。

reselect: 再認証のために RADIUS サーバを再選択します。

説明

reauthentication server-select コマンドは再認証を行うために RADIUS サーバの選択モードを設定します。

undo reauthentication server-select コマンドはデフォルトに戻します。

コマンドは再認証を行う際に、RADIUS サーバの選択メカニズムを設定します。ネットワークの状況に従い、以下のモードのどちらかを使用します。

- **Inherit**—装置は、ユーザの認証を実行した RADIUS サーバを使用して、そのユーザの再認証を実行します。このモードでは、再認証に使用される時間が短縮されます。ただし、RADIUS サーバに到達できない場合、再認証は失敗します。
- **Reselect**—装置は、ユーザの再認証を実行するために到達可能な RADIUS サーバを検索します。このモードは、inherit モードよりも時間がかかります。ただし、このモードでは、装置が再認証に最適な到達可能な RADIUS サーバを見つけることができます。RADIUS サーバの選択には、次の要因が影響します。
  - 設定順を含む RADIUS スキームのサーバ設定。
  - RADIUS サーバのロードシェアリング機能の有効化状態。
  - RADIUS スキーム内の RADIUS サーバの状態。

例

RADIUS スキーム radius1 で再認証を行うために RADIUS サーバの選択モードを reselect に設定します。

<Switch> system-view

[Switch] radius scheme radius1

[Switch-radius-radius1] reauthentication server-select reselect

関連コマンド

display radius scheme

1.3.14 reset radius statistics

Syntax

reset radius statistics

View

User view

定義済みユーザロール

network-admin

説明

reset radius statistics コマンドは、RADIUS 統計情報を削除します。

例

RADIUS 統計情報を削除します。

<Switch> reset radius statistics

関連コマンド

display radius statistics

1.3.15 reset stop-accounting-buffer (for RADIUS)

Syntax

reset stop-accounting-buffer { **radius-scheme** *radius-scheme-name* | **session-id** *session-id* | **time-range** *start-time end-time* | **user-name** *user-name* }

View

User view

定義済みユーザロール

network-admin

パラメータ

radius-scheme *radius-scheme-name*: RADIUS スキーム名を指定します。設定範囲は 1～32 です。大文字、小文字を区別しません。

session-id *session-id*: セッションの ID を指定します。設定範囲は 1～64 です。英字を含めることはできません。セッション ID は RADIUS スキームのオンラインユーザを固有に識別します。

time-range *start-time end-time*: タイムレンジを指定します。開始時刻と終了時刻の形式は hh:mm:ss-mm/dd/yyyy あるいは hh:mm:ss-yyyy/mm/dd です。

user-name *user-name*: ユーザ名を指定します。設定範囲は 1～255 文字です。ユーザ名は RADIUS スキームの **user-name-format** コマンドの設定によって、ユーザ名にドメイン名が含まれるかどうかを示します。

説明

reset stop-accounting-buffer コマンドは応答が受け付けられずにバッファされた RADIUS ストップアカウンティング要求の情報を削除します。

例

ユーザ user0001@test にバッファされた RADIUS ストップアカウンティング要求の情報を削除します。

<Switch> reset stop-accounting-buffer user-name user0001@test

2015 年 8 月 31 日の 0:0:0 から 23:59:59 の間にバッファされた RADIUS ストップアカウンティング要求の情報を削除します。

<Switch> reset stop-accounting-buffer time-range 0:0:0-08/31/2015 23:59:59-08/31/2015

関連コマンド

- **display stop-accounting-buffer (for RADIUS)**
- **stop-accounting-buffer enable (RADIUS scheme view)**

1.3.16 retry

Syntax

retry *retries*

undo retry

デフォルト

3

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

retries: RADIUS パケットの再送信の最大試行回数を設定します。設定範囲は 1～20 です。

説明

retry コマンドは 1 つの RADIUS サーバに再送 RADIUS パケットを送信する最大試行回数を設定します。

undo retry コマンドはデフォルトに戻します。

RADIUS はデータ送信に UDP パケットを使用しているため、通信に信頼性がありません。

装置が応答タイムアウト時間以内に RADIUS サーバから要求に対する応答を受信しない場合、装置は RADIUS 要求を再送します。タイムアウト時間を設定する場合、**timer response-timeout** コマンドを使用します。

再送の試行回数が上限に達しても、RADIUS サーバから応答がない場合、装置は要求が失敗したとみなします。

クライアントが認証プロセスの間にタイムアウトした場合、ユーザはすぐにログオフします。ユーザのログオフを防ぐため、以下によって乗算した値は、アクセスモジュールによって定義したクライアントのタイムアウト時間よりも大きくすることができません。

- RADIUS パケットの最大試行回数
- RADIUS サーバ応答タイムアウト時間
- RADIUS スキームの RADIUS 認証サーバ数

装置が新しい RADIUS サーバに RADIUS 要求を送信するとき、RADIUS パケットを転送する総時間を確認してください。総時間が 300 秒を超過した場合、次の RADIUS サーバへの RADIUS 要求の送信を停止します。

パケットの再送試行回数と RADIUS サーバの応答タイムアウト時間を設定する際に、RADIUS サーバの数を考慮してください。

例

RADIUS スキーム radius1 の再送 RADIUS パケットの最大試行回数を 5 に設定します。

<Switch> system-view

[Switch] radius scheme radius1

[Switch-radius-radius1] retry 5

関連コマンド

- **radius scheme**
- **timer response-timeout (RADIUS scheme view)**

1.3.17 retry realtime-accounting

Syntax

retry realtime-accounting *retries*

undo retry realtime-accounting

デフォルト

5

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

retries: アカウンティング要求の再送信の最大試行回数を設定します。設定範囲は 1～255 です。

説明

retry realtime-accounting コマンドはアカウンティング要求を再送信する最大試行回数を設定します。

undo retry realtime-accounting コマンドはデフォルトに戻します。

通常、RADIUS アカウンティングサーバはタイムアウトタイマを使用して、ユーザがオンラインかどうかを確認します。タイムアウト時間内にサーバがリアルタイムアカウンティング要求を受信しない場合、回線または装置に不具合があるとみなします。サーバはユーザのアカウンティングを停止します。

この状況は、予期しない不具合が生じた場合に起こります。この場合、NAS は、アカウンティング要求の再送の最大試行回数に応じて、ユーザを適宜に切断するよう要求されます。最大回数に達しても応答がない場合、NAS は、ユーザを切断します。

たとえば、以下の条件があると仮定します。

- RADIUS サーバの応答タイムアウト時間が 3 秒とします。(**timer response-timeout** コマンドで設定します)
- RADIUS パケットの再送試行回数が 3 回とします。(**retry** コマンドで設定します)
- リアルタイムアカウンティング間隔が 12 分とします。(**timer realtime-accounting** コマンドで設定します。)
- アカウンティング要求を送信する最大試行回数が 5 回(**retry realtime-accounting** コマンドで設定します。)とします。

装置は 12 分ごとにアカウンティング要求を生成し、3 秒以内に応答がなければ、要求を再送します。3 回要求を送信する間に応答がなければアカウンティングは失敗とみなし、別のアカウンティングを試行します。5 回連続してアカウンティングの送信が失敗した場合、装置はユーザ接続を切断します。

例

RADIUS スキーム radius1 のアカウンティング要求を送信する最大試行回数を 10 に設定します。

<Switch> system-view

[Switch] radius scheme radius1

[Switch-radius-radius1] retry realtime-accounting 10

関連コマンド

- **retry**
- **timer realtime-accounting (RADIUS scheme view)**
- **timer response-timeout (RADIUS scheme view)**

1.3.18 retry stop-accounting (RADIUS scheme view)

Syntax

retry stop-accounting *retries*

undo retry stop-accounting

デフォルト

500

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

retries: 再送試行回数を指定します。設定範囲は 10～65535 です。

説明

retry stop-accounting コマンドは各 RADIUS ストップアカウンティング要求の最大試行回数を設定します。

undo retry stop-accounting コマンドはデフォルトに戻します。

ストップアカウンティング要求の試行回数は以下のパラメータと同時に管理します。

- RADIUS サーバ応答タイムアウトタイマ（**timer response-timeout** コマンドで設定します。）
- RADIUS パケットを送信する最大試行回数（**retry** コマンドで設定します。）

たとえば、以下の条件があると仮定します。

- RADIUS サーバの応答タイムアウト時間が 3 秒とします。
- アカウンティング要求を送信する最大試行回数が 5 回とします。
- ストップアカウンティング要求の最大試行回数が 20 回とします。

装置が 3 秒以内に応答を受信しない場合、ストップアカウンティング要求を再送します。5 回再送する間に応答がない場合、装置はその要求をバッファに保存します。別の要求を再送します。20 回連続で試行が失敗した場合、装置は要求を廃棄します。

例

RADIUS スキーム radius1 のストップアカウンティング要求の最大試行回数を 1000 に設定します。

<Switch> system-view

[Switch] radius scheme radius1

[Switch-radius-radius1] retry stop-accounting 1000

関連コマンド

- **display stop-accounting-buffer (for RADIUS)**
- **retry**
- **timer response-timeout (RADIUS scheme view)**

1.3.19 secondary accounting (RADIUS scheme view)

Syntax

secondary accounting { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string*] *

undo secondary accounting [{ *ipv4-address* | **ipv6** *ipv6-address* } [*port-number*]]

デフォルト

設定なし

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

ipv4-address: セカンダリ RADIUS アカウンティングサーバの IPv4 アドレスを指定します。

ipv6 *ipv6-address*: セカンダリ RADIUS アカウンティングサーバの IPv6 アドレスを指定します。

port-number: セカンダリ RADIUS アカウンティングサーバのサービスポート番号を UDP ポート番号で指定します。設定範囲は 1～65535 です。デフォルトは 1813 です。

key: セキュアなセカンダリ RADIUS アカウンティングサーバの通信を行うために共有キーを設定します。

cipher: 暗号テキストを指定します。

simple: プレーンテキストを指定します。セキュリティのため、プレーンテキストで設定された共有キーを含めたすべての共有キーは、暗号化されて保存されます。

string: 共有キーを指定します。大文字、小文字を区別します。暗号テキストの設定範囲は 1～117 文字です。プレーンテキストの設定範囲は 1～64 文字です。

説明

secondary accounting コマンドはセカンダリ RADIUS アカウンティングサーバを指定します。

undo secondary accounting コマンドはセカンダリ RADIUS アカウンティングサーバを削除します。

セカンダリ RADIUS アカウンティングサーバのポート番号と共有キーの設定は、サーバで設定された値と同一にしてください。

RADIUS スキームに最大 16 のセカンダリ RADIUS アカウンティングサーバを設定することができます。プライマリサーバが故障したとき、装置はアクティブ状態のセカンダリサーバと通信しようとします。装置は設定された順番でセカンダリサーバと接続します。

スキームのプライマリとセカンダリの 2 つのアカウンティングサーバでホスト名、IP アドレス、ポート番号を同一にすることはできません。

secondary accounting コマンドで設定された共有キーは **key accounting** コマンドで設定された共有キーよりも優先されます。

secondary accounting コマンドを使用してスタートアカウンティング要求を送信するセカンダリアカウンティングサーバを修正あるいは削除する場合、セカンダリサーバとの通信はタイムアウトします。

装置はアカウンティングを行うため、もっとも高い優先度のアクティブなサーバと通信をしようとします。

もしアクティブな使用されているアカウンティングサーバを削除する場合、装置はユーザのリアルタイムアカウンティング要求とストップアカウンティング要求を送信しません。ストップアカウンティング要求を保持することはできません。

例

RADIUS スキーム radius1 に IP アドレス 10.110.1.1、UDP ポート番号 1813 のセカンダリアカウンティングサーバを指定します。

<Switch> system-view

[Switch] radius scheme radius1

[Switch-radius-radius1] secondary accounting 10.110.1.1 1813

RADIUS スキーム radius2 の 2 つのセカンダリアカウンティングサーバの IP アドレスを 10.110.1.1 と 10.110.1.2、UDP ポートを 1813 に指定します。

<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

関連コマンド

- **display radius scheme**
- **key (RADIUS scheme view)**
- **primary accounting (RADIUS scheme view)**

1.3.20 secondary authentication (RADIUS scheme view)

Syntax

secondary authentication { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string*] *

undo secondary authentication [{ **ipv4-address** | **ipv6** *ipv6-address* } [*port-number*]]

デフォルト

設定なし

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

ipv4-address: セカンダリ RADIUS 認証サーバの IPv4 アドレスを指定します。

ipv6 *ipv6-address*: セカンダリ RADIUS 認証サーバの IPv6 アドレスを指定します。

port-number: セカンダリ RADIUS 認証サーバのサービスポート番号を UDP ポート番号で指定します。設定範囲は 1～65535 です。デフォルトは 1812 です。

key: プライマリ RADIUS 認証サーバのサービスポート番号を UDP ポート番号で指定します。

cipher: 暗号テキストを指定します。

simple: プレーンテキストを指定します。セキュリティのため、プレーンテキストで設定された共有キーを含めたすべての共有キーは、暗号化されて保存されます。

string: 共有キーを指定します。大文字、小文字を区別します。暗号テキストの設定範囲は 1～117 文字です。プレーンテキストの設定範囲は 1～64 文字です。

説明

secondary authentication コマンドはセカンダリ RADIUS 認証サーバを指定します。

undo secondary authentication コマンドはセカンダリ RADIUS 認証サーバの設定を削除します。

セカンダリ RADIUS 認証サーバのポート番号と共有キーの設定は、サーバで設定された値と同一にしてください。

RADIUS スキームに最大 16 のセカンダリ RADIUS 認証サーバを設定することができます。プライマリサーバが故障したとき、装置はアクティブ状態のセカンダリサーバと通信しようとします。装置は設定された順番でセカンダリサーバと接続します。

スキームのプライマリとセカンダリの 2 つの認証サーバでホスト名、IP アドレス、ポート番号を同一にすることはできません。

secondary authentication コマンドで設定された共有キーは **key authentication** コマンドで設定された共有キーよりも優先されます。

secondary authentication コマンドを使用して認証の処理中にセカンダリ認証サーバを修正あるいは削除する場合、セカンダリサーバとの通信はタイムアウトします。

装置は認証を行うため、もっとも高い優先度のアクティブなサーバと通信をしようとします。

例

RADIUS スキーム radius1 に IP アドレス 10.110.1.2、UDP ポート番号 1812 のセカンダリ認証サーバを指定します。

<Switch> system-view

[Switch] radius scheme radius1

[Switch-radius-radius1] secondary authentication 10.110.1.2 1812

RADIUS スキーム radius2 の 2 つのセカンダリ認証サーバの IP アドレスを 10.110.1.1 と 10.110.1.2、UDP ポートを 1812 に指定します。

<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

関連コマンド

- **display radius scheme**
- **key (RADIUS scheme view)**
- **primary authentication (RADIUS scheme view)**

1.3.21 snmp-agent trap enable 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**] *

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

パラメータ

accounting-server-down: RADIUS アカウンティングサーバに到達不能になったとき、notification を送信します。

accounting-server-up: RADIUS アカウンティングサーバに到達可能になったとき、notification を送信します。

authentication-error-threshold: 認証の失敗がしきい値を超過したとき、notification を送信します。しきい値は認証を試行する総数に対する認証失敗の割合を示します。設定範囲は 1～100%です。デフォルトは 30%です。しきい値は MIB を通してのみ設定できます。

authentication-server-down: RADIUS 認証サーバに到達不能になったとき、notification を送信します。

authentication-server-up: RADIUS 認証サーバに到達可能になったとき、notification を送信します。

説明

snmp-agent trap enable radius コマンドは RADIUS の SNMP notification（inform あるいはトラップ）の通知を有効にします。

undo snmp-agent trap enable radius コマンドは RADIUS の SNMP notification（inform あるいはトラップ）の通知を無効にします。

パラメータを指定しない場合、RADIUS のすべてのタイプの notification を指定します。

RADIUS の SNMP notification が有効であるとき、SNMP エージェントは RADIUS によって作成された以下の notification をサポートします。

- **RADIUS server unreachable notification**－RADIUS サーバに通信できません。指定した RADIUS 要求の再送信の最大試行回数以内にアカウンティング要求あるいは認証要求に対する応答を受信できない場合、RADIUS は notification を作成します。
- **RADIUS server reachable notification**－RADIUS サーバと通信できます。RADIUS サーバが停止タイマの満了後、以前にブロックされた RADIUS サーバに対して notification を作成します。
- **Excessive authentication failures notification**－認証を行った際、失敗した総数が指定したしきい値を超過しています。

例

SNMP エージェントが RADIUS アカウンティングサーバに到達不能になったとき、notification を送信します。

<Switch> system-view

[Switch] snmp-agent trap enable radius accounting-server-down

1.3.22 state primary

Syntax

state primary { **accounting** | **authentication** } { **active** | **block** }

デフォルト

active

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

accounting: プライマリ RADIUS アカウンティングサーバの状態を設定します。

authentication: プライマリ RADIUS 認証サーバの状態を設定します。

active: RADIUS サーバの状態を **active**（正常稼動の状態）に設定します。

block: RADIUS サーバの状態を **block**（サービス外の状態）に設定します。

説明

state primary コマンドはプライマリ RADIUS サーバの状態を設定します。

プライマリサーバがアクティブ状態であるとき、装置は最初にプライマリサーバと通信しようとします。プライマリサーバが使用できない場合、以下の処理を行います。

- プライマリサーバの状態をブロックに変更します。
- サーバの停止タイマを開始します。
- アクティブ状態のセカンダリサーバと通信します。

プライマリサーバの停止タイマがタイムアウトすると、サーバの状態が自動的にアクティブに変化します。停止タイマがタイムアウトする前にサーバの状態をブロックに設定した場合、手動でアクティブ状態に設定しない限り、サーバが自動的にアクティブ状態に戻ることはありません。

プライマリサーバとすべてのセカンダリサーバがブロック状態であるとき、装置はプライマリサーバと通信しようとします。

例

RADIUS スキーム radius1 のプライマリ認証サーバの状態を block に設定します。

<Switch> system-view

[Switch] radius scheme radius1

[Switch-radius-radius1] state primary authentication block

関連コマンド

- **display radius scheme**
- **state secondary**

1.3.23 state secondary

Syntax

state secondary { **accounting** | **authentication** } [{ *ipv4-address* | **ipv6** *ipv6-address* } [*port-number*]] { **active** | **block** }

デフォルト

active

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

accounting: セカンダリ RADIUS アカウンティングサーバの状態を設定します。

authentication: セカンダリ RADIUS 認証サーバの状態を設定します。

ipv4-address: セカンダリ RADIUS サーバの IPv4 アドレスを指定します。

ipv6 *ipv6-address*: セカンダリ RADIUS サーバの IPv6 アドレスを指定します。

port-number: セカンダリ RADIUS サーバのサービスポート番号を UDP ポート番号で指定します。設定範囲は 1～65535 です。セカンダリ RADIUS 認証サーバのデフォルトは 1812 です。セカンダリ RADIUS アカウンティングサーバのデフォルトは 1813 です。

active: RADIUS サーバの状態を **active**（正常稼動の状態）に設定します。

block: RADIUS サーバの状態を **block**（サービス外の状態）に設定します。

説明

state secondary コマンドはセカンダリ RADIUS サーバの状態を設定します。

IP アドレスが設定されていない場合、このコマンドはすべてのセカンダリサーバの状態を変更します。

装置がアクティブ状態のセカンダリサーバと通信できないことを知った場合、以下の処理を行います。

- 装置はセカンダリサーバの状態をブロックに変更します。
- サーバの停止タイマを開始します。
- 別のアクティブ状態のセカンダリサーバと通信しようとします。

サーバの停止タイマがタイムアウトとなった場合、サーバの状態は自動的にアクティブに変化します。タイマがタイムアウトする前にサーバをブロックの状態にした場合、そのサーバの状態は、手動で切り替えない限り自動的にはアクティブに戻ることはありません。すべてのセカンダリサーバが到達不能である場合、装置は認証あるいはアカウンティングに失敗します。

例

RADIUS スキーム radius1 のすべてのセカンダリ認証サーバの状態を block に設定します。

<Switch> system-view

[Switch] radius scheme radius1

[Switch-radius-radius1] state secondary authentication block

関連コマンド

- **display radius scheme**
- **state primary**

1.3.24 stop-accounting-buffer enable (RADIUS scheme view)

Syntax

stop-accounting-buffer enable

undo stop-accounting-buffer enable

デフォルト

有効

View

RADIUS scheme view

定義済みユーザロール

network-admin

説明

stop-accounting-buffer enable コマンドは応答を受け付けられない RADIUS ストップアカウンティング要求のバッファを有効にします。

undo stop-accounting-buffer enable コマンドは応答を受け付けられない RADIUS ストップアカウンティング要求のバッファを無効にします。

RADIUS ストップアカウンティング要求が最大試行回数（**retry** コマンドで設定します）に到達しても応答がない要求をバッファに記録します。装置はサーバの応答を受信するか、ストップアカウンティング要求の試行回数が上限になるまでバッファされた要求を

再送します。試行回数が上限になった場合、装置は RADIUS ストップアカウンティング要求を廃棄します。しかし、もしアカウンティングサーバを削除した場合、サーバ向けのストップアカウンティング要求はバッファに記録されません。

例

応答を受け付けられない RADIUS ストップアカウンティング要求のバッファを有効にします。

<Switch> system-view

[Switch] radius scheme radius1

[Switch-radius-radius1] stop-accounting-buffer enable

関連コマンド

- **display stop-accounting-buffer (for RADIUS)**
- **reset stop-accounting-buffer (for RADIUS)**

1.3.25 timer quiet (RADIUS scheme view)

Syntax

timer quiet *minutes*

undo timer quiet

デフォルト

5 分

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

minutes: サーバの停止タイマを指定します。設定範囲は 0～255 です。0 に設定した場合、装置はユーザの認証またはアカウンティング要求をそのサーバに送信しようとした後、到達不能なサーバの状態をブロックに変更しません。その結果、装置が後続のユーザに認証またはアカウンティング要求を送信しようとすると、サーバはまだアクティブ状態であるため、装置は引き続きそのサーバに要求を送信しようとします。

説明

timer quiet コマンドは RADIUS スキームの指定されたサーバの停止タイマを設定します。

undo timer quiet コマンドはデフォルトに戻します。

サーバの停止タイマが正しく設定されていることを確認してください。

タイマが短すぎる場合、装置がアクティブ状態の通信不能サーバと繰り返し通信しようとするため、頻繁に認証またはアカウンティングの失敗が発生します。

タイマが長すぎる場合、サーバの停止タイマが終了するまでサーバはブロック状態のままとなるため、故障から回復した到達可能なサーバを一時的にブロック状態にします。

例

RADIUS スキーム radius1 でサーバの停止タイマを 10 分に設定します。

<Switch> system-view

[Switch] radius scheme radius1

[Switch-radius-radius1] timer quiet 10

関連コマンド

display radius scheme

1.3.26 timer realtime-accounting (RADIUS scheme view)

Syntax

timer realtime-accounting *interval*

undo timer realtime-accounting

デフォルト

12 分

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

interval: リアルタイムのアカウンティング間隔を指定します。設定範囲は 0～71582 分です。

説明

timer realtime-accounting コマンドはリアルタイムのアカウンティング間隔を設定します。

undo timer realtime-accounting コマンドはデフォルトに戻します。

装置のリアルタイムのアカウンティング間隔が 0 でないとき、装置は設定された間隔で RADIUS アカウンティングサーバにオンラインユーザのアカウンティング情報を送信します。

装置のリアルタイムのアカウンティング間隔が 0 であるとき、装置はサーバに設定されたリアルタイムのアカウンティング間隔で RADIUS アカウンティングサーバにオンラインユーザのアカウンティング情報を送信します。サーバでリアルタイムのアカウンティング間隔が設定されていない場合、装置はオンラインユーザのアカウンティング情報を送信しません。

リアルタイムのアカウンティング間隔が短いと、アカウンティング情報の精度が上がりますが、多くのシステムリソースが必要となります。

表 1-7 リアルタイムのアカウンティング間隔の推奨値

ユーザ数	リアルタイムのアカウンティング間隔
1～99	3分
100～499	6分
500～999	12分
1000以上	15分以上

例

RADIUS スキーム radius1 のリアルタイムのアカウンティング間隔を 51 分に設定します。

<Switch> system-view

[Switch] radius scheme radius1

[Switch-radius-radius1] timer realtime-accounting 51

関連コマンド

retry realtime-accounting

1.3.27 timer response-timeout (RADIUS scheme view)

Syntax

timer response-timeout *seconds*

undo timer response-timeout

デフォルト

3 秒

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

seconds: RADIUS サーバの応答タイムアウト時間を指定します。設定範囲は 1～10 秒です。

説明

timer response-timeout コマンドは RADIUS サーバの応答タイムアウトタイマを設定します。

undo timer response-timeout コマンドはデフォルトに戻します。

RADIUS 要求を送信した後、一定時間内に RADIUS サーバから応答がない場合、NAS はユーザが多くの RADIUS サービスを受ける機会を持てるように、RADIUS リクエストを再送します。NAS は、RADIUS サーバの応答タイムアウトタイマを使用して、この送信間隔を制御します。

クライアントが認証プロセスの間にタイムアウトした場合、ユーザはすぐにログオフします。ユーザのログオフを防ぐため、以下によって乗算した値は、アクセスモジュールによって定義したクライアントのタイムアウト時間よりも大きくすることができません。

- RADIUS パケットの最大試行回数
- RADIUS サーバ応答タイムアウト時間
- RADIUS スキームの RADIUS 認証サーバ数

装置が新しい RADIUS サーバに RADIUS 要求を送信するとき、RADIUS パケットを転送する総時間を確認してください。総時間が 300 秒を超過した場合、次の RADIUS サーバへの RADIUS 要求の送信を停止します。

パケットの再送試行回数と RADIUS サーバの応答タイムアウト時間を設定する際に、RADIUS サーバの数を考慮してください。

例

RADIUS スキーム radius1 の RADIUS サーバの応答タイムアウトタイマを 5 秒に設定します。

<Switch> system-view

[Switch] radius scheme radius1

[Switch-radius-radius1] timer response-timeout 5

関連コマンド

- **display radius scheme**
- **retry**

1.3.28 user-name-format (RADIUS scheme view)

Syntax

user-name-format { **keep-original** | **with-domain** | **without-domain** }

undo user-name-format

デフォルト

with-domain

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

keep-original: RADIUS サーバに入力するユーザ名を送信します。

with-domain: RADIUS サーバに送信されるユーザ名に、ISP ドメイン名を含めます。

without-domain: RADIUS サーバに送信されるユーザ名から ISP ドメイン名を除外します。

説明

user-name-format コマンドは RADIUS サーバに送信されるユーザ名の形式を設定します。

undo user-name-format コマンドはデフォルトに戻します。

通常、ユーザ名の形式は *userid@isp-name* です。*isp-name* はユーザが所属する ISP ドメインを判断するために装置によって使用されます。しかし、旧型の RADIUS サーバの中には、ISP ドメイン名を含むユーザ名を認識できないものがあります。このような RADIUS サーバにドメイン名を含むユーザ名を送信する前に、装置はドメイン名を削除する必要があります。**user-name-format** コマンドを使用することで、RADIUS サーバに送信されるユーザ名にドメイン名を含めるかどうかを指定することができます。

RADIUS スキームが ISP ドメイン名を含まずにユーザ名を送信するよう定義している場合、この RADIUS スキームを複数の ISP ドメインに適用しないでください。これは、異なる 2 つの ISP ドメインに属する 2 つのユーザが、ユーザ ID が同じため、RADIUS サーバには 1 ユーザとみなされる、という混乱を避けるためです。

802.1X ユーザが EAP 認証を使用する場合、RADIUS スキームで設定された **user-name-format** コマンドは適用されません。RADIUS サーバに転送する際、装置はクライアントからユーザ名を変更できません。

例

RADIUS スキーム radius1 で、RADIUS サーバに送信されるユーザ名に、装置がドメイン名を削除するように指定します。

<Switch> system-view

[Switch] radius scheme radius1

[Switch-radius-radius1] user-name-format without-domain

関連コマンド

display radius scheme

目次

このセクションのページは **9-x-x** です。

2 章 802.1X 2-1
2.1 802.1X 設定コマンド 2-1
2.1.1 display dot1x 2-1
2.1.2 display dot1x connection 2-7
2.1.3 display dot1x unicast-trigger quiet-mac 2-10
2.1.4 dot1x 2-11
2.1.5 dot1x access-user log enable 2-12
2.1.6 dot1x authentication-method 2-13
2.1.7 dot1x auth-fail vlan 2-14
2.1.8 dot1x guest-vlan 2-15
2.1.9 dot1x guest-vlan-delay 2-16
2.1.10 dot1x handshake 2-18
2.1.11 dot1x handshake reply enable 2-19
2.1.12 dot1x mandatory-domain 2-19
2.1.13 dot1x max-user 2-20
2.1.14 dot1x multicast-trigger 2-21
2.1.15 dot1x port-control 2-22
2.1.16 dot1x port-method 2-23
2.1.17 dot1x quiet-period 2-24
2.1.18 dot1x re-authenticate 2-25
2.1.19 dot1x retry 2-26
2.1.20 dot1x timer 2-27
2.1.21 dot1x unauthenticated-user aging enable 2-29
2.1.22 dot1x timer reauth-period 2-31
2.1.23 dot1x unicast-trigger 2-32
2.1.24 reset dot1x access-user 2-33
2.1.25 reset dot1x guest-vlan 2-34
2.1.26 reset dot1x statistics 2-35
2.1.27 reset dot 1 x unicast-trigger quiet-mac 2-35

2章 802.1X

2.1 802.1X設定コマンド

2.1.1 display dot1x

Syntax

display dot1x [**sessions** | **statistics**] [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

sessions: 802.1X のセッション接続情報を表示します。

statistics: 802.1X の統計情報を表示します。

interface *interface-type interface-number*: ポートのタイプと番号を指定します。

説明

display dot1x コマンドは 802.1X についての情報を表示します。

sessions パラメータあるいは **statistics** パラメータのいずれのパラメータを指定しない場合、セッション情報、統計情報、設定情報を含む 802.1X のすべての情報を表示します。

interface *interface-type interface-number* パラメータを指定しない場合、グローバルとすべてのポートの 802.1X の情報を表示します。

例

802.1X のすべての情報を表示します。

<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
  SmartOn switch ID     : 30
  SmartOn supp timeout   : 30 s
  SmartOn retry counts   : 3
  EAD assistant function : Disabled
     URL              : http://jpn.nec.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
  SmartOn                  : Disabled
  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
```

表 2-1 コマンド出力

フィールド	説明
Global 802.1X parameters	グローバル802.1Xの設定です。
802.1X authentication	802.1Xがグローバルで有効かどうかを示します。
CHAP authentication	RADIUSサーバと通信する際にEAPを終端しCHAPを実行しています。
EAP authentication	RADIUSサーバと通信する際にEAPパケットの中継とEAP認証のいずれかを実行しています。
PAP authentication	RADIUSサーバと通信する際にEAPを終端しPAPを実行しています。
Max-tx period	ユーザ名の要求タイムアウトタイマです。単位は秒です。
Handshake period	ハンドシェイクタイマです。単位は秒です。
Quiet timer	停止タイマの状態をenabledあるいはdisabledで示します。
Quiet period	停止タイマです。単位は秒です。
Supp timeout	クライアントタイムアウトタイマです。単位は秒です。
Server timeout	サーバタイムアウトタイマです。単位は秒です。
Reauth period	定期再認証タイマです。単位は秒です。
Max auth requests	認証要求をクライアントに送信する最大試行回数です。
SmartOn switch ID	SmartOn認証のSwitch IDです。 このフィールドは現在のソフトウェアバージョンでサポートしていません。

フィールド	説明
SmartOn supp timeout	SmartOnクライアントタイムアウトタイマです。単位は秒です。 このフィールドは現在のソフトウェアバージョンでサポートしていません。
SmartOn retry counts	EAP-Request/Notificationパケットをクライアントに再送する最大試行回数です。 このフィールドは現在のソフトウェアバージョンでサポートしていません。
EAD assistant function	EAP assistantが有効であるかを示します。
URL	認証されていないユーザがWebブラウザでネットワークに接続するためのリダイレクト用URLです。
Free IP	認証されていないユーザがアクセス可能なネットワークセグメントです。
EAD timeout	EADルールタイマです。単位は分です。
Domain delimiter	装置がサポートするドメインデリミタです。
Online 802.1X wired users	接続されたオンライン802.1Xユーザの数です。802.1X認証をパスしたユーザ、802.1X認証を実行しているユーザが含まれます。
Online 802.1X users	オンライン802.1Xユーザ数です。
GigabitEthernet1/0/1 is link-up	ポートの状態です。たとえば、GigabitEthernet 1/0/1がupです。
802.1X authentication	802.1Xがポートで有効かを示します。
Handshake	オンラインユーザハンドシェイク機能がポートで有効かを示します。
Handshake reply	オンラインユーザハンドシェイク応答機能がポートで有効かを示します。
Handshake security	オンラインユーザハンドシェイクセキュリティ機能がポートで有効かを示します。
Unicast trigger	802.1Xユニキャストトリガがポートで有効かを示します。
Periodic reauth	定期オンラインユーザの再認証機能がポートで有効かを示します。
Port role	ポートの役割です。ポートは認証のみ機能します。
Authorization mode	ポートの許可状態です。 • **Force-Authorized** • **Auto** • **Force-Unauthorized**

フィールド	説明
Port access control	ポートのアクセス制御方式です。 ● **MAC-based**—MACベースアクセス制御です。 ● **Port-based**—ポートベースアクセス制御です。
Multicast trigger	802.1Xマルチキャストトリガ機能が有効かどうかを示します。
Mandatory auth domain	ポートの802.1X強制認証ドメインを示します。
Guest VLAN	ポートの802.1XゲストVLANを示します。 802.1XゲストVLANが設定されていない場合、**Not configured**と表示されます。
Auth-Fail VLAN	ポートの802.1X制限VLANを示します。 802.1X制限VLANが設定されていない場合、**Not configured**と表示されます。
Critical VLAN	ポートの802.1X critical VLANを示します。 このフィールドはサポートしていません。
Critical voice VLAN	ポートで802.1X critical voice VLANを示します。 このフィールドはサポートしていません。
Add Guest VLAN delay	802.1XゲストVLANに割り当てられている遅延機能の状態とモードです。 ● **EAPOL**—EAPOLトリガの802.1XゲストVLAN遅延が有効です。 ● **NewMac**—New MACトリガの802.1XゲストVLAN遅延が有効です。 ● **ALL**—EAPOLトリガとnew MACトリガの両方の802.1XゲストVLAN遅延が有効です。 ● **Disabled**—802.1XゲストVLAN遅延が無効です。
Re-auth server-unreachable	オンライン802.1Xがログオフしているか、802.1Xの再認証を行う際、サーバに到達不能状態であるかを示します。
Max online users	ポートの802.1Xユーザの同時接続最大数です。
SmartOn	ポートでSmartOn認証が有効かどうかを示します。 このフィールドは現在のソフトウェアバージョンでサポートしていません。
User IP freezing	ユーザのIPアドレスがポートで据え置いているかどうかを示します。 このフィールドはサポートしていません。
Reauth period	ポートの定期再認証タイマです。単位は秒です。
Send Packets Without Tag	VLANタグなしで802.1Xプロトコルパケットを送信するかどうかを示します。

フィールド	説明
Max Attempts Fail Number	MACアドレス認証ユーザの802.1X認証最大試行回数です。
Guest VSI	ポートで設定された802.1XゲストVSIです。 ポートで802.1XゲストVSIが設定されていない場合、**Not configured**と表示されます。 このフィールドは現在のソフトウェアバージョンでサポートしていません。
Auth-Fail VSI	ポートで設定された802.1X制限VSIです。 ポートで802.1X制限VSIが設定されていない場合、**Not configured**と表示されます。 このフィールドは現在のソフトウェアバージョンでサポートしていません。
Critical VSI	ポートで設定された802.1X critical VSIです。 ポートで802.1X critical VSIが設定されていない場合、**Not configured**と表示されます。 このフィールドは現在のソフトウェアバージョンでサポートしていません。
Add Guest VSI delay	ポートの802.1XゲストVSI割り当て遅延機能の状態とモードです。 • **EAPOL only** —EAPOLトリガの802.1XゲストVSI割り当て遅延機能が有効です。 • **NewMAC only** —New MACトリガの802.1XゲストVSI割り当て遅延機能が有効です。 • **EAPOL or NewMAC** —EAPOLトリガとnew MACトリガの両方の802.1XゲストVSI割り当て遅延機能が有効です。 • **Disabled**—802.1XゲストVSI割り当て遅延機能が無効です。 このフィールドは現在のソフトウェアバージョンでサポートしていません。
EAPOL packets	EAPOLパケットの送信数（Tx）および受信数（Rx）です。
Sent EAP Request/Identity packets	EAP-Request/Identityパケットの送信数です。
EAP Request/Challenge packets	EAP-Request/MD5 Challengeパケットの送信数です。
EAP Success packets	EAP-Successパケットの送信数です。
EAP Failure packets	EAP-Failureパケットの送信数です。
Received EAPOL Start packets	EAPOL-Startパケットの受信数です。
EAPOL LogOff packets	EAPOL-LogOffパケットの受信数です。

フィールド	説明
EAP Response/Identity packets	EAP-Response/Identityパケットの受信数です。
EAP Response/Challenge packets	EAP-Response/MD5 Challengeパケットの受信数です。
Error packets	エラーパケットの受信数です。
Online 802.1X users	ポートのオンライン802.1Xユーザ数です。 802.1X認証にパスしたユーザ、802.1X認証を実行しているユーザが含まれます。
MAC address	オンライン802.1XユーザのMACアドレスです。
Auth state	オンライン802.1Xユーザの認証状態です。

2.1.2 display dot1x connection

Syntax

display dot1x connection [**interface** *interface-type interface-number* | **slot** *slot-number* | **user-mac** *mac-address* | **user-name** *name-string*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: ポートのタイプと番号を指定します。ポートが指定されない場合、すべてのポートのオンライン 802.1X ユーザの情報を表示します。

slot *slot-number*: メンバ ID によって IRF スタックのメンバ装置を指定します。もしこのオプションが指定されない場合、すべての IRF スタックのメンバ装置のオンライン 802.1X ユーザの情報を表示します。

user-mac *mac-address*: 802.1X ユーザの MAC アドレスを指定します。形式は H-H-H です。指定しない場合、すべての 802.1X ユーザの情報を表示します。

user-name *name-string*: 802.1X ユーザの名前を指定します。設定範囲は 1～253 文字です。大文字、小文字を区別します。指定しない場合、すべてのオンライン 802.1X ユーザの情報を表示します。

説明

display dot1x connection コマンドはオンライン 802.1X ユーザの情報を表示します。

例

すべてのオンライン 802.1X ユーザの情報を表示します。

<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
Termination action: Default
Session timeout period: 2 s
Online from: 2013/03/02  13:14:15
Online duration: 0h 2m 15s
```

表 2-2 コマンド出力

フィールド	説明
Total connections	オンライン802.1Xユーザの数です。
User MAC address	ユーザのMACアドレスです。
Access interface	ユーザが装置にアクセスするインタフェースです。

フィールド	説明
User access state	ユーザのアクセス状態です。 ● **Successful**—ユーザが802.1X認証にパスし、オンラインになりました。 ● **Open**—オンラインでオープンな認証モードを実行するため、ユーザは存在しないユーザ名あるいは間違ったパスワードを使用しています。
Authentication domain	802.1X認証で使用されるISPドメインです。
IPv4 address	ユーザのIPv4アドレスです。 装置がユーザのIPv4アドレスを取得できない場合、このフィールドは無効です。
IPv6 address	ユーザのIPv6アドレスです。 装置がユーザのIPv6アドレスを取得できない場合、このフィールドは無効です。
Authentication method	EAPメッセージ操作方式です。 ● **CHAP**—RADIUSサーバと通信するEAPを終端しCHAPを実行しています。 ● **EAP**— RADIUSサーバと通信する際にEAPパケットの中継とEAP認証のいずれかを実行しています。 ● **PAP**—RADIUSサーバと通信する際にEAPを終端しPAPを実行しています。
Initial VLAN	802.1X認証を行う前にユーザが所属するVLANです。
Authorization untagged VLAN	ユーザに許可されたタグなしVLANです。
Authorization tagged VLAN list	ユーザに許可されたタグづけVLANです。
Authorization VSI	ユーザに許可されたVSIです。 このフィールドは現在のソフトウェアバージョンでサポートしていません。
Authorization ACL ID	ユーザに許可されたACLです。
Authorization user profile	ユーザに許可されたユーザプロファイルです。

フィールド	説明
Termination action	セッションタイムアウトタイマが終了したときにサーバに割り当てられたアクションです。 ● **Default**—認証されたオンライン802.1Xユーザをログオフします。定期オンラインユーザの再認証が有効で、セッションタイムアウトタイマより定期再認証タイマが短い場合は、適用されません。 ● **Radius-request**—セッションタイムアウトタイマが終了したとき、定期オンラインユーザの再認証の設定に関わらず、オンラインユーザを再認証します。 装置がローカル認証を実行するとき、このフィールドは**Default**と表示されます。
Session timeout period	サーバによって割り当てられたセッションタイムアウトタイマです。
Online from	802.1Xユーザがオンラインになったとき時間です。
Online duration	802.1Xユーザがオンラインになってからの経過時間です。

2.1.3 display dot1x unicast-trigger quiet-mac

🕮 **メモ**:

display dot1x unicast-trigger quiet-mac コマンドは Version7.1.7 を含む以降のソフトウェアからサポートしています。

Syntax

display dot1x unicast-trigger quiet-mac [interface *interface-type interface-number***]**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*:インタフェースをタイプと番号で指定します。インタフェースを指定しない場合、このコマンドはデバイス上のすべての 802.1 X ユニキャストトリガークワイエットアドレスを表示します。

説明

display dot1x unicast-trigger quiet-mac コマンドで、802.1 X ユニキャストトリガークワイエット MAC アドレスを表示します。

例

#802.1 X ユニキャストトリガークワイエット MAC アドレスをすべて表示します。

<Sysname>display dot1x unicast-trigger quiet-mac

```
<Sysname> display dot1x unicast-trigger quiet-mac
Total unicast-trigger quiet MAC addresses: 1
 MAC address          VLAN ID        Interface
 0800-2700-a4f7       1              GE1/0/1
```

Table 1 コマンド出力

フィールド	説明
Total unicast-trigger quiet MAC addresses	ユニキャストトリガーのクワイエットMACアドレスの総数。
MAC address	ユニキャストトリガークワイエットMACアドレス。
VLAN ID	MACアドレスが属するVLANのID。
Interface	MACアドレスが接続されているインタフェース。

関連コマンド

dot 1 x timer

reset dot 1 x unicast-trigger quiet-mac

2.1.4 dot1x

Syntax

dot1x

undo dot1x

デフォルト

802.1X はグローバルおよびポートで無効です。

View

System view

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

説明

dot1x コマンドは 802.1X をグローバルあるいはポートで有効にします。

undo dot1x コマンドは 802.1X をグローバルあるいはポートで無効にします。

802.1X はグローバルとポートの両方で有効にする必要があります。そうでない場合、動作しません。

例

802.1X をグローバルで有効にします。

<Switch> system-view

[Switch] dot1x

GigabitEthernet 1/0/1 で 802.1X を有効にします。

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] dot1x

[Switch-GigabitEthernet1/0/1] quit

関連コマンド

display dot1x

2.1.5 dot1x access-user log enable

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**] *

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

パラメータ

abnormal-logoff: 正しくログオフしなかったときのログ送信を有効にします。

failed-login: ログインに失敗したときのログ送信を有効にします。

normal-logoff: 正しくログオフしたときのログ送信を有効にします。

successful-login: ログインに成功したときのログ送信を有効にします。

説明

dot1x access-user log enable コマンドは 802.1X ユーザのログ出力機能を有効にします。

undo dot1x access-user log enable コマンドは 802.1X ユーザのログ出力機能を無効にします。

パラメータを指定しない場合、802.1X のすべてのログ出力機能を有効にします。

例

802.1X のすべてのログ出力機能を有効にします。

<Switch> system-view

[Switch] dot1x access-user log enable

2.1.6 dot1x authentication-method

Syntax

dot1x authentication-method { **chap** | **eap** | **pap** }

undo dot1x authentication-method

デフォルト

chap

View

System view

定義済みユーザロール

network-admin

パラメータ

chap: RADIUS サーバと通信するために EAP（Extensible Authentication Protocol）を終端し、CHAP（Challenge Handshake Authentication Protocol）認証を使用します。

eap: RADIUS サーバと通信するために、EAP パケットを中継し、EAP 認証をサポートします。

pap: RADIUS サーバと通信するために、EAP を終端し、PAP（Password Authentication Protocol）認証をサポートします。

説明

dot1x authentication-method コマンドは EAP メッセージ操作方法を指定することで 802.1X ユーザの認証方法を設定します。

undo dot1x authentication-method コマンドはデフォルトに戻します。

装置は EAP パケットを終端する、あるいは中継します。

- **EAP 終端モード**—アクセス装置は標準の RADIUS パケットの認証データを再カプセル化し、クライアントから RADIUS サーバに送信します。装置は RADIUS サーバの CHAP あるいは PAP 認証のどちらかを実行します。このモードでは RADIUS サーバは MD5-チャレンジ EAP 認証のみをサポートします。
  - PAP はプレーンテキストでユーザ名とパスワードを転送します。この認証方法は高いセキュリティを必要としないシナリオに適用します。
  - CHAP はネットワークを越えてプレーンテキストのユーザ名と暗号化されたパスワードを転送します。CHAP は PAP よりもセキュリティが高いです。
- EAP 中継モードーアクセス装置はクライアントと RADIUS サーバ間の EAP メッセージを中継します。EAP 中継モードは MD5-チャレンジ、EAP-TLS、PEAP のような複数の EAP 認証方式をサポートします。このモードを使用するため、RADIUS サーバは以下の要件に適用する必要があります。
  - EAP メッセージとメッセージ-認証属性をサポートします。
  - クライアントとして同じ EAP 認証方式を使用します。

  このモードが使用されると、RADIUS scheme view で **user-name-format** コマンドは適用されません。**user-name-format** コマンドについての詳細は、コマンドマニュアルのセクション 9 *セキュリティ* “*AAA*”を参照してください。

RADIUS 認証が使用されると、RADIUS サーバとして同じ認証方式（PAP、CHAP、EAP）を使用するようにアクセス装置を設定する必要があります。

例

EAP パケットを終端するアクセス装置を有効にし、RADIUS サーバで PAP 認証を実行します。

<Switch> system-view

[Switch] dot1x authentication-method pap

関連コマンド

display dot1x

2.1.7 dot1x auth-fail vlan

Syntax

dot1x auth-fail vlan *authfail-vlan-id*

undo dot1x auth-fail vlan

デフォルト

設定なし

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

authfail-vlan-id: ポートで 802.1X 制限 VLAN の ID を指定します。設定範囲は 1～4094 です。VLAN が作成されている必要があります。

説明

dot1x auth-fail vlan コマンドはポートで 802.1X 制限 VLAN を設定します。

undo dot1x auth-fail vlan コマンドは デフォルトに戻します。

802.1X 制限 VLAN は、サーバと通信不能以外の理由により、802.1X 認証に失敗したユーザに適用されます。

802.1X 制限 VLAN として設定された VLAN を削除する場合、最初に **undo dot1x auth-fail vlan** コマンドを使用します。

例

GigabitEthernet 1/0/1 で 802.1X 制限 VLAN 100 を設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] dot1x auth-fail vlan 100

関連コマンド

display dot1x

2.1.8 dot1x guest-vlan

Syntax

dot1x guest-vlan *guest-vlan-id*

undo dot1x guest-vlan

デフォルト

設定なし

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

guest-vlan-id: 802.1X ゲスト VLAN の ID を指定します。設定範囲は 1～4094 です。VLAN が作成されている必要があります。

説明

dot1x guest-vlan コマンドはポートで 802.1X ゲスト VLAN を設定します。

undo dot1x guest-vlan コマンドは デフォルトに戻します。

802.1X ゲスト VLAN は 802.1X 認証を実行していないユーザに適用されます。ユーザは 802.1X ゲスト VLAN で、アンチウィルスソフトウェアをダウンロードするため、ソフトウェアサーバなどの制限されたネットワークリソースを使用します。

802.1X ゲスト VLAN として設定された VLAN を削除する場合、最初に **undo dot1x guest-vlan** コマンドを使用します。

例

GigabitEthernet 1/0/1 で 802.1X ゲスト VLAN100 を設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] dot1x guest-vlan 100

関連コマンド

display dot1x

2.1.9 dot1x guest-vlan-delay

Syntax

dot1x guest-vlan-delay { **eapol** | **new-mac** }

undo dot1x guest-vlan-delay [**eapol** | **new-mac**]

デフォルト

無効

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

eapol: EAPOL により 802.1X ゲスト VLAN の割り当てを遅延させます。EAPOL-Start パケットによって 802.1X 認証が開始する場合、このパラメータを適用します。

new-mac: 新しいMACアドレスにより802.1Xゲスト VLANの割り当てを遅延させます。不明な MAC アドレスからのパケットによって 802.1X 認証が開始される場合、このパラメータを適用します。

説明

dot1x guest-vlan-delay コマンドはポートで 802.1X ゲスト VLAN の割り当ての遅延機能を有効にさせます。

undo dot1x guest-vlan-delay コマンドはポートで 802.1X ゲスト VLAN の割り当ての遅延機能を無効にさせます。

802.1X 認証がポートで開始されたとき、802.1X ゲスト VLAN に 802.1X が有効なポートを割り当てることを遅らせます。

この機能を使用する場合、802.1X が有効なポートで MAC ベースアクセス制御機能を有効にする必要があります。

802.1X 認証がポートで開始された場合、装置は以下の処理を行います。

1) ユニキャスト EAP-Request/Identity パケットの認証を開始する MAC アドレスに送信します。
2) **dot1x timer tx-period** コマンドで設定されるユーザ名要求タイムアウトタイマの間隔以内に応答を受信しない場合、パケットを再送します。
3) **dot1x retry** コマンドで設定されるパケットの最大試行回数の上限に到達したのち、802.1X ゲスト VLAN にポートを割り当てます。

パラメータなしで **undo dot1x guest-vlan-delay** コマンドを使用した場合、ポートで EAPOL トリガと新しい MAC アドレストリガの両方の 802.1X ゲスト VLAN の割り当ての遅延機能を無効にします。

例

GigabitEthernet 1/0/1 で新しい MAC アドレストリガの 802.1X ゲスト VLAN の割り当ての遅延機能を有効にさせます。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] dot1x guest-vlan-delay new-mac

関連コマンド

- **display dot1x**
- **dot1x guest-vlan**

- **dot1x retry**
- **dot1x timer tx-period**

2.1.10 dot1x handshake

Syntax

dot1x handshake

undo dot1x handshake

デフォルト

無効

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

説明

dot1x handshake コマンドはオンラインユーザハンドシェイク機能を有効にします。

undo dot1x handshake コマンドは機能を無効にします。

オンラインユーザハンドシェイク機能は、オンライン 802.1X ユーザの接続状態を確認するため、装置が定期的にハンドシェイクメッセージをクライアントに送信することを有効にします。もし装置がハンドシェイクタイマの時間に、ハンドシェイクの最大試行回数を実行してもオンラインユーザからの応答を受信しない場合、ユーザをオフライン状態に設定します。ハンドシェイクタイマを設定する場合、**dot1x timer handshake-period** コマンドを使用します。ハンドシェイクの最大試行回数を設定する場合、**dot1x retry** コマンドを使用します。

例

GigabitEthernet 1/0/1 でオンラインユーザハンドシェイク機能を有効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] dot1x handshake

関連コマンド

- **display dot1x**
- **dot1x timer handshake-period**
- **dot1x retry**

2.1.11 dot1x handshake reply enable

Syntax

dot1x handshake reply enable

undo dot1x handshake reply enable

デフォルト

無効

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

説明

dot1x handshake reply enable コマンドはハンドシェイクリプライ機能を有効にします。

undo dot1x handshake reply enable コマンドはハンドシェイクリプライ機能を無効にします。

dot1x handshake reply enable コマンドは、オンラインハンドシェイク処理中に、802.1X クライアントの EAP-Response/Identity パケットに応答するため、EAP-Success パケットを使用することを有効にします。

802.1X クライアントが装置から EAP-Success パケットを受信しないでオフラインになった場合のみ使用します。

例

GigabitEthernet 1/0/1 でハンドシェイクリプライ機能を設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] dot1x handshake reply enable

関連コマンド

dot1x handshake

2.1.12 dot1x mandatory-domain

Syntax

dot1x mandatory-domain *domain-name*

undo dot1x mandatory-domain

デフォルト

設定なし

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

domain-name: ドメイン名を指定します。設定範囲は 1～255 です。大文字、小文字を区別しません。

説明

dot1x mandatory-domain コマンドはポートで強制 802.1X 認証ドメインを指定します。

undo dot1x mandatory-domain コマンドは強制 802.1X 認証ドメインを削除します。

システムがポートにアクセスを行う 802.1X ユーザの認証を行うとき、以下の順番で認証ドメインを選択します。

1) 強制ドメイン
2) ユーザ名で指定された ISP ドメイン
3) デフォルト ISP ドメイン

例

GigabitEthernet 1/0/1 で 802.1X ユーザに強制 802.1X 認証ドメインを設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] dot1x mandatory-domain my-domain

関連コマンド

display dot1x

2.1.13 dot1x max-user

Syntax

dot1x max-user *max-number*

undo dot1x max-user

デフォルト

4294967295

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

max-number: ポートで 802.1X ユーザが同時に接続する最大数を指定します。設定範囲は 1～4294967295 です。

🕮 **メモ**:

QX-S5100G シリーズは 2048 まで認証動作が可能です。

説明

dot1x max-user コマンドはポートで 802.1X ユーザが同時に接続する最大数を指定します。

undo dot1x max-user コマンドは デフォルトに戻します。

システムリソースが乱用されることを防止するため、ポートで 802.1X ユーザが同時に接続する最大数を設定します。最大数に到達したとき、ポートで後続の 802.1X ユーザは拒否されます。

例

GigabitEthernet 1/0/1 で 802.1X ユーザが同時に接続する最大数を 32 に指定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] dot1x max-user 32

関連コマンド

display dot1x

2.1.14 dot1x multicast-trigger

Syntax

dot1x multicast-trigger

undo dot1x multicast-trigger

デフォルト

無効

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

説明

dot1x multicast-trigger コマンドは 802.1X マルチキャストトリガ機能を有効にします。

undo dot1x multicast-trigger コマンドは機能を無効にします。

802.1X マルチキャストトリガ機能は装置がイニシエータとして動作することを有効にします。装置は 802.1X クライアントを検出し、認証を開始するため、定期的に EAP-Request/Identity パケットをマルチキャストします。マルチキャスト EAP-Request/Identity パケットを送信する間隔を設定するため、**dot1x timer tx-period** コマンドを使用します。

例

GigabitEthernet 1/0/1 で 802.1X マルチキャストトリガ機能を有効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] dot1x multicast-trigger

関連コマンド

- **display dot1x**
- **dot1x timer tx-period**
- **dot1x unicast-trigger**

2.1.15 dot1x port-control

Syntax

dot1x port-control { **authorized-force** | **auto** | **unauthorized-force** }

undo dot1x port-control

デフォルト

auto

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

authorized-force: ポートを許可された状態に設定します。認証を行わずネットワークにアクセスできるようにポートのユーザを有効にします。

auto: 指定されたポートあるいはすべてのポートを最初は EAPOL フレームだけは通す許可されていない状態に設定し、認証に成功した後は、ネットワークへのアクセスを許可する許可状態に変更します。これが最も一般的な使用方法です。

unauthorized-force: ポートを許可されていない状態に設定します。ポートのユーザからのアクセス要求を拒否します。

説明

dot1x port-control コマンドはポートの許可状態を設定します。

undo dot1x port-control コマンドは デフォルトに戻します。

このコマンドを使用することで、クライアントのネットワークへのアクセスを許可されるかどうかを決定するため、ポートに許可状態を設定することができます。

例

GigabitEthernet 1/0/1 の許可状態を unauthorized-force に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] dot1x port-control unauthorized-force

関連コマンド

display dot1x

2.1.16 dot1x port-method

Syntax

dot1x port-method { **macbased** | **portbased** }

undo dot1x port-method

デフォルト

macbased

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

macbased: MAC ベースアクセス制御方式を使用します。この方式はポートのそれぞれのユーザを個別に認証します。認証されたユーザがログオフしたとき、この方式を使用しても、他のオンラインユーザには影響しません。

portbased: ポートでポートベースアクセス制御方式を使用します。この方式はポートで最初のユーザが認証に成功すると他のすべてのユーザが認証なしでネットワークへアクセスすることができます。最初のユーザがログオフになったとき、同時に他のすべてのユーザもログオフになります。

説明

dot1x port-method コマンドはポートのアクセス制御方式を指定します。

undo dot1x port-method コマンドは デフォルトに戻します。

例

GigabitEthernet 1/0/1 をポートベースアクセス制御方式に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] dot1x port-method portbased

関連コマンド

display dot1x

2.1.17 dot1x quiet-period

Syntax

dot1x quiet-period

undo dot1x quiet-period

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

dot1x quiet-period コマンドは停止タイマを有効にします。

undo dot1x quiet-period コマンドは停止タイマを無効にします。

クライアントが 802.1X 認証に失敗したとき、装置は、クライアントから認証要求を処理する前に、一定期間を待つ必要があります。停止タイマの時間を設定する場合、**dot1x timer quiet-period** コマンドを使用します。

例

停止タイマを有効にし、停止時間を 100 秒に設定します。

<Switch> system-view

[Switch] dot1x quiet-period

[Switch] dot1x timer quiet-period 100

関連コマンド

- **display dot1x**
- **dot1x timer**

2.1.18 dot1x re-authenticate

Syntax

dot1x re-authenticate

undo dot1x re-authenticate

デフォルト

無効

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

説明

dot1x re-authenticate コマンドは定期的なオンラインユーザの再認証機能を有効にします。

undo dot1x re-authenticate コマンドは機能を無効にします。

定期再認証機能を有効にすると、アクセス装置は、ポートのオンライン 802.1X ユーザを定期的に認証します。この機能はオンラインユーザの接続状態を確認し、ACL や VLAN などの、サーバに割り当てられた許可属性をアップデートします。

再認証を行う期間を設定する場合、**dot1x timer reauth-period** コマンドを使用します。

例

GigabitEthernet 1/0/1 で 802.1X オンラインユーザの再認証機能を有効にし、再認証を行う期間を 1800 秒に設定します。

<Switch> system-view

[Switch] dot1x timer reauth-period 1800

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] dot1x re-authenticate

関連コマンド

- **display dot1x**
- **dot1x timer**

2.1.19 dot1x retry

Syntax

dot1x retry *retries*

undo dot1x retry

デフォルト

2

View

System view

定義済みユーザロール

network-admin

パラメータ

retries: クライアントに認証要求を送信する最大試行回数を指定します。設定範囲は 1～10 です。

説明

dot1x retry コマンドはクライアントに認証要求を送信する最大試行回数を設定します。

undo dot1x retry コマンドは デフォルトに戻します。

以下のいずれかの状況により、アクセス装置はクライアントに認証要求を再送します。

- 装置はユーザ名の要求タイマ内にクライアントから応答を受信しません。EAP-Request/Identity パケットのタイマは **dot1x timer tx-period** *tx-period-value* コマンドで設定することができます。

- 装置はクライアントタイムアウトタイマ内にクライアントから応答を受信しません。EAP-Request/MD5-Challenge パケットのタイマは **dot1x timer supp-timeout** *supp-timeout-value* コマンドで設定することができます。

認証要求を送信する試行回数が最大に到達しても応答を受信しない場合、アクセス装置は要求の再送を停止します。

例

クライアントに認証要求を送信する最大試行回数を 9 に設定します。

<Switch> system-view

[Switch] dot1x retry 9

関連コマンド

- **display dot1x**
- **dot1x timer**

2.1.20 dot1x timer

Syntax

dot1x timer { **ead-timeout** *ead-timeout-value* | **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* | **unicast-trigger quiet-period** *quiet-period-value*}

undo dot1x timer { **handshake-period** | **quiet-period** | **reauth-period** | **server-timeout** | **supp-timeout** | **tx-period** | **unicast-trigger quiet-period** }

デフォルト

- ハンドシェイクタイマ：15 秒
- 停止タイマ：60 秒
- 定期再認証タイマ：3600 秒
- サーバタイムアウトタイマ：100 秒
- クライアントタイムアウトタイマ：30 秒
- ユーザ名要求タイムアウトタイマ：30 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

handshake-period *handshake-period-value*: ハンドシェイクタイマを設定します。設定範囲は 5～1024 秒です。

quiet-period *quiet-period-value*: 停止タイマを設定します。設定範囲は 10～120 秒です。

reauth-period *reauth-period-value*: 定期再認証タイマを設定します。設定範囲は 60～86400 秒です。

🕮 **メモ：**

reauth-period *reauth-period-value* オプションの最大設定値は Version7.1.8 を含む以降のソフトウェアで 86400 まで設定が可能です。
Version7.1.7 を含むそれ以前のソフトウェアは、7200 秒までとなります。

---

server-timeout *server-timeout-value*: サーバタイムアウトタイマを設定します。設定範囲は 100～300 秒です。

supp-timeout *supp-timeout-value*: クライアントタイムアウトタイマを設定します。設定範囲は 1～120 秒です。

tx-period *tx-period-value*: ユーザ名要求タイムアウトタイマを設定します。設定範囲は 1～120 秒です。

unicast-trigger quiet-period *quiet-period-value*: ユニキャストトリガーのタイムアウトタイマを設定します。設定範囲は 0～3600 秒です。

🕮 **メモ：**

unicast-trigger quiet-period *quiet-period-value* オプションは Version7.1.7 を含む以降のソフトウェアからサポートしています。

説明

dot1x timer コマンドは 802.1X タイマを設定します。

undo dot1x timer コマンドはデフォルトに戻します。

ほとんどの状況ではデフォルトの設定で十分です。ネットワークの状況に依存してタイマを設定することができます。

- 低速ネットワークでは、クライアントタイムアウトタイマを増加します。
- 脆弱なネットワークでは、停止タイマの値を大きい値に設定します。
- 認証の応答が早急な高性能ネットワークでは、停止タイマを小さい値に設定します。
- 異なる性能の認証サーバがあるネットワークではサーバタイムアウトタイマを適切に設定します。

ネットワーク装置は以下の 802.1X タイマを使用します。

- **ハンドシェイクタイマ（handshake-period）**－装置が認証ユーザのオンライン状況の確認のためハンドシェイク要求を定期的に送信する間隔を設定します。ハンドシェイク要求に応答がない場合には、認証ユーザがログオフしたと判断します。
- **停止タイマ（quiet-period）**—クライアントが認証に失敗したとき開始します。アクセス装置はクライアントから認証処理を開始する前に、タイマの時間を待つ必要があります。
- **定期再認証タイマ（reauth-period）**—ポート上の定期再認証を有効にすると、装置は、タイマで設定された間隔でポート上のオンラインユーザを再認証します。この設定は **dot1x re-authenticate** コマンドで設定します。まだオンラインにユーザが存在しているときに再認証間隔を変更すると、装置は、変更前の間隔での再認証を継続します。オンラインユーザの再認証を終了した後、装置は新しく設定された再認証間隔を使います。
- **サーバタイムアウトタイマ（server-timeout）**—アクセス装置が認証サーバに RADIUS Access-Request パケットを送信するときに開始します。このタイマが時間切れになるまでに応答がなかった場合、アクセス装置は、サーバに要求を再送します。
- **クライアントタイムアウトタイマ（supp-timeout）**—アクセス装置がクライアントに EAP-Request/MD5 Challenge パケットを送信するときに開始します。このタイマが時間切れになるまで応答がなかった場合、アクセス装置は、クライアントに要求を再送します。
- **ユーザ名要求タイムアウトタイマ（tx-period）**—装置が EAP-Request/Identity パケットをクライアントに認証要求の応答として送信するときに開始します。タイマが終了する前に装置が応答を受信しない場合、要求を再送します。認証をアクティブに要求できないクライアントを検出するため、EAP-Request/Identity パケットをネットワーク装置に、設定されたタイマの間隔でマルチキャストします。

定期再認証タイマは古い再認証タイマが終了した後、新しく設定された再認証の間隔が適用されます。他のタイマは設定を変更するとすぐに適用されます。

例

サーバタイムアウトタイマを 150 秒に設定します。

<Switch> system-view

[Switch] dot1x timer server-timeout 150

関連コマンド

display dot1x

2.1.21 dot1x unauthenticated-user aging enable

Syntax

dot1x unauthenticated-user aging enable

undo dot1x unauthenticated-user aging enable

デフォルト

有効

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

dot1x unauthenticated-user aging enable コマンドは、認証されていない 802.1X ユーザのエージング機能を有効にします。

undo dot1x unauthenticated-user aging enable コマンドは、認証されていない 802.1X ユーザのエージング機能を無効にします。

802.1X 非認証ユーザのエージングは、未認証か、認証に失敗したために 802.1 X ゲスト、または Auth-Fail VLAN に追加されたユーザに適用されます。

これらの VLAN のいずれかのユーザがエージングアウトすると、装置は VLAN からユーザを削除し、アクセスポートからユーザの MAC エントリアドレスを削除します。

ポートの 802.1X ユーザのエージングメカニズムはアクセス制御モードに依存します。

- ポートがポートベースアクセス制御を使用している場合、ポートが critical、認証に失敗した VLAN に割り当てられると、ユーザエージングタイマが開始されます。エージングタイマが満了すると、ポートは VLAN から削除され、VLAN 内のユーザのすべての MAC アドレスエントリも削除されます。
- ポートが MAC ベースのアクセス制御を使用する場合、認証失敗、critical、またはゲスト VLAN に割り当てられた 802.1X ユーザごとにユーザエージングタイマが開始されます。ユーザエージングタイマが満了すると、装置は VLAN のユーザを削除します。

1 つのポートでこれらの VLAN のいずれかのユーザが正常に認証されて別のポートでオンラインになるには、この機能を有効にします。それ以外の場合は、この機能を無効にすることをお勧めします。

削除されたユーザは、別の認証がトリガされるまでネットワークリソースにアクセスできません。

例

GigabitEthernet 1/0/1 のポートで、802.1X ユーザのエージングを無効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] undo dot1x unauthenticated-user aging enable

関連コマンド

dot1x timer

2.1.22 dot1x timer reauth-period

Syntax

dot1x timer reauth-period *reauth-period-value*

undo dot1x timer reauth-period

デフォルト

ポートでの定期的な 802.1X 再認証タイマは設定されていません。グローバルの定期的な 802.1X 再認証タイマを使用します。

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

reauth-period-value: 定期的な 802.1X 再認証タイマを設定します。設定範囲は 60～7200 秒です。

説明

dot1x timer reauth-period コマンドはポートで定期的な 802.1X 再認証タイマを設定します。

undo dot1x timer reauth-period コマンドは デフォルトに戻します。

ポートで定期的なオンライン 802.1X ユーザの再認証を有効にした場合、装置は指定された定期的な再認証の間隔でポート上のオンライン 802.1X ユーザを再認証します。ポートで定期的なオンライン 802.1X ユーザの再認証を有効にする場合、**dot1x re-authenticate** コマンドを使用します。

古い再認証タイマが終了した後、新しく設定された再認証タイマが適用されます。

装置は以下の優先度で定期的な 802.1X 再認証タイマを選択します。

1) サーバが割り当てた再認証タイマ
2) ポートで設定された再認証タイマ
3) グローバルで設定された再認証タイマ
4) デフォルトの再認証タイマ

例

GigabitEthernet1/0/1 で定期的な 802.1X 再認証タイマを 60 秒に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1 1/0/1

[Switch-GigabitEthernet1/0/1] dot1x timer reauth-period 60

関連コマンド

dot1x timer

2.1.23 dot1x unicast-trigger

Syntax

dot1x unicast-trigger

undo dot1x unicast-trigger

デフォルト

有効

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

説明

dot1x unicast-trigger コマンドは 802.1X ユニキャストトリガ機能を有効にします。

undo dot1x unicast-trigger コマンドは 802.1X ユニキャストトリガ機能を無効にします。

802.1X ユニキャストトリガ機能は、未知の送信元 MAC アドレスからデータフレームを受信したときに 802.1X 認証を開始する機能です。装置は、ユニキャスト EAP-Request/Identity パケットを未知の送信元の MAC アドレスに送信しますが、一定時間内（**dot1x timer tx-period** コマンドで指定されます）に反応がない場合、パケットを再送します。このプロセスはで設定された最大試行回数（**dot1x retry** コマンドで指定されます）、実施します。

例

GigabitEthernet 1/0/1 のユニキャストトリガ機能を有効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] dot1x unicast-trigger

関連コマンド

- **display dot1x**
- **dot1x multicast-trigger**
- **dot1x retry**
- **dot1x timer**

2.1.24 reset dot1x access-user

Syntax

reset dot1x access-user [**interface** *interface-type interface-number* | **mac** *mac-address* | **username** *username* | **vlan** *vlan-id*]

View

User view

定義済みユーザロール

network-admin

パラメータ

interface *interface-type interface-number*: インタフェースのタイプと番号でポートを指定します。

mac *mac-address*: MAC address で 802.1X ユーザを指定します。*mac-address* は H-H-H の形式です。

username *username*: 802.1X ユーザをユーザ名で指定します。*username* は 1～253 文字の大文字小文字を区別する文字列です。

vlan *vlan-id*: VLAN を VLAN ID で指定します。*vlan-id* の範囲は 1～4094 です。

説明

reset dot1x access-user コマンドは 802.1X ユーザをログオフします。

reset dot1x access-user コマンドは特定の 802.1X ユーザをログオフし、そのユーザ情報を装置から消去します。再度オンラインになるためには、ユーザは 802.1X 認証を実行してください。

VLAN を指定すると、指定した VLAN の次の 802.1X ユーザをログオフします。

- 802.1X 認証を通過し、指定された VLAN を認証 VLAN としてサーバに許可されたユーザ。
- 802.1X 認証を通過後、認証 VLAN を許可されていないため、指定の VLAN に留まるユーザ。
- 指定の VLAN で 802.1X 認証を実行中のユーザ。

ユーザが使用中の VLAN を識別するには、**display mac-address** コマンドを使います。

パラメータを指定しない場合は、**reset dot1x access-user** コマンドで装置上の 802.1X ユーザを全てログオフできます。

例

GigabitEthernet 1/0/1 の全 802.1X ユーザをログオフします。

<Switch> reset dot1x access-user interface gigabitethernet 1/0/1

関連コマンド

display dot1x connection

2.1.25 reset dot1x guest-vlan

Syntax

reset dot1x guest-vlan interface *interface-type interface-number* [**mac-address** *mac-address*]

View

User view

定義済みユーザロール

network-admin

パラメータ

interface *interface-type interface-number*: ポートのタイプと番号を指定します。

mac-address *mac-address*: ゲスト VLAN の 802.1X ユーザの MAC アドレスを指定します。指定しない場合、ポートのすべての 802.1X ユーザを削除します。

説明

reset dot1x guest-vlan コマンドはポートの 802.1X ゲスト VLAN からユーザを削除します。

例

GigabitEthernet 1/0/1 の 802.1X ゲスト VLAN から MAC アドレスが 1-1-1 のユーザを削除します。

<Switch> reset dot1x guest-vlan interface gigabitethernet 1/0/1 mac-address 1-1-1

関連コマンド

dot1x guest-vlan

2.1.26 reset dot1x statistics

Syntax

reset dot1x statistics [**interface** *interface-type interface-number*]

View

User view

定義済みユーザロール

network-admin

パラメータ

interface *interface-type interface-number*: ポートのタイプと番号を指定します。指定されない場合、すべてのポートの 802.1X の統計情報を削除します。

説明

reset dot1x statistics コマンドはポートの 802.1X の統計情報を削除します。

例

GigabitEthernet 1/0/1 の 802.1X の統計情報を削除します。

<Switch> reset dot1x statistics interface gigabitethernet 1/0/1

関連コマンド

display dot1x

2.1.27 reset dot 1 x unicast-trigger quiet-mac

🕮 **メモ**:

display dot1x unicast-trigger quiet-mac コマンドは Version7.1.7 を含む以降のソフトウェアからサポートしています。

Syntax

reset dot 1 x unicast-trigger quiet-mac [インタフェース interface-type interface-number] [mac-address mac-address]

View

User view

定義済みのユーザロール

network-admin

パラメータ

interface *interface-type interface-number*:インタフェースをタイプと番号で指定します。

mac-address *mac-address*:H-H-H 形式の 802.1 X ユニキャストトリガークワイエット MAC アドレスを指定します。

説明

reset dot 1 x unicast-trigger quiet-mac コマンドで、802.1 X ユニキャストトリガークワイエット MAC アドレスをクリアします。

パラメータを指定しない場合、このコマンドは全ての 802.1 X ユニキャストトリガークワイエット MAC アドレスをクリアします。

例

#GigabitEthernet 1/0/1 上の 802.1 X ユニキャストトリガークワイエット MAC アドレスをクリアします。

```
<Switch>reset dot 1 x unicast-trigger quiet-mac gigabitethernet 1/0/1
```

関連コマンド

display dot 1 x unicast-trigger quiet-mac

目次

このセクションのページは **9-x-x** です。

3 章 MAC アドレス認証 3-1
3.1 MAC アドレス認証設定コマンド 3-1
3.1.1 display mac-authentication 3-1
3.1.2 display mac-authentication connection 3-6
3.1.3 mac-authentication 3-8
3.1.4 mac-authentication access-user log enable 3-9
3.1.5 mac-authentication domain 3-10
3.1.6 mac-authentication guest-vlan 3-11
3.1.7 mac-authentication guest-vlan auth-period 3-12
3.1.8 mac-authentication max-user 3-13
3.1.9 mac-authentication offline-detect enable 3-14
3.1.10 mac-authentication parallel-with-dot1x 3-15
3.1.11 mac-authentication re-authenticate 3-16
3.1.12 mac-authentication timer (system view) 3-17
3.1.13 mac-authentication timer (interface view) 3-19
3.1.14 mac-authentication timer user-aging 3-20
3.1.15 mac-authentication unauthenticated-user aging enable 3-21
3.1.16 mac-authentication user-name-format 3-23
3.1.17 reset mac-authentication access-user 3-24
3.1.18 reset mac-authentication guest-vlan 3-26
3.1.19 reset mac-authentication statistics 3-26

3章 MAC アドレス認証

3.1 MACアドレス認証設定コマンド

3.1.1 display mac-authentication

Syntax

display mac-authentication [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: ポートのタイプと番号を指定します。指定しない場合、すべてのグローバルと指定したポートの MAC アドレス認証の情報を表示します。

説明

display mac-authentication コマンドは MAC アドレス認証の設定と統計情報を表示します。グローバルの設定、指定したポートに関する設定、MAC アドレス認証の統計情報、オンラインユーザの統計情報を表示します。

例

すべての MAC アドレス認証の設定と統計情報を表示します。

<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
  Max online users          : 256
  Authentication attempts   : successful 2, failed 3
  Current online users      : 1
        MAC address      Auth state
        0001-0000-0000    Authenticated
        0001-0000-0001    Unauthenticated
```

表 3-1 コマンド出力

フィールド	説明
MAC authentication	MACアドレス認証がグローバルで有効かどうかを示します。

フィールド	説明
Username format	ユーザアカウントタイプです。MACベースあるいは共有があります。 ● MACベースアカウントが使用される場合、ユーザ名のフォーマットで表示されます。たとえば、ハイフンなし、16進数表示、小文字でMACアドレスが**MAC address in lowercase(xxxxxxxxxxxx)**と表示されます。 ● 共有アカウントが使用される場合、**Fixed account**と表示されます。
Username:	MACアドレス認証のユーザ名です。 ● MACベースアカウントが使用される場合、**mac**と表示されます。装置はMACアドレス認証のユーザ名とパスワードとして各ユーザのMACアドレスを使用します。 ● 共有アカウントが使用される場合、MACアドレス認証ユーザの共有アカウントのユーザ名が表示されます。デフォルトのユーザ名は**mac**です。
Password:	MACアドレス認証のパスワードです。 ● MACベースアカウントが使用されている場合、あるいは共有アカウントでパスワードが設定されていない場合、**Not configured**と表示されます。 ● 共有アカウントでパスワードが設定されている場合、とアスタリスク（******）の文字列が表示されます。
Offline detect period	オフライン検出タイマです。
Quiet period	Quietタイマです。
Server timeout	サーバタイムアウトタイマです。
Reauth period	定期MACアドレス再認証タイマです。単位は秒です。
Authentication domain	system viewで指定されたMACアドレス認証のドメインです。system viewでMACアドレス認証のドメインが指定されていない場合、**Not configured, use default domain**と表示されます。
Online MAC-auth wired users	MACアドレス認証の接続されたオンラインユーザ数です。MACアドレス認証にパスしたユーザとMACアドレス認証を実行しているユーザが含まれます。
Silent MAC users	サイレントMACアドレスについての情報です。
MAC address	サイレントMACアドレスです。
VLAN ID	サイレントMACアドレスが所属するVLANのIDです。

フィールド	説明
From port	サイレントMACアドレスとしてMACアドレスを記載するポート名です。
Port index	サイレントMACアドレスとしてMACアドレスを記載するポートのインデックスです。
GigabitEthernet1/0/1 is link-up	GigabitEthernet 1/0/1のリンクの状態です。この例ではリンクがupしています。
MAC authentication	MACアドレス認証がポートで有効かどうかを示します。
Carry User-IP	MACアドレス認証要求にユーザのIPアドレスが含まれるかどうかを示します。 このフィールドは現在のソフトウェアバージョンでサポートしていません。
Authentication domain	ポートのために指定されたMACアドレス認証のドメインです。
Auth-delay timer	MACアドレス認証の開始を遅らせる機能が有効かどうかを示します。
Auth-delay period	MACアドレス認証の開始を遅らせる遅延時間のタイマです。
Periodic reauth	定期的なMACアドレス認証の再認証がポートで有効かどうかを示します。
Reauth period	ポートの定期MACアドレス再認証タイマです。
Re-auth server-unreachable	サーバが到達不能であるときのMACアドレス認証の再認証を行う際のアクションです。 ● **Logoff**—オンラインユーザをログオフします。 ● **Online**—MACアドレス認証ユーザのログインを保持します。
Guest VLAN	ポートでゲストVLANが設定されています。 MACアドレス認証ゲストVLANが設定されていない場合、**Not configured**と表示されます。
Guest VLAN auth-period	ポートのMACアドレス認証のゲストVLANの認証を行う間隔です。
Critical VLAN	ポートで設定されたMACアドレス認証のcritical VLANです。 critical VLANをサポートしていない場合、**Not configured**と表示されます。 このフィールドはサポートしていません。
Critical voice VLAN	ポートでMACアドレス認証のcritical voice VLANが有効かどうかを示します。 このフィールドはサポートしていません。

フィールド	説明
Host mode	● マルチVLANモードが無効の場合、**Single VLAN**と表示されます。 ● マルチVLANモードが無効の場合、**Multiple VLAN**と表示されます。
Offline detection	MACアドレス認証のオフライン検出機能の状態です。 ● **Enabled**－有効です。 ● **Disabled**－無効です。
Authentication order	MACアドレス認証と802.1X認証の並列処理が無効である場合、**Default**と表示します。 MACアドレス認証と802.1X認証の並列処理が有効である場合、**Parallel**と表示します。
Guest VSI	ポートで設定されたMACアドレス認証ゲストVSIです。 ポートで802.1Xゲスト VSIが設定されていない場合、**Not configured**と表示されます。 このフィールドは現在のソフトウェアバージョンでサポートしていません。
Guest VSI auth-period	ポートのMACアドレス認証のユーザのゲストVSIの認証を行う間隔です。 このフィールドは現在のソフトウェアバージョンでサポートしていません。
Critical VSI	ポートで設定されたMACアドレス認証のcritical VSIです。 ポートでMACアドレス認証のcritical VSIが設定されていない場合、**Not configured**と表示されます。 このフィールドは現在のソフトウェアバージョンでサポートしていません。
Max online users	ポートで許可されたオンラインユーザの同時接続最大数です。
Authentication attempts: successful 1, failed 0	MACアドレス認証の統計情報です。MACアドレス認証に成功した試行回数、認証に失敗した試行回数です。
MAC address	オンラインユーザのMACアドレスです。
Auth state	ユーザの状態です。 ● **Authenticated**—ユーザがMACアドレス認証に成功しています。 ● **Unauthenticated**—ユーザがMACアドレス認証に失敗しています。

3.1.2 display mac-authentication connection

Syntax

display mac-authentication connection [**interface** *interface-type interface-number* | **slot** *slot-number* | **user-mac** *mac-address* | **user-name** *user-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: ポートのタイプと番号を指定します。指定しない場合、すべてのポートのオンライン MAC アドレス認証ユーザの情報を表示します。

slot *slot-number*: IRF スタックメンバ装置を指定します。*slot-number* は IRF スタックメンバ装置の ID を示します。指定しない場合、IRF スタックユニットのすべてのメンバ装置のオンライン MAC アドレス認証ユーザの情報を表示します。

user-mac *mac-address*: オンライン MAC アドレス認証ユーザの MAC アドレスです。*mac-address* はユーザの MAC アドレスを示します。形式は H-H-H です。指定しない場合、すべてのオンライン MAC アドレス認証ユーザの情報を表示します。

user-name *user-name*: オンライン MAC アドレス認証ユーザのユーザ名です。設定範囲は 1～55 文字です。大文字、小文字を区別します。ドメイン名を含むことができます。指定しない場合、すべてのオンライン MAC アドレス認証ユーザの情報を表示します。

説明

display mac-authentication connection コマンドはオンライン MAC アドレス認証ユーザの情報を表示します。

例

すべてのオンライン MAC アドレス認証ユーザの情報を表示します。

<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: nec
```

```
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
Termination action: Radius-request
Session timeout period: 2 s
Online from: 2013/03/02  13:14:15
Online duration: 0h 2m 15s
```

表 3-2 コマンド出力

フィールド	説明
Total connections	オンラインMACアドレス認証ユーザの総数です。
User MAC address	ユーザのMACアドレスです。
Access interface	ユーザが装置にアクセスするインタフェースです。
User access state	ユーザのアクセス状態です。 • **Successful**—ユーザが802.1X認証にパスし、オンラインになりました。 • **Open**—オンラインでオープンな認証モードを実行するため、ユーザは存在しないユーザ名あるいは間違ったパスワードを使用しています。
Authentication domain	ユーザが所属するMACアドレス認証のドメインです。
Initial VLAN	MACアドレス認証を行う前にユーザを保持するVLANです。
Authorization untagged VLAN	ユーザに許可されたタグつきVLANです。
Authorization tagged VLAN	ユーザに許可されたタグなしVLANです。
Authorization VSI	ユーザに許可されたVSIです。 このフィールドは現在のソフトウェアバージョンでサポートしていません。
Authorization ACL ID	ユーザに許可されたACLです。
Authorization user profile	ユーザに許可されたユーザプロファイルです。

フィールド	説明
Termination action	セッションタイムアウトタイマが終了したとき、サーバに割り当てられたアクションの属性です。 • **Default**—セッションタイムアウトタイマが終了したときオンライン認証ユーザをログオフします。この状態は定期的なMACアドレス認証が有効で定期再認証タイマがセッションタイムアウトタイマより短い場合、適用されません。 • **Radius-request**—セッションタイムアウトタイマが終了したとき、定期再認証機能が有効かどうかにかかわらずオンラインユーザを再認証します。 ローカル認証が実行されている場合、**Default**と表示されます。
Session timeout period	サーバによって割り当てられたセッションタイムアウトタイマです。
Online from	MACアドレス認証ユーザがオンラインになった時間です。
Online duration	MACアドレス認証ユーザがオンラインになってからの経過時間です。

3.1.3 mac-authentication

Syntax

mac-authentication

undo mac-authentication

デフォルト

無効

View

System view

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

説明

mac-authentication コマンドはグローバルあるいはポートで MAC アドレス認証を有効にします。

undo mac-authentication コマンドはグローバルあるいはポートで MAC アドレス認証を無効にします。

ポートで MAC アドレス認証を使用する場合、グローバルとポートの両方で MAC アドレス認証を有効にする必要があります。

例

グローバルで MAC アドレス認証を有効にします。

<Switch> system-view

[Switch] mac-authentication

GigabitEthernet 1/0/1 で MAC アドレス認証を有効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] mac-authentication

関連コマンド

display mac-authentication

3.1.4 mac-authentication access-user log enable

Syntax

mac-authentication access-user log enable [**failed-login** | **logoff** | **successful-login**] *

undo mac-authentication access-user log enable [**failed-login** | **logoff** | **successful-login**] *

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

パラメータ

failed-login: ログインに失敗したときのログ送信を有効にします。

logoff: ログオフしたときのログ送信を有効にします。

successful-login: ログインに成功したときのログ送信を有効にします。

説明

mac-authentication access-user log enable コマンドは MAC アドレス認証ユーザのログ出力機能を有効にします。

undo mac-authentication access-user log enable コマンドは MAC アドレス認証ユーザのログ出力機能を無効にします。

パラメータを指定しない場合、MAC アドレス認証のすべてのログ出力機能を有効にします。

例

MAC アドレス認証のすべてのログ出力機能を有効にします。

<Switch> system-view

[Switch] mac-authentication access-user log enable

3.1.5 mac-authentication domain

Syntax

mac-authentication domain *domain-name*

undo mac-authentication domain

デフォルト

MAC アドレス認証ユーザの認証ドメインは指定されていません。システムはデフォルトの認証ドメインを使用します。デフォルト認証ドメインの詳細は、オペレーションマニュアルのセクション 9 *セキュリティ*”*AAA*”の **domain default enable** コマンドを参照してください。

View

System view

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

domain-name: ISP ドメインの名前を指定します。設定範囲は 1～255 文字です。大文字、小文字を区別しません。

説明

mac-authentication domain コマンドはグローバルあるいは指定ポートで認証ドメインを指定します。

undo mac-authentication domain コマンドはデフォルトに戻します。

グローバルの認証ドメインは MAC アドレス認証が有効なすべてのポートに適用します。指定ポートの認証ドメインは指定ポートのみに適用します。異なるポートで異なる認証ドメインを指定することができます。

ポートは、以下の順番で MAC アドレス認証ユーザの認証ドメインを選択します。

1) ポートで指定された認証ドメインを指定します。
2) system view で指定されたグローバルの認証ドメインを指定します。
3) デフォルトの認証ドメインを指定します。

例

グローバルの MAC アドレス認証ドメインとしてドメイン domain1 を指定します。

<Switch> system-view

[Switch] mac-authentication domain domain1

GigabitEthernet 1/0/1 の MAC アドレス認証ドメインとしてドメイン aabbcc を指定します。

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] mac-authentication domain aabbcc

関連コマンド

- **display mac-authentication**
- **domain default enable**

3.1.6 mac-authentication guest-vlan

Syntax

mac-authentication guest-vlan *guest-vlan-id*

undo mac-authentication guest-vlan

デフォルト

設定なし

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

guest-vlan-id: MAC アドレス認証ゲスト VLAN として VLAN を指定します。設定範囲は 1～4094 です。VLAN はすでに作成されている必要があります。

説明

mac-authentication guest-vlan コマンドはポートで MAC アドレス認証ゲスト VLAN を指定します。

undo mac-authentication guest-vlan コマンドはデフォルトに戻します。

ポートで MAC アドレス認証に失敗したユーザを適応させるため、ポートで MAC アドレス認証ゲスト VLAN を設定することができます。MAC アドレス認証ゲスト VLAN のユーザは、ソフトウェアやシステムパッチなどをダウンロードするため、ソフトウェアサーバのような制限されたネットワークリソースにアクセスすることができます。MAC アドレス認証ゲスト VLAN が設定されていない場合、MAC アドレス認証に失敗したユーザはネットワークリソースにアクセスすることができません。

MAC アドレス認証ゲスト VLAN として設定された VLAN を削除する前に、**undo mac-authentication guest-vlan** コマンドでゲスト VLAN の設定を削除してください。

例

GigabitEthernet 1/0/1 の MAC アドレス認証ゲスト VLAN として VLAN 100 を設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] mac-authentication guest-vlan 100

関連コマンド

- **display mac-authentication**
- **reset mac-authentication guest-vlan**

3.1.7 mac-authentication guest-vlan auth-period

Syntax

mac-authentication guest-vlan auth-period *period-value*

undo mac-authentication guest-vlan auth-period

デフォルト

30 秒

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

period-value: MAC アドレス認証ゲスト VLAN のユーザを認証する間隔を指定します。設定範囲は 1～3600 秒です。

説明

mac-authentication guest-vlan auth-period コマンドは MAC アドレス認証ゲスト VLAN のユーザを認証する間隔を設定します。

undo mac-authentication guest-vlan auth-period コマンドはデフォルトに戻します。

例

GigabitEthernet 1/0/1 の MAC アドレス認証ゲスト VLAN のユーザを認証する間隔を 150 秒に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] mac-authentication guest-vlan auth-period 150

関連コマンド

- **display mac-authentication**
- **mac-authentication guest-vlan**

3.1.8 mac-authentication max-user

Syntax

mac-authentication max-user *max-number*

undo mac-authentication max-user

デフォルト

4294967295

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

max-number: ポートの MAC アドレス認証のユーザが同時に接続可能な最大数を設定します。設定範囲は 1～4294967295 です。

🕮 **メモ**:

QX-S5100G シリーズは 2048 まで認証動作が可能です。

説明

mac-authentication max-user コマンドはポートの MAC アドレス認証のユーザが同時に接続可能な最大数を設定します。

undo mac-authentication max-user コマンドはデフォルトに戻します。

システムリソースが乱用されることを防止するため、ポートで MAC アドレス認証ユーザが同時に接続する最大数を設定します。最大数に到達したとき、ポートで後続の MAC アドレス認証ユーザは拒否されます。

例

GigabitEthernet 1/0/1 の MAC アドレス認証のユーザが同時に接続可能な最大数を 32 に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] mac-authentication max-user 32

関連コマンド

display mac-authentication

3.1.9 mac-authentication offline-detect enable

Syntax

mac-authentication offline-detect enable

undo mac-authentication offline-detect enable

デフォルト

有効

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

説明

mac-authentication offline-detect enable コマンドはポートで MAC アドレス認証のオフライン状態の検出機能を有効にします。

undo mac-authentication offline-detect enable コマンドはポートで MAC アドレス認証のオフライン状態の検出機能を無効にします。

offline detect timer の期間内にユーザからパケットを受信しない場合、装置はユーザをログオフします。装置は同時にユーザにアカウンティングの停止を要求します。offline detect timer を設定する場合、**mac-authentication timer** コマンドを使用します。

undo mac-authentication offline-detect enable コマンドを設定すると装置は MAC アドレス認証の状態を検出しません。

例

GigabitEthernet 1/0/1 で MAC アドレス認証のオフライン状態の検出を無効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] undo mac-authentication offline-detect enable

関連コマンド

mac-authentication timer

3.1.10 mac-authentication parallel-with-dot1x

Syntax

mac-authentication parallel-with-dot1x

undo mac-authentication parallel-with-dot1x

デフォルト

有効

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

説明

mac-authentication parallel-with-dot1x コマンドはポートで MAC アドレス認証と 802.1X 認証の並列処理を有効にします。

undo mac-authentication parallel-with-dot1x コマンドは無効にします。

ポートでコマンドを設定するとき、以下の制限とガイドラインに従ってください。

- 以下の要件に合うことを確認してください。
  - ポートで 802.1X 認証と MAC アドレス認証の両方を設定してください。802.1X 認証ようにポートで MAC ベースアクセス制御を行ってください。
  - ポートで 802.1X ユニキャストトリガ機能を有効にしてください。
- 802.1X ゲスト VLAN よりも MAC アドレス認証を優先させためには、**dot1x guest-vlan-delay** コマンドで 802.1X ゲスト VLAN を遅延させる必要があります。**dot1x guest-vlan-delay** コマンドの詳細は、コマンドマニュアルのセクション 9 *セキュリティ “802.1X”*を参照してください。
- ポートで MAC アドレス認証の遅延を有効にしないでください。この処理は 802.1X 認証を先に開始させるため MAC アドレス認証を遅延させます。
- ポートで 802.1X 認証と MAC アドレス認証を設定する場合、以下の方法の 1 つを使用してください。
  - ポートで 802.1X と MAC アドレス認証を別々に有効にしてください。
  - ポートでポートセキュリティを有効にしてください。ポートセキュリティのモードは **userlogin-secure-or-mac** あるいは **userlogin-secure-or-mac-ext** に設定してください。

  ポートセキュリティのモードの詳細は、オペレーションマニュアルのセクション 9 *セキュリティ “ポートセキュリティ”*を参照してください。

例

GigabitEthernet 1/0/1 で MAC アドレス認証と 802.1X 認証の並列処理を有効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] mac-authentication parallel-with-dot1x

関連コマンド

display mac-authentication

3.1.11 mac-authentication re-authenticate

Syntax

mac-authentication re-authenticate

undo mac-authentication re-authenticate

デフォルト

無効

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

説明

mac-authentication re-authenticate コマンドはポートで定期的な MAC 再認証機能を有効にします。

undo mac-authentication re-authenticate コマンドはポートで定期的な MAC 再認証機能を無効にします。

定期的 MAC アドレス認証再認証を使用すると、アクセス装置はポートでオンラインの MAC ユーザを定期的に認証できます。この機能は、オンラインユーザの接続状態を追跡し、ACL や VLAN など、サーバによって割り当てられた認証属性を更新します。

定期的再認証タイマを設定するには、system view または Ethernet interface view で **mac-authentication timer reauth-period** コマンドを使用します。

例

GigabitEthernet 1/0/1 で定期的な MAC 再認証機能を有効にし、グローバル定期的再認証タイマを 1800 秒に設定します。

<Switch> system-view

[Switch] mac-authentication timer reauth-period 1800

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] mac-authentication re-authenticate

関連コマンド

- **display mac-authentication**
- **mac-authentication timer**

3.1.12 mac-authentication timer (system view)

Syntax

mac-authentication timer { **offline-detect** *offline-detect-value* | **quiet** *quiet-value* | **reauth-period** *reauth-period-value* | **server-timeout** *server-timeout-value* | **temporary-user-aging** *aging-time-value* | **user-aging** { **critical-vlan** | **guest-vlan** } *aging-time-value* }

undo mac-authentication timer { **offline-detect** | **quiet** | **reauth-period** | **server-timeout** | **temporary-user-aging** *aging-time-value* | **user-aging** { **critical-vlan** | **guest-vlan** } *aging-time-value* }

デフォルト

offline detect timer は 300 秒、quiet timer は 60 秒、server timeout timer は 100 秒です。

View

System view

定義済みユーザロール

network-admin

パラメータ

offline-detect *offline-detect-value*: offline detect timer を設定します。設定範囲は 60～2147483647 秒です。

quiet *quiet-value*: quiet timer を設定します。設定範囲は 1～3600 秒です。

reauth-period *reauth-period-value*: グローバルな定期タイマ再認証 MAC を指定します。設定範囲は 60~86400 秒です。

🕮 **メモ：**

reauth-period *reauth-period-value*オプションの最大設定値はVersion7.1.8 を含む以降のソフトウェアで 86400 まで設定が可能です。
Version7.1.7 を含むそれ以前のソフトウェアは、7200 秒までとなります。

---

server-timeout *server-timeout-value*: server timeout timer を設定します。設定範囲は 100～300 秒です。

temporary-user-aging *aging-time-value*: 一時ユーザエージングタイムを設定します。設定範囲は 60～2147483647 秒です。

説明

mac-authentication timer コマンドは MAC アドレス認証のタイマを設定します。

undo mac-authentication timer コマンドはデフォルトに戻します。

MAC アドレス認証ユーザは以下のタイマを使用します。

- **Offline detect timer**—ユーザがアイドル状態であることを検出するために、装置がユーザからのトラフィックを待つ期間を設定します。ユーザの接続が期間内でアイドル状態になっている場合、装置はユーザをログアウトし、ユーザのアカウントを停止します。このタイマは MAC アドレス認証のオフライン状態の検出機能が有効である場合のみ有効です。

  Offline detect timer を設定したのち、コマンドで MAC アドレスエージングタイマに、**Offline detect timer** と同一の値を設定してください。これによって **Offline**

detect timer の期間内に許可されたユーザの MAC アドレスエントリが終了してしまわないように防止します。

- **Quiet timer**—MAC アドレス認証に失敗したユーザが MAC アドレス認証を実行できるようになるまで、装置が待つ時間をタイマに設定します。Quiet タイムの間は、MAC アドレスからのパケットはすべて廃棄されます。この Quiet メカニズムは、認証が繰り返され、システムのパフォーマンスに影響を与えることを防ぎます。**Quiet timer** は、1 分以内の設定が可能ですが、過去 1 分以内に同じ MAC の認証を失敗していたときは、1 分以内に設定している場合であっても、認証失敗から 1 分間は再認証を処理しません。また、MAC 認証が失敗したとき、失敗したユーザ(MAC アドレス)を Silent MAC users に追加し、**Quiet timer** が動き始めますが、MAC 認証失敗時に 802.1x 認証が動いている期間中だった場合は、失敗したユーザは Silent MAC users へ追加されず、**Quiet timer** が動き始めません。802.1x 認証が失敗したときに、**Quiet timer** が動き始めます。このタイミングで失敗したユーザは Silent MAC users へ追加されます。**Quiet timer** が終了したとき、MAC 認証はすぐには再認証されません。MAC 認証は、802.1x 認証が動き出したときに再認証されます。
- **Server timeout timer**—RADIUS サーバが使用不能であることを検出するために、装置が RADIUS サーバからの応答を待つ時間をタイマに設定します。MAC アドレス認証中にタイムアウトした場合、ユーザはネットワークにアクセスすることはできません。

例

server timeout timer を 150 秒に設定します。

<Switch> system-view

[Switch] mac-authentication timer server-timeout 150

関連コマンド

display mac-authentication

3.1.13 mac-authentication timer (interface view)

Syntax

mac-authentication timer { auth-delay *auth-delay-time* | **reauth-period** *reauth-period-value* }

undo mac-authentication timer { auth-delay | reauth-period }

デフォルト

MAC アドレス認証の開始を遅らせる機能は無効です。ユーザパケットによってすぐに MAC アドレス認証を開始します。

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

auth-delay *auth-delay-time*: MAC アドレス認証の開始を遅らせる遅延時間を指定します。設定範囲は 1～180 秒です。

reauth-period *reauth-period-value*: ポート固有の定期的なタイマ再認証 MAC を秒単位で指定します。設定範囲は 60～7200 です。

説明

mac-authentication timer auth-delay コマンドは MAC アドレス認証の開始を遅らせる機能を有効にし、遅延時間を設定します。

undo mac-authentication timer auth-delay コマンドはデフォルトに戻します。

ポートで 802.1X 認証と MAC アドレス認証の両方の設定が有効である場合、802.1X 認証を優先させるため、MAC アドレス認証を開始する時間を遅らせます。もし遅延時間内に、802.1X 認証が動作しないあるいは 802.1X 認証に失敗したとき、MAC アドレス認証を行います。

MAC アドレス認証の開始を遅らせる機能を設定するとき、ポートセキュリティのモードで **mac-else-userlogin-secure** あるいは **mac-else-userlogin-secure-ext** を設定しないでください。2 つのポートセキュリティのモードのどちらかを設定した場合、ポートで遅延時間の設定は動作しません。ポートセキュリティのモードの詳細は、コマンドマニュアルのセクション 9 *セキュリティ”ポートセキュリティ”*を参照してください。

例

GigabitEthernet 1/0/1 で MAC アドレス認証の開始を遅らせる機能を有効にし、遅延時間を 10 秒に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] mac-authentication timer auth-delay 10

関連コマンド

- **display mac-authentication**
- **port-security port-mode**

3.1.14 mac-authentication timer user-aging

Syntax

mac-authentication timer user-aging { **guest-vlan** } *aging-time-value*

undo mac-authentication timer user-aging guest-vlan

デフォルト

1000 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

user-aging: 指定されたタイプの未認証 VLAN に追加されたユーザのエージングタイマを設定します。

guest-vlan: ゲスト VLAN に参加したユーザのエージングタイマを設定します。

aging-time-value: ユーザエージングタイマの値を設定します。設定範囲は 60～2147483647 です。単位は秒です。

説明

mac-authentication timer user-aging コマンドは、MAC アドレス認証用の非認証 VLAN ユーザエージングタイマーパラメータを設定するには、します。

undo mac-authentication timer user-aging コマンドは、デフォルトに戻します。

ユーザエージングタイマは、指定された VLAN 内のユーザのエージングタイマを設定するために使用されます。ユーザがゲスト VLAN に追加した後、装置はタイマを開始します。設定されたエージングタイマに達すると、ユーザは指定された VLAN を離れます。

このタイマは、**mac-authentication unauthenticated-user aging enable** の場合のみ、有効になります。

ゲスト VLAN 内のユーザのエージングタイマを（**mac-authentication guest-vlan auth-period** による）再認証の間隔の整数倍に設定しないでください。そうでない場合、ユーザエージングタイマは無効になります。

ユーザエージングタイマは、変更後すぐに変更できます。

関連コマンド

- **display mac-authentication**
- **mac-authentication unauthenticated-user aging enable**

3.1.15 mac-authentication unauthenticated-user aging enable

Syntax

mac-authentication unauthenticated-user aging enable

undo mac-authentication unauthenticated-user aging enable

デフォルト

有効

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

mac-authentication unauthenticated-user aging enable コマンドは、認証されていない MAC アドレス認証ユーザエージング機能を有効にします。

undo mac-authentication unauthenticated-user aging enable コマンドは、認証されていない MAC アドレス認証ユーザエージング機能を無効にします。

認証されていない MAC アドレス認証ユーザエージングは、認証されていないか、認証に失敗したために MAC アドレス認証ゲストに追加されたユーザに適用されます。

これらの VLAN のいずれかのユーザがエージングアウトすると、装置は VLAN からユーザを削除し、アクセスポートからユーザのエントリアドレスを削除します。

1 つのポートでこれらの VLAN または VSI のいずれかのユーザが正常に認証され、別のポートでオンラインになるには、この機能を有効にします。それ以外の場合は、この機能を無効にすることをお勧めします。

例

GigabitEthernet 1/0/1 のポートで、認証されていない MAC アドレス認証ユーザのエージング機能を無効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] undo mac-authentication unauthenticated-user aging enable

関連コマンド

mac-authentication timer

3.1.16 mac-authentication user-name-format

Syntax

mac-authentication user-name-format { **fixed** [**account** *name*] | **mac-address** [{ **with-hyphen** | **without-hyphen** } [**lowercase** | **uppercase**]] } [**password** { **cipher** | **simple** } *string*]

undo mac-authentication user-name-format

デフォルト

MAC アドレス認証のユーザ名とパスワードとして各ユーザの MAC アドレスが使用されます。MAC アドレスは 16 進数で、ハイフンなし、小文字です。

View

System view

定義済みユーザロール

network-admin

パラメータ

fixed: すべての MAC アドレス認証ユーザの共有アカウントを使用します。

account *name*: 共有アカウントのユーザ名を指定します。設定範囲は 1～55 文字です。大文字、小文字を区別します。アットマーク（@）は指定できません。指定しない場合、デフォルトのユーザ名が適用されます。

password: 共有ユーザアカウントのパスワードを指定します。

cipher: 暗号テキストのパスワードを設定します。

simple: プレーンテキストのパスワードを設定します。セキュリティのため、プレーンテキストで設定されたパスワードを含むすべてのパスワードは、暗号テキストで保存されます。

string: パスワードを指定します。大文字、小文字を区別します。

- **simple** が指定された場合、設定範囲は 1～63 文字です。
- **cipher** が指定された場合、設定範囲は 1～117 文字です。

mac-address: MAC アドレス認証ユーザの MAC ベースユーザアカウントを使用します。以下のパラメータを使用してユーザ名とパスワードの形式を指定することができます。

- **with-hyphen**: MAC アドレスにハイフンを含みます。たとえば、xx-xx-xx-xx-xx-xx です。
- **without-hyphen**: MAC アドレスにハイフンを含みません。たとえば、xxxxxxxxxxxx です。
- **lowercase**: 小文字を指定します。
- **uppercase**: 大文字を指定します。

説明

mac-authentication user-name-format コマンドは MAC アドレス認証ユーザのユーザアカウントのタイプを設定します。

undo mac-authentication user-name-format コマンドはデフォルトに戻します。

MAC ベースのユーザアカウントを指定する場合、装置はユーザの MAC アドレス認証のユーザ名とパスワードとしてユーザの MAC アドレスを使用します。ユーザアカウントタイプは認証のセキュリティを高めます。しかし、認証サーバはユーザ名とパスワードとしてユーザの MAC アドレスを使用し、各ユーザのユーザアカウントを作成する必要があります。

共有ユーザアカウントを使用する場合、装置は、すべてのユーザの MAC アドレス認証を行うため指定されたユーザ名とパスワードを使用します。すべての MAC アドレスユーザは、認証用に 1 つのアカウントを使用するため、認証サーバで 1 つのアカウントのみを作成します。このユーザアカウントタイプは信頼されたネットワーク用に適しています。

password { **cipher** | **simple** } *string* オプションを使用して、MAC アドレス認証ベースのすべての MAC ユーザアカウントのパスワードを指定できます。パスワードを指定しない場合、各ユーザは独自の MAC アドレスをパスワードとして使用します。

例

MAC アドレス認証ユーザの共有アカウントを設定し、ユーザ名を abc、パスワードをプレーンテキストで xyz に設定します。

<Switch> system-view

[Switch] mac-authentication user-name-format fixed account abc password simple xyz

MAC アドレス認証ユーザの MAC ベースユーザアカウントを設定します。各 MAC アドレスはハイフンつき、大文字の 16 進数で設定します。

<Switch> system-view

[Switch] mac-authentication user-name-format mac-address with-hyphen uppercase

関連コマンド

display mac-authentication

3.1.17 reset mac-authentication access-user

Syntax

reset mac-authentication access-user [**interface** *interface-type interface-number* | **mac** *mac-address* | **username** *username* | **vlan** *vlan-id*]

View

User view

定義済みユーザロール

network-admin

パラメータ

interface *interface-type interface-number*: インタフェースのタイプと番号でポートを指定します。

mac *mac-address*: MAC アドレスで MAC アドレス認証ユーザを指定します。*mac-address* は H-H-H の形式です。

username *username*: ユーザ名で MAC アドレス認証ユーザを指定します。*username* は大文字小文字を区別する 1～253 文字の文字列です。

vlan *vlan-id*: VLAN ID で VLAN を指定します。*vlan-id* の範囲は 1～4094 です。

説明

reset mac-authentication access-user コマンドは MAC アドレス認証ユーザをログオフします。

reset mac-authentication access-user コマンドは特定の MAC アドレス認証ユーザをログオフし、そのユーザ情報を装置から消去します。再度オンラインになるためには、ユーザは MAC アドレス認証を実行してください。

VLAN を指定すると、指定した VLAN の次の MAC アドレス認証ユーザをログオフします。

- MAC アドレス認証を通過し、指定された VLAN を認証 VLAN としてサーバに許可されたユーザ。
- MAC アドレス認証を通過後、認証 VLAN を許可されていないため、指定の VLAN に留まるユーザ。
- 指定の VLAN で MAC アドレス認証を実行中のユーザ。

ユーザが使用中の VLAN を識別するには、**display mac-address** コマンドを使います。

パラメータを指定しない場合は、**reset mac-authentication access-user** コマンドで装置上の MAC アドレス認証ユーザを全てログオフできます。

例

GigabitEthernet 1/0/1 の全 MAC アドレス認証ユーザをログオフします

<Switch> reset mac-authentication access-user interface gigabitethernet 1/0/1

関連コマンド

display mac-authentication connection

3.1.18 reset mac-authentication guest-vlan

Syntax

reset mac-authentication guest-vlan interface *interface-type interface-number* [**mac-address** *mac-address*]

View

User view

定義済みユーザロール

network-admin

パラメータ

interface *interface-type interface-number*: ポートのタイプと番号を指定します。

mac-address *mac-address*: MAC アドレスのユーザを指定します。指定しない場合、ポートの MAC アドレス認証ゲスト VLAN からすべてのユーザを削除します。

説明

reset mac-authentication guest-vlan コマンドはポートの MAC アドレス認証ゲスト VLAN からユーザを削除します。

例

GigabitEthernet 1/0/1 の MAC アドレス認証ゲスト VLAN から MAC アドレス 1-1-1 のユーザを削除します。

<Switch> reset mac-authentication guest-vlan interface gigabitethernet 1/0/1 mac-address 1-1-1

関連コマンド

- **display mac-authentication**
- **mac-authentication guest-vlan**

3.1.19 reset mac-authentication statistics

Syntax

reset mac-authentication statistics [**interface** *interface-type interface-number*]

View

User view

定義済みユーザロール

network-admin

パラメータ

interface *interface-type interface-number*: ポートのタイプと番号を指定します。指定しない場合、すべてのグローバルと指定したポートに関する MAC アドレス認証の統計情報を削除します。

説明

reset mac-authentication statistics コマンドは MAC アドレス認証の統計情報を削除します。

例

GigabitEthernet 1/0/1 の MAC アドレス認証の統計情報を削除します。

<Switch> reset mac-authentication statistics interface gigabitethernet 1/0/1

関連コマンド

display mac-authentication

目次

このセクションのページは **9-x-x** です。

4 章 Web 認証..... 4-1

4章 Web 認証

Web 認証の設定に関するコンフィグについては、別紙の共通マニュアル“*QX シリーズ Ethernet スイッチ Web 認証コマンドマニュアル*（V7）”の“*WebAuth*”を参照してください。

目次

このセクションのページは**9-x-x** です。

5 章 ポートセキュリティ 5-1
5.1 ポートセキュリティ設定コマンド 5-1
5.1.1 display port-security 5-1
5.1.2 display port-security mac-address block 5-5
5.1.3 display port-security mac-address security 5-6
5.1.4 port-security access-user log enable 5-8
5.1.5 port-security authorization ignore 5-9
5.1.6 port-security enable 5-10
5.1.7 port-security enhanced-hardware-mode 5-11
5.1.8 port-security intrusion-mode 5-12
5.1.9 port-security mac-address security 5-13
5.1.10 port-security mac-move bypass-vlan-check 5-15
5.1.11 port-security mac-move permit 5-16
5.1.12 port-security max-mac-count 5-17
5.1.13 port-security ntk-mode 5-18
5.1.14 port-security oui 5-19
5.1.15 port-security port-mode 5-20
5.1.16 port-security timer autolearn aging 5-25
5.1.17 port-security timer disableport 5-26
5.1.18 port-security triple-auth-order mac-dot 1 x-web 5-27
5.1.19 snmp-agent trap enable port-security 5-29

5章 ポートセキュリティ

5.1 ポートセキュリティ設定コマンド

5.1.1 display port-security

Syntax

display port-security [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: ポートのタイプと番号を指定します。指定しない場合、すべてのポートセキュリティの情報を表示します。

説明

display port-security コマンドは、1 つあるいは複数のポートのポートセキュリティの設定、稼働状況、統計情報を表示します。

例

すべてのポートのポートセキュリティの情報を表示します。

<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
  Loop detection action         : Block-drop
```

表 5-1 コマンド出力

フィールド	説明
Port security	ポートセキュリティ機能が有効か無効かを示します。
AutoLearn aging time	Sticky MACアドレスエージングタイマです。単位は分あるいは秒です。
Disableport timeout	不正なパケットを受信するポートの無効状態を解除するタイムアウト時間です。単位は秒です。
MAC move	MAC移動機能の状態です。 ● MAC移動機能が有効である場合、**Permitted**と表示されます。 ● MAC移動機能が無効である場合、**Denied**と表示されます。
Authorization fail	ACLに失敗あるいはユーザプロファイルの許可に失敗したユーザのアクションです。 ● **Online**–ユーザがオンライン接続することを許可します。 ● **Offline**–ユーザをログオフします。
NAS-ID profile	グローバルに適用されたNAS IDのプロファイルです。

フィールド	説明
Dot1x-failure trap	802.1X認証に失敗した際、SNMP notificationの送信を有効にするかどうかを示します。
Dot1x-logon trap	802.1X認証に成功した際、SNMP notificationの送信を有効にするかどうかを示します。
Dot1x-logoff trap	802.1X認証ユーザがログオフした際、SNMP notificationの送信を有効にするかどうかを示します。
Intrusion trap	侵入防止機能のSNMP notificationが有効かどうかを示します。有効な場合、不正なパケットを検出したのち、SNMP notificationを送信します。
Address-learned trap	MACアドレス学習機能のSNMP notificationが有効かどうかを示します。有効な場合、新しいMACアドレスを学習したのち、SNMP notificationを送信します。
Mac-auth-failure trap	MACアドレス認証に失敗した際、SNMP notificationの送信を有効にするかどうかを示します。
Mac-auth-logon trap	MACアドレス認証に成功した際、SNMP notificationの送信を有効にするかどうかを示します。
Mac-auth-logoff trap	MACアドレス認証ユーザがログオフした際、SNMP notificationの送信を有効にするかどうかを示します。
Open authentication	グローバルopen認証モードが有効かどうかを示します。
OUI value list	認証に許可したOUIのリストです。
Port mode	ポートセキュリティモードです。 • **noRestrictions** • **autoLearn** • **macAddressWithRadius** • **macAddressElseUserLoginSecure** • **macAddressElseUserLoginSecureExt** • **secure** • **userLogin** • **userLoginSecure** • **userLoginSecureExt** • **macAddressOrUserLoginSecure** • **macAddressOrUserLoginSecureExt** • **userLoginWithOUI** セキュリティモードの詳細は、オペレーションマニュアルのセクション9 *セキュリティ* “*ポートセキュリティ*”を参照してください。

フィールド	説明
NeedToKnow mode	NTK（Need to know）モードです。 ● **NeedToKnowOnly**–認証された宛先MACアドレスのユニキャストパケットのみ許可します。 ● **NeedToKnowWithBroadcast**–認証された宛先MACアドレスのユニキャストパケット、ブロードキャストパケットのみ許可します。 ● **NeedToKnowWithMulticast**–認証された宛先MACアドレスのユニキャストパケット、マルチキャストパケット、ブロードキャストパケットのみ許可します。 ● **Disabled**–NTKが無効です。
Intrusion protection mode	侵入防止アクションです。 ● **BlockMacAddress**–不正なパケットの送信元MACアドレスをブロックMACアドレスリストに追加します。 ● **DisablePort**–不正なパケットを受信したポートを手動でアップするまでシャットダウンします。 ● **DisablePortTemporarily**–不正なパケットを受信したポートを指定した期間、シャットダウンします。 ● **NoAction**–侵入防止アクションを実行しません。
Learning mode	セキュアMACアドレス学習モードです。 ● **Dynamic** ● **Sticky**
Aging type	セキュアMACアドレスエージングのタイプです。 ● **Periodical**–エージングタイマのみです。 ● **Inactivity**–エージングタイマと一緒にエージング機能を無効にします。
Max secure MAC addresses	ポートでポートセキュリティを許可しているセキュアMACアドレス（あるいはオンラインユーザ）の最大数です。
Current secure MAC addresses	セキュアMACアドレスが記録された数です。
Authorization	認証サーバ（RADIUSサーバあるいはローカル装置）から許可情報が無視されたかどうかを示します。 ● **Permitted**–認証サーバからの許可情報を適用します。 ● **Ignored**–認証サーバからの許可情報を適用しません。
NAS-ID profile	ポートに適用されたNAS IDのプロファイルです。

フィールド	説明
Free VLANs	パケットが認証を開始しないVLANです。 free VLANを設定しない場合、**Not configured**と表示されます。 このフィールドは現在のソフトウェアバージョンでサポートしていません。
Open authentication	open認証モードがポートで有効かどうかを示します。
Loop detection action	ポートのループ検出結果に従って、送信元が不明な受信パケットに対して実行するアクションを示します。 • **Forwarding**–ポートでループが検出されない場合、ポートセキュリティモジュールにより、送信元が不明な受信パケットがポートで認証できます。 • **Block-drop**–ポートでループが検出されると、ポートセキュリティモジュールはポートをブロックし、送信元が不明な受信パケットがポートで認証できません。

5.1.2 display port-security mac-address block

Syntax

display port-security mac-address block [**interface** *interface-type interface-number*] [**vlan** *vlan-id*] [**count**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: ポートのタイプと番号を指定します。

vlan *vlan-id*: VLAN ID を指定します。設定範囲は 1～4094 です。

count: ブロックされた MAC アドレスの数のみを表示します。

説明

display port-security mac-address block コマンドは、ブロックされた MAC アドレスの情報を表示します。

パラメータを指定しない場合、ブロックされたすべての MAC アドレスの情報を表示します。

例

#ブロックされたすべての MAC アドレスの情報を表示します。

<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 ---
```

ブロックされたすべての MAC アドレスの数を表示します。

<Switch> display port-security mac-address block count

```
--- On slot 1, 1 MAC address(es) found ---

--- 1 MAC address(es) found ---
```

表 5-2 コマンド出力

フィールド	説明
MAC ADDR	ブロックされたMACアドレスです。
Port	ブロックされたMACアドレスが送信元アドレスのフレームを受信したポートです。
VLAN ID	ポートが所属するVLANのIDです。
number mac address(es) found	ブロックされたMACアドレスの数です。

関連コマンド

port-security intrusion-mode

5.1.3 display port-security mac-address security

Syntax

display port-security mac-address security [**interface** *interface-type interface-number*] [**vlan** *vlan-id*] [**count**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: ポートのタイプと番号を指定します。

vlan *vlan-id*: VLAN ID を指定します。設定範囲は 1～4094 です。

count: セキュア MAC アドレスの数のみを表示します。

説明

display port-security mac-address security コマンドは、セキュア MAC アドレスの情報を表示します。

セキュア MAC アドレスは、**autoLearn** モードのポートで自動的に学習されるか、**port-security mac-address security** コマンドで設定します。

パラメータを指定しない場合、すべてのセキュア MAC アドレスの情報を表示します。

例

すべてのセキュア MAC アドレスの情報を表示します。

<Switch> display port-security mac-address security

```
MAC addr        VLAN ID  State         Port index                 Aging time
0002-0002-0002  1        Secure        GE1/0/1                    Not aged

--- Number of secure MAC addresses: 1 ---
```

セキュア MAC アドレスの数を表示します。

<Switch> display port-security mac-address security count

```
---  1 mac address(es) found
```

表 5-3 コマンド出力

フィールド	説明
MAC addr	セキュアMACアドレスです。
VLAN ID	ポートが所属するVLANのIDです。
State	追加されたMACアドレスのタイプです。セキュアMACアドレスのタイプは**Secure**と表示されます。
Port index	セキュアMACアドレスが所属するポートです。

フィールド	説明
Aging time	セキュアMACアドレスがエージアウトするまでの時間です。 ● セキュアMACアドレスがスタティックアドレスである場合、**Not aged**と表示されます。 ● セキュアMACアドレスがsticky MACアドレスである場合、エージアウトするまでの時間を表示します。エージングタイマが60秒より短い場合、単位は秒で表示されます。エージングタイマが60秒以上である場合、単位は分で表示されます。デフォルトでsticky MACアドレスはエージアウトしません。**Not aged**と表示されます。
Number of secure MAC addresses	記録されたセキュアMACアドレスの数です。

関連コマンド

port-security mac-address security

5.1.4 port-security access-user log enable

Syntax

port-security access-user log enable [**failed-authorization** | **mac-learning** | **violation**] *

undo port-security access-user log enable [**failed-authorization** | **mac-learning** | **violation**] *

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

パラメータ

failed-authorization: 802.1X または MAC アドレス認証ユーザの認証失敗に対して生成されるログを指定します。

mac-learning: 新しい MAC アドレス学習のために生成されるログを指定します。

violation: 侵入防止がトリガされたときに生成されるログを指定します。

説明

port-security access-user log enable コマンドは、ポートセキュリティユーザのロギングを有効にします。

undo port-security access-user log enable コマンドは、ポートセキュリティユーザのロギングを無効にします。

ポートセキュリティユーザのログが過剰に出力されないようにするには、この機能を無効にすることをお勧めします。

パラメータを指定しない場合、このコマンドはポートセキュリティユーザのすべての種類のロギングを有効にします。

例

侵入防止のログを有効にします。

<Switch> system-view

[Switch] port-security access-user log enable violation

関連コマンド

info-center source portsec logfile deny (コマンドマニュアルのセクション 11 *システム管理*)

5.1.5 port-security authorization ignore

Syntax

port-security authorization ignore

undo port-security authorization ignore

デフォルト

ポートはサーバから受信した許可情報を使用します。

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

説明

port-security authorization ignore コマンドは、認証サーバ（RADIUS サーバあるいはローカル装置）から受信した許可情報を無視するようポートを設定します。

undo port-security authorization ignore コマンドは、デフォルトに戻します。

ユーザが RADIUS あるいはローカル認証を通過後、サーバはユーザのアカウント用に設定された許可属性にもとづいて許可を実行します。たとえば、VLAN が付与されることもあります。ポートがユーザの許可属性を使用しない場合、このコマンドを設定し、サーバから受信した許可情報を無視します。

例

認証サーバから受信した許可情報を無視するように GigabitEthernet 1/0/1 を設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] port-security authorization ignore

関連コマンド

display port-security

5.1.6 port-security enable

Syntax

port-security enable

undo port-security enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

port-security enable コマンドは、ポートセキュリティを有効にします。

undo port-security enable コマンドは、ポートセキュリティを無効にします。

ポートでポートセキュリティを有効にする前にグローバルで 802.1X 認証と MAC アドレス認証を無効にする必要があります。

ポートセキュリティを有効あるいは無効にすると、以下のセキュリティの設定がデフォルトに戻ります。

- 802.1X アクセス制御モードが MAC ベースになります。
- 802.1X ポート許可状態が auto になります。

ポートにオンラインユーザが存在する場合、ポートセキュリティを無効にするとオンラインユーザもログオフします。

例

ポートセキュリティを有効にします。

<Switch> system-view

[Switch] port-security enable

関連コマンド

- **display port-security**
- **dot1x**
- **dot1x port-control**
- **dot1x port-method**
- **mac-authentication**

5.1.7 port-security enhanced-hardware-mode

Syntax

port-security enhanced-hardware-mode

undo port-security enhanced-hardware-mode

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

port-security enhanced-hardware-mode コマンドは拡張ハードウェアモードを有効にします。

undo port-security enhanced-hardware-mode コマンドは、デフォルトに戻します。

デフォルトでは、ハードウェアのリソースを節約するために、一部のプロセスで認証を開始するユーザパケットの VLAN 情報をチェックしません。その結果、ユーザがポート移動できなくなる可能性があります。この問題を回避するため、**port-security mac-move permit** コマンドが設定されている場合には、本機能を一緒に設定します。

ハードウェアリソースを節約するため、**port-security mac-move permit** コマンドを設定していない場合は、拡張ハードウェアモードを無効にしてください。

例

拡張ハードウェアモードを有効にします。

<Sysname> system-view

[Sysname] port-security enhanced-hardware-mode

関連コマンド

- **display port-security**
- **port-security mac-move permit**

5.1.8 port-security intrusion-mode

Syntax

port-security intrusion-mode { **blockmac** | **disableport** | **disableport-temporarily** }

undo port-security intrusion-mode

デフォルト

無効

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

blockmac: 不正なフレームの送信元 MAC アドレスをブロック MAC アドレスリストに追加し、そのフレームを破棄します。ポート上で不正なトラフィックをフィルタします。ブロック MAC アドレスは 3 分間ブロックされた後、正常状態への戻り、確定、変更することができません。**display port-security mac-address block** コマンドを使用して、ブロック MAC アドレスリストを表示することができます。

disableport: 不正なフレームの受信を検出し次第、ポートを無効にします。

disableport-temporarily: 不正なフレームを受信した場合、指定した期間の間、ポートを無効にします。**port-security timer disableport** コマンドで、不正なフレームを受信した際にポートを無効にする期間を設定します。

説明

port-security intrusion-mode コマンドは、ポートが不正なパケットを受信した際に設定されたアクションを行うように、侵入防止機能を設定します。

undo port-security intrusion-mode コマンドは、デフォルトに戻します。

侵入防止機能で無効になったポートの接続を up 状態にする場合、**undo shutdown** コマンドを使用します。

例

侵入防止機能の実行したのち、不正なフレームの送信元 MAC アドレスをブロックするように GigabitEthernet 1/0/1 を設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] port-security intrusion-mode blockmac

関連コマンド

- **display port-security**
- **display port-security mac-address block**
- **port-security timer disableport**

5.1.9 port-security mac-address security

Syntax

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*

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*]

デフォルト

設定なし

View

System view

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

sticky *mac-address*: sticky MAC アドレスを指定します。形式は H-H-H です。**sticky** パラメータを指定しない場合、スタティックセキュア MAC アドレスを設定します。

interface *interface-type interface-number*: ポートのタイプと番号を指定します。

vlan *vlan-id*: セキュア MAC アドレスがある VLAN を指定します。設定範囲は 1～4094 です。指定された VLAN にポートが割り当てられていることを確認してください。

説明

port-security mac-address security コマンドは、セキュア MAC アドレスを追加します。

undo port-security mac-address security コマンドは、セキュア MAC アドレスを削除します。

セキュア MAC アドレスは **autoLearn** モードで設定する、あるいは学習された MAC アドレスです。一度保存されると、装置のリブートが行われても変更されません。VLAN に 1 ポートのみに MAC アドレスを割り当てることができます。

ポートが **autoLearn** モードのとき、認証失敗によってセキュア送信元 MAC アドレスが制限となることを防ぐため、sticky またはスタティックセキュア MAC アドレスとして、重要な MAC アドレスやよく使われる MAC アドレスを追加することができます。ポートにセキュア MAC アドレスを追加するため、最初に以下の作業を完了してください。

- ポートでポートセキュリティを有効にします。
- ポートのセキュリティモードを **autoLearn** に設定します。
- ポートで指定した VLAN のパケットが通過できるように許可する、あるいは VLAN にポートを追加するように設定を行ってください。VLAN が既に存在することを確認してください。

sticky MAC アドレスは **autoLearn** モードで設定または学習されます。sticky MAC アドレスはデフォルトではエージアウトしません。**port-security timer autolearn aging** コマンドで sticky MAC アドレスのエージアウト時間を設定できます。タイマがエージアウトしたとき、sticky MAC アドレスは削除されます。

スタティックセキュア MAC アドレスは、以下の作業を行わない限り、エージアウトしません。

- **undo port-security mac-address security** コマンドで MAC アドレスを削除します。
- ポートセキュリティモードを変更します。
- ポートセキュリティ機能を無効にします。

追加されたセキュア MAC アドレスのタイプを変更することはできません。あるいは追加されたエントリタイプを除いた同一の 2 つのエントリを追加することができません。たとえば、**port-security mac-address security** 1-1-1 **vlan** 10 コマンドが設定されているとき、**port-security mac-address security sticky** 1-1-1 **vlan** 10 を設定することはできません。新しく設定する場合、古い設定を削除する必要があります。

例

ポートセキュリティを有効にし、GigabitEthernet 1/0/1 のポートセキュリティモードを **autoLearn** に設定します。ポートで許可されるセキュア MAC アドレスの最大数を 100 に設定します。

<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

sticky MAC アドレスとして VLAN 4 の MAC アドレス 0001-0002-0003 を指定します。

[Switch-GigabitEthernet1/0/1] port-security mac-address security sticky 0001-0002-0003 vlan 4

[Switch-GigabitEthernet1/0/1] quit

system view で GigabitEthernet 1/0/1 に VLAN 10 に属するセキュア MAC アドレス 0001-0001-0002 を追加します。

[Switch] port-security mac-address security 0001-0001-0002 interface gigabitethernet 1/0/1 vlan 10

関連コマンド

- **display port-security**
- **port-security timer autolearn aging**

5.1.10 port-security mac-move bypass-vlan-check

Syntax

port-security mac-move bypass-vlan-check

undo port-security mac-move bypass-vlan-check

デフォルト

無効

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

説明

port-security mac-move bypass-vlan-check コマンドは VLAN チェックバイパス機能を有効にします。

undo port-security mac-move bypass-vlan-check コマンドは、デフォルトに戻します。

ポート上で VLAN チェックバイパス機能を有効にして、そのポートに移動するユーザの 802.1 X 認証または MAC アドレス認証を開始するパケット内の VLAN 情報のチェックをスキップします。

MAC ベース VLAN でダイナミック VLAN を使用するユーザがポート移動を行う環境では、本コマンドを設定してください。設定をしない場合、移動前後のポートにダイナミック VLAN によって割り当てられる VLAN を明示的に設定する必要があります。

例

VLAN チェックバイパス機能を他のポートから GE1/0/1 ポートへ移動するユーザのために設定します。

<Sysname> system-view

[Sysname] interface gigabitethernet 1/0/1

[Sysname-GigabitEthernet1/0/1] port-security mac-move bypass-vlan-check

関連コマンド

- **display port-security**
- **port-security mac-move permit**

5.1.11 port-security mac-move permit

Syntax

port-security mac-move permit

undo port-security mac-move permit

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

port-security mac-move permit コマンドは、装置で MAC アドレス移動機能を有効にします。

undo port-security mac-move permit コマンドは、デフォルトに戻します。

このコマンドは 802.1X 認証ユーザと MAC アドレス認証ユーザの両方に適用します。

MAC アドレス移動機能を有効にすることで、802.1X 認証あるいは MAC アドレス認証が許可されたユーザが装置のポートを移動できるようになります。たとえば、802.1X 認証ユーザが、802.1X が有効な装置の別のポートに移動する場合、認証セッションが最初のポートから削除され、新しいポートで再認証されます。

もし MAC アドレス移動機能が無効で 802.1X 認証ユーザが別のポートに移動した場合、802.1X 認証あるいは MAC アドレス認証は再認証されません。

認証サーバ（ローカルあるいはリモート）のオンラインユーザが上限に到達した場合、802.1X 認証ユーザあるいは MAC アドレス認証ユーザは装置間のポートを移動することができません。

本機能を使用する場合は、**port-security enhanced-hardware-mode** コマンドを一緒に設定することを推奨します。

例

MAC アドレス移動機能を有効にします。

<Switch> system-view

[Switch] port-security mac-move permit

関連コマンド

- **display port-security**
- **port-security mac-move bypass-vlan-check**
- **port-security enhanced-hardware-mode**

5.1.12 port-security max-mac-count

Syntax

port-security max-mac-count *max-count*

undo port-security max-mac-count

デフォルト

設定なし

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

max-count: ポートに登録できるセキュア MAC アドレスの最大数を指定します。設定範囲は 1～4294967295 です。

説明

port-security max-mac-count コマンドは、ポートセキュリティでポートに登録できるセキュア MAC アドレスの最大数を設定します。

undo port-security max-mac-count コマンドは、デフォルトに戻します。

autoLearn モードでは、ポートでセキュア MAC アドレス（設定した MAC アドレスおよび自動で学習された MAC アドレスの両方）の最大数を設定します。

802.1X 認証モード、MAC アドレス認証モード、もしくは 802.1X 認証と MAC アドレス認証の両方のモードでは、ポートで認証された MAC アドレスの最大数を設定します。

ポートで許可する実際の同時接続ユーザ最大数は、以下の値のいずれか小さい方になります。

- このコマンドで設定される最大数
- 認証モードで許可される同時に接続しているユーザの最大数

たとえば、**userLoginSecureExt** モードにおいて、802.1X 認証がポートセキュリティの MAC アドレスの制限数より多くの同時ユーザを許可している場合、ポートセキュリティの制限が適用されます。

ポートが **autoLearn** モードで動作するとき、ポートセキュリティでセキュア MAC アドレスの最大数を設定することはできません。

🕮 **メモ**：

802.1X 認証や MAC アドレス認証を使用する認証モードの使用可能数は、各認証機能の最大数に依存します。

例

ポートセキュリティで GigabitEthernet 1/0/1 に登録できるセキュア MAC アドレスの最大数を 100 に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] port-security max-mac-count 100

関連コマンド

display port-security

5.1.13 port-security ntk-mode

Syntax

port-security ntk-mode { **ntk-withbroadcasts** | **ntk-withmulticasts** | **ntkonly** }

undo port-security ntk-mode

デフォルト

NTK はポートで設定されていません。すべてのフレームは送信されます。

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

ntk-withbroadcasts: 認証された宛先 MAC アドレスのブロードキャストフレーム、ユニキャストフレームのみを送信します。

ntk-withmulticasts: 認証された宛先 MAC アドレスのブロードキャストフレーム、マルチキャストフレーム、ユニキャストフレームのみを送信します。

ntkonly: 認証された宛先 MAC アドレスのユニキャストフレームのみを送信します。

説明

port-security ntk-mode コマンドは、NTK 機能を設定します。

undo port-security ntk-mode コマンドは、デフォルトに戻します。

NTK（need to know）機能は、送信フレームの宛先 MAC アドレスを確認します。この機能は、不正な装置がネットワークトラフィックを遮断することを防止し、認証にパスした装置のみフレームを送信できるようにします。

例

認証にパスした装置に受信パケットを転送するため、GigabitEthernet 1/0/1 の NTK モードを ntkonly に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] port-security ntk-mode ntkonly

関連コマンド

display port-security

5.1.14 port-security oui

Syntax

port-security oui index *index-value* **mac-address** *oui-value*

undo port-security oui index *index-value*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

index-value: OUI インデックスを指定します。設定範囲は 1～16 です。

oui-value: OUI 値を指定します。形式は H-H-H で 48 ビットの MAC アドレスです。システムは自動的に上位 24 ビットを OUI 値として使用します。

説明

port-security oui コマンドは、ユーザ認証の OUI（Organizationally Unique Identifier）値を設定します。

undo port-security oui コマンドは、指定された OUI インデックスの OUI 値を削除します。

複数の OUI 値を設定することができます。

OUI（MAC アドレスの上位 24 ビット）は、装置ベンダを識別するために IEEE によって割り当てられます。特定の有線装置からのパケットの認証通過や、特定のワイヤレス装置からのパケットの認証開始を装置に設定するときに、このコマンドを使用します。たとえば、会社がイントラネットでベンダ A の IP 電話とプリンタを許可するとき、ベンダ A の OUI を設定するために、このコマンドを使用します。

このコマンドで設定された OUI 値は **userLoginWithOUI** モードで動作するポートにのみ適用します。**userLoginWithOUI** モードのポートは 802.1X ユーザと設定された OUI 値に一致する MAC アドレスのユーザのみ許可します。

例

OUI 値 000d2a を設定し、OUI インデックスを 4 に設定します。

<Switch> system-view

[Switch] port-security oui index 4 mac-address 000d-2a10-0033

関連コマンド

display port-security

5.1.15 port-security port-mode

Syntax

port-security port-mode { **autolearn** | **mac-and-userlogin-secure-ext** | **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

🕮 **メモ：**

mac-and-userlogin-secure-ext オプションは Version7.1.7 を含む以降のソフトウェアからサポートしています。

デフォルト

ポートは **noRestrictions** モードで動作します。ポートセキュリティは適用しません。

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

キーワード	セキュリティモード	説明
autolearn	autoLearn	このポートはMACアドレスを記憶できます。自動で学習されたMACアドレスは、ダイナミックMACアドレスとしてMACアドレステーブルに追加されません。セキュアMACアドレスとしてセキュアMACアドレステーブルに追加されます。**port-security mac-address security**コマンドでセキュアMACアドレスを設定することができます。 **autoLearn**モードのポートは、以下の送信元MACアドレスのフレームを許可します。 ● セキュアMACアドレス ● **mac-address dynamic**コマンドと**mac-address static**コマンドで設定されたMACアドレス **port-security max-mac-count**コマンドで設定されたセキュアMACアドレス数が上限に到達したとき、ポートは**secure**モードに変更します。

キーワード	セキュリティモード	説明
mac-and-userlogin-secure-ext	MacAddressAndUserLoginSecureExt	このモードのポートは、ユーザのMACアドレス認証と、802.1X認証を実行し、ポートベースのアクセス制御を行います。
mac-authentication	macAddressWithRadius	このモードのポートは、ユーザのMACアドレス認証を実行します。複数のユーザを処理します。
mac-else-userlogin-secure	macAddressElseUserLoginSecure	このモードは高いプライオリティを持つMACアドレス認証を行う**macAddressWithRadius**モードと**userLoginSecure**モードの組み合わせです。このモードのポートは、1つの802.1X認証ユーザと複数のMACアドレス認証を許可します。 ● non-802.1Xフレームを受信しているとき、MACアドレス認証のみを実行します。 ● 802.1Xフレームを受信しているとき、MACアドレス認証を行います。MACアドレス認証に失敗した場合は、802.1X認証を行います。
mac-else-userlogin-secure-ext	macAddressElseUserLoginSecureExt	このモードは、ポート上の複数の802.1X認証およびMACアドレス認証を受けたユーザをサポートすること以外は、**macAddressElseUserLoginSecure**モードと同じです。
secure	secure	このモードでは、ポート上のMACアドレスの学習が無効です。**mac-address static** コマンドと**mac-address dynamic**コマンドを使ってMACアドレスの設定ができます。 以下の送信元MACアドレスのフレームを許可します。 ● セキュアMACアドレス ● **mac-address dynamic**コマンドと**mac-address static**コマンドで設定されたMACアドレス

キーワード	セキュリティモード	説明
userlogin	userLogin	このモードのポートは、802.1X認証を実行し、ポートベースのアクセス制御を行います。 1つの802.1Xユーザが認証をパスした場合、他のすべての802.1Xユーザは、認証を受けることなく、ネットワークにアクセスできます。
userlogin-secure	userLoginSecure	このモードのポートは、802.1X認証を実行し、MACベースのアクセス制御を行います。802.1X認証をパスした1ユーザのみに対し、サービスを提供します。
userlogin-secure-ext	userLoginSecureExt	ポート上の複数のオンライン802.1X認証を受けたユーザをサポートすることを除き、**userLoginSecure**モードと同じです。
userlogin-secure-or-mac	macAddressOrUserLoginSecure	このモードは、**userLoginSecure**モードと**macAddressWithRadius**モードを組み合わせたものです。ポートは1つの802.1X認証ユーザと複数のMACアドレス認証を許可します。 このモードでは802.1X認証を最初に実行します。デフォルトで802.1X認証が失敗した場合、MACアドレス認証が実行されます。 このモードのポートは以下の場合、処理が異なります。 ● MACアドレス認証(port-security port-mode mac-authentication)と802.1X認証(port-security port-mode userlogin)の並列処理が有効です。 ● 802.1Xユニキャストトリガ(dot1x unicast-trigger)が有効です。 ● 未認証のMACアドレスからパケットを受信しました。 ポートは802.1X認証を初期化するため、MACアドレスにユニキャストEAP-Request/Identityパケットを送信します。送信後、ポートは802.1X認証結果を待つことなくMACアドレスの処理を即座に行います。

キーワード	セキュリティモード	説明
userlogin-secure-or-mac-ext	macAddressOrUserLoginSecureExt	このモードは、複数の802.1X認証およびMACアドレス認証を受けたポート上のユーザをサポートすること以外は、**macAddressOrUserLoginSecure** モードと同じです。
userlogin-withoui	userLoginWithOUI	**userLoginSecure**モードと同じです。加えて、このモードのポートは、指定されたOUIを含むMACアドレスを持つユーザからのフレームを許可します。 このモードのポートは、OUIの確認を最初に実行します。OUIの確認が失敗した場合、802.1X認証を実行します。ポートはOUIの確認あるいは802.1X認証にパスしたフレームを許可します。

説明

port-security port-mode コマンドは、ポートのセキュリティモードを設定します。

undo port-security port-mode コマンドは、デフォルトに戻します。

ポートセキュリティが有効なポートのセキュリティモードを変更する場合、最初に **noRestrictions** モードに設定します。ポートにオンラインユーザがいる場合、セキュリティモードを変更することができません。

重要:

autoLearn モードで設定している場合、最初に **port-security max-mac-count** コマンドを使用して MAC アドレス数のポートセキュリティ制限を最初に設定してください。ポートが **autoLearn** モードで動作しているとき、設定を変更することはできません。

ポートセキュリティが有効なとき、802.1X や MAC アドレス認証を手動で有効にすることはできません。また、アクセスコントロールモードやポート許可状態を変更することはできません。ポートセキュリティは、異なるセキュリティモードの設定を自動で修正します。

MAC アドレス認証の開始を遅らせる機能が有効なポートで **mac-else-userlogin-secure** モードあるいは **mac-else-userlogin-secure-ext** モードを有効にしないことを推奨します。2 つのモードは MAC アドレス認証の開始を遅らせる機能と同時に設定することができません。MAC アドレス認証の開始を遅らせる機能の詳細は、コマンドマニュアルのセクション 9 *セキュリティ”MAC アドレス認証”*を参照してください。

例

ポートセキュリティを有効にし、GigabitEthernet 1/0/1 が secure モードで動作するように設定します。

<Switch> system-view

[Switch] port-security enable

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] port-security port-mode secure

GigabitEthernet 1/0/1 のポートセキュリティモードを userLogin に変更します。

[Switch-GigabitEthernet1/0/1] undo port-security port-mode

[Switch-GigabitEthernet1/0/1] port-security port-mode userlogin

関連コマンド

- **display port-security**
- **port-security max-mac-count**

5.1.16 port-security timer autolearn aging

Syntax

port-security timer autolearn aging *time-value*

undo port-security timer autolearn aging

デフォルト

セキュア MAC アドレスはエージアウトしません。

View

System view

定義済みユーザロール

network-admin

パラメータ

time-value: セキュア MAC アドレスのエージングタイマを設定します。設定範囲は 0～129600 分です。エージングタイマを無効にする場合、0 に設定します。

説明

port-security timer autolearn aging コマンドは、セキュア MAC アドレスのエージングタイマを設定します。

undo port-security timer autolearn aging コマンドは、デフォルトに戻します。

タイマはすべての sticky セキュア MAC アドレスとポートで自動に学習された MAC アドレスに適用されます。

エージングタイマを短くするとポートアクセスのセキュリティとポートのリソースのユーティリティを向上させますが、オンラインユーザの安定性に影響します。装置の性能とネットワーク環境に従ってセキュア MAC アドレスエージングタイマを適切に設定してください。

エージングタイマを短く（60 秒より短い時間）設定する場合、ポートで設定できるセキュア MAC アドレスの最大数を大きい値に設定しないでください。最大数を大きくすると、性能に影響を及ぼします。

例

セキュア MAC アドレスのエージングタイマを 30 分に設定します。

<Switch> system-view

[Switch] port-security timer autolearn aging 30

関連コマンド

- **display port-security**
- **port-security mac-address security**

5.1.17 port-security timer disableport

Syntax

port-security timer disableport *time-value*

undo port-security timer disableport

デフォルト

20 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

time-value: ポートの無効状態を解除するタイムアウト時間を指定します。設定範囲は 20～300 秒です。

説明

port-security timer disableport コマンドは、ポートの無効状態を解除するタイムアウト時間を設定します。

undo port-security timer disableport コマンドは、デフォルトに戻します。

不正なフレームを受信するたびに一時的にポートを無効にするように侵入防止アクションを設定した場合、このコマンドを使用してタイムアウト時間を設定してください。

例

GigabitEthernet 1/0/1 で不正なフレームを受信するたびに一時的にポートを無効にするように侵入防止アクションを設定し、タイムアウト時間を 30 秒に設定します。

<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

関連コマンド

- **display port-security**
- **port-security intrusion-mode**

5.1.18 port-security triple-auth-order mac-dot 1 x-web

Syntax

port-security triple-auth-order mac-dot 1 x-web

undo port-security triple-auth-order

デフォルト

トリプル認証環境では、最初にトリガーされる認証は、エンドポイントから送信されるパケットのタイプによって異なります。

View

Layer 2 Ethernet interface view

定義済みのユーザロール

network-admin

説明

port-security triple-auth-order mac-dot1x-web コマンドで、トリプル認証環境で MAC アドレス認証、802.1 X 認証、Web 認証の認証方式のトリガーオーダーを設定します。

undo port-security triple-auth-order でデフォルトに戻します。

このコマンドは、トリプル認証がイネーブルになっているポートでのみ有効です。トリプル認証を使用すると、ユーザアクセス用のレイヤ 2 ポートで Web 認証、MAC アドレス認証、および 802.1 X 認証を同時にイネーブルにできます。エンドポイントパケットのタイプが異なると、最初に異なるタイプの認証がトリガーされます。

エンドポイントパケットが最初に MAC アドレス認証をトリガーできるようにするには、このコマンドを使用します。

ポートは、複数の認証方式に対して同時に認証プロセスを実行できます。1 つの認証が失敗しても、他の認証方式のプロセスには影響しません。ただし、エンドポイントがポート上で 1 つの認証を渡すと、デバイスはポート上の他の認証方式のプロセスを次のように処理します。

- エンドポイントが MAC アドレス認証を通過する場合、デバイスはポート上に MAC アドレス認証 ユーザ エントリを生成し、ポート上のエンドポイントに対して 802.1 X 認証を実行し続けます。ただし、デバイスはポート上のエンドポイントの Web 認証を続行できません。
  - MAC アドレス認証の後にエンドポイントが 802.1 X 認証に合格すると、デバイスはポート上のエンドポイントに対して 802.1 X ユーザ エントリを生成します。802.1 X ユーザ エントリは、MAC アドレス認証 ユーザ エントリを上書きします。
  - MAC アドレス認証後にエンドポイントが 802.1 X 認証に合格しない場合、MAC アドレス認証 ユーザ エントリはポートに保持されます。エンドポイントは 802.1 X 認証を再度トリガーできますが、Web 認証はトリガーできません。
- エンドポイントが MAC アドレス認証に失敗し、802.1 X または Web 認証を通過した場合、デバイスは、エンドポイントが通過した認証方式を除き、ポート上のすべての認証方式をただちに停止します。さらに、デバイスは、ポート上のエンドポイントに対して停止した認証方法の認証プロセスをトリガーできなくなります。

このコマンドを使用すると、認証されるユーザは認証に失敗します。ユーザは、オンラインになるために認証を再トリガーする必要があります。ユーザがオンラインにならないようにするためのベストプラクティスとして、このコマンドは注意して使用してください。

例

#MAC アドレス認証、802.1 X 認証、および Web 認証として、GigabitEthernet 1/0/1 での認証方式のトリガー順序を設定化します。

```
<Switch>system-view
[Switch] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet 1/0/1] port-security triple-auth-order mac-dot 1 x-web
```

関連コマンド

- mac-authentication
- dot1x

- web-auth enable

5.1.19 snmp-agent trap enable 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**] *

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

network-operator

パラメータ

address-learned: MAC アドレスを学習した場合、SNMP notification の送信を有効にします。

dot1x-failure: 802.1X 認証に失敗した場合、SNMP notification の送信を有効にします。

dot1x-logoff: 802.1X 認証ユーザがログオフした場合、SNMP notification の送信を有効にします。

dot1x-logon: 802.1X 認証に成功した場合、SNMP notification の送信を有効にします。

intrusion: 不正なフレームを検出した場合、SNMP notification の送信を有効にします。

mac-auth-failure: MAC アドレス認証に失敗した場合、SNMP notification の送信を有効にします。

mac-auth-logoff: MAC アドレス認証ユーザがログオフした場合、SNMP notification の送信を有効にします。

mac-auth-logon: MAC アドレス認証に成功した場合、SNMP notification の送信を有効にします。

説明

snmp-agent trap enable port-security コマンドはポートセキュリティに関する SNMP notification（inform あるいはトラップ）の送信を有効にします。

undo snmp-agent trap enable port-security コマンドはポートセキュリティに関する SNMP notification（inform あるいはトラップ）の送信を無効にします。

NMS に重大なポートセキュリティに関するイベントを通知するため、ポートセキュリティの SNMP notification を有効にします。SNMP notification を正常に送信するため、装置で SNMP の設定を行ってください。SNMP の設定については、オペレーションマニュアルのセクション 11 *システム管理* “*SNMP*”を参照してください。

パラメータを指定しない場合、ポートセキュリティのすべての SNMP notification の送信を有効にします。

snmp-agent trap enable port-security コマンドを適用させるため、侵入防止機能が設定されていることを確認してください。

例

ポートセキュリティに関する SNMP notification の送信を有効にします。

<Switch> system-view

[Switch] snmp-agent trap enable port-security address-learned

関連コマンド

- **display port-security**
- **port-security enable**

目次

このセクションのページは **9-x-x** です。

6 章 User profile 6-1
6.1 User profile 設定コマンド 6-1
6.1.1 display user-profile 6-1
6.1.2 user-profile 6-2

6章 User profile

6.1 User profile 設定コマンド

6.1.1 display user-profile

Syntax

display user-profile [**name** *profile-name*] [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

name *profile-name*: ユーザプロファイル名を指定します。大文字、小文字を区別します。設定範囲は 1～31 文字です。有効な文字は、英字、数字、アンダースコア(_)です。名前は英語の文字で始まり、一意である必要があります。指定しない場合、このコマンドはすべてのユーザプロファイルの設定およびオンラインユーザ情報を表示します。

slot *slot-number*: メンバ ID によって IRF スタックメンバ装置を指定します。指定しない場合、このコマンドは、すべてのメンバ装置のユーザプロファイル設定およびオンラインユーザ情報を表示します。

説明

display user-profile コマンドはユーザプロファイルの設定およびオンラインユーザ情報を表示します。

例

ユーザプロファイル **aaa** の設定とオンラインユーザ情報を表示します。

<Switch> display user-profile name aaa

```
User-Profile: aaa
  Inbound:
    Policy: p1

  User user_1:
    Authentication type: 802.1X
    Network attributes:
```

```
  Interface    : GigabitEthernet1/0/1
  MAC address  : 0000-1111-2222
Failed action list:
  Inbound: Policy p1
```

表 6-1 コマンド出力

フィールド	説明
User-Profile	ユーザプロファイル名です。
Inbound	受信トラフィックに適用されるポリシーです。
Outbound	送信トラフィックに適用されるポリシーです。
Policy	ポリシー名です。
User user_1	ユーザプロファイルが関連付けられているユーザアカウントのユーザ名です。
Authentication type	認証の種類です。 • **802.1X**—802.1X 認証です。 • **Portal**—ポータル認証です。 • **PPP**—PPP 認証です。
Network attributes	オンラインユーザ情報です。
Failed action list	ユーザに適用できなかったアクションです。

6.1.2 user-profile

Syntax

user-profile *profile-name*

undo user-profile *profile-name*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

profile-name: ユーザプロファイル名を指定します。大文字、小文字を区別します。設定範囲は 1～31 文字です。ユーザプロファイル名には英語の文字、数字、アンダースコア(_)のみを使用でき、英語の文字で始まらなければなりません。名前は一意である必要があります。

説明

user-profile コマンドはユーザプロファイルを作成し、そのビューに移行するか、既存のユーザプロファイルのビューに移行します。

undo user-profile コマンドはユーザプロファイルを削除します。

例

ユーザプロファイル **a123** を作成し、**a123** のビューに移行します。

<Switch> display user-profile name aaa

<Switch> system-view

[Switch] user-profile a123

[Switch-user-profile-a123]

目次

このセクションのページは **9-x-x** です。

7 章 パスワード管理 7-1
7.1 パスワード管理設定コマンド 7-1
7.1.1 display password-control 7-1
7.1.2 display password-control blacklist 7-3
7.1.3 password-control { aging | composition | history | length } enable 7-4
7.1.4 password-control aging 7-6
7.1.5 password-control alert-before-expire 7-7
7.1.6 password-control change-password first-login enable 7-8
7.1.7 password-control complexity 7-9
7.1.8 password-control composition 7-10
7.1.9 password-control enable 7-12
7.1.10 password-control expired-user-login 7-13
7.1.11 password-control history 7-14
7.1.12 password-control length 7-15
7.1.13 password-control login idle-time 7-17
7.1.14 password-control login-attempt 7-18
7.1.15 password-control super aging 7-21
7.1.16 password-control super composition 7-21
7.1.17 password-control super length 7-22
7.1.18 password-control update-interval 7-23
7.1.19 reset password-control blacklist 7-24
7.1.20 reset password-control history-record 7-25

7章 パスワード管理

7.1 パスワード管理設定コマンド

7.1.1 display password-control

Syntax

display password-control [**super**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

super: super パスワードのパスワード管理の情報を表示します。指定しない場合、グローバルのパスワード管理の設定を表示します。

説明

display password-control コマンドはパスワード管理の設定を表示します。

Enabled と表示されているコマンドでも、**password-control enable** コマンドの有効化が必要な機能は、**Enabled** と表示されている状態でも動作しません。

例

グローバルのパスワード管理の設定を表示します。

<Switch> display password-control

```
Global password control configurations:
 Password control:                  Enabled (device management users)
                                  Enabled (network access users)
 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
 User authentication timeout:          600 seconds
 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)
```

super パスワードのパスワード管理の設定を表示します。

<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)
```

表 7-1 コマンド出力

フィールド	説明
Password control	パスワード管理機能が有効かどうかを示します。
Password aging	パスワードの有効期限の設定が有効かどうかを示します。有効である場合、有効期限が表示されます。
Password length	最小パスワード長の設定が有効かどうかを示します。有効である場合、設定を表示します。
Password composition	パスワード構成ポリシー機能が有効かどうかを示します。有効である場合、設定を表示します。
Password history	パスワード履歴機能が有効かどうかを示します。有効である場合、設定を表示します。
Early notice on password expiration	ユーザのパスワードの有効期限が終了する前に、ユーザに通知するまでの日数です。
Maximum login attempts	FTPユーザとVTYユーザがログインできる最大試行回数です。
Action for exceeding login attempts	ユーザが試行回数後にログインに失敗したときのアクションです。
Minimum interval between two updates	パスワードアップデートの最小間隔です。
Login with aged password	パスワードの有効期限後、ユーザがログインできる最大日時と最大回数です。
Password complexity	パスワード複雑性の確認が有効かどうかを示します。 ● **username checking**—パスワードはユーザ名あるいはユーザ名の逆の順番を含むかどうかを確認します。 ● **repeated characters checking**—文字あるいは数字が3回以上連続して続くかどうかを確認します。

7.1.2 display password-control blacklist

Syntax

display password-control blacklist [**user-name** *user-name* | **ip** *ipv4-address* | **ipv6** *ipv6-address*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

user-name *user-name*: ユーザ名を指定します。設定範囲は 1～55 文字です。大文字、小文字を区別します。

ip *ipv4-address*: ユーザの IPv4 アドレスを指定します。

ipv6 *ipv6-address*: ユーザの IPv6 アドレスを指定します。

説明

display password-control blacklist コマンドはパスワード管理ブラックリストの情報を表示します。

パラメータを指定しない場合、パスワード管理ブラックリストのすべてのユーザの情報を表示します。

コンソールポートを経由してアクセスしたユーザが認証に失敗すると、そのユーザアカウントがパスワード制御ブラックリストに追加されます。FTP や VTY ユーザが認証に失敗すると、その IP アドレスおよびユーザアカウントがパスワード制御ブラックリストに追加されます。**display password-control blacklist** コマンドを使用して、ブラックリストに掲載されたユーザに関する情報を表示できます。

例

パスワード管理ブラックリストのユーザの情報を表示します。

<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
```

表 7-2 コマンド出力

フィールド	説明
Blacklist items matched	ブラックリストのユーザ数です。
IP address	ユーザのIPアドレスです。
Login failures	ログイン失敗回数です。
Lock flag	ユーザログインの禁止が行われているかどうかを示します。IPアドレスを持つユーザの場合、ユーザアカウントとIPアドレスの両方がロックされます。 IPアドレスを持たないユーザの場合は、ユーザアカウントだけがロックされます。ユーザは、このユーザアカウントを使用してコンソール回線経由でログインすることはできません。 ● **unlock**—禁止されていません。 ● **lock**— **password-control login-attempt**コマンドによって一時的あるいは永久に禁止されています。

7.1.3 password-control { aging | composition | history | length } enable

Syntax

password-control { **aging** | **composition** | **history** | **length** } **enable**

undo password-control { **aging** | **composition** | **history** | **length** } **enable**

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

パラメータ

aging: パスワードの有効期限の設定を有効にします。

composition: パスワード構成ポリシー機能を有効にします。

history: パスワード履歴機能を有効にします。

length: 最小パスワード長の設定を有効にします。

説明

password-control { **aging | composition | history | length** } **enable** コマンドはパスワード管理機能（有効期限、パスワード構成ポリシー、パスワード履歴、最小パスワード長の機能）を有効にします。

undo password-control { **aging | composition | history | length** } **enable** コマンドはパスワード管理機能を無効にします。

グローバルパスワード制御機能（**password-control enable** コマンド）が有効であるかどうかに関係なく、パスワード構成の制限および最小パスワード長制限がデフォルトで有効になります。デフォルトでは、パスワード構成ポリシーと最小パスワード長は次のとおりです。

- パスワードには、2 つ以上の文字タイプと、各タイプにつき 1 つ以上の文字を含める必要があります。
- パスワードは 10 文字以上にする必要があります。

装置管理ユーザのパスワードがハッシュ形式の場合、次の要件を満たしていても、パスワードに対する制限設定は有効になりません。

- グローバルパスワード制御が有効
- パスワード制限機能が有効

undo password-control history enable コマンドを実行した後、システムは新しいパスワードと履歴パスワードを比較しませんが、履歴パスワードの記録は停止しません。ユーザの履歴パスワードレコードの数が **password-control history** コマンドで設定された最大数に達すると、最新の履歴レコードによって最も古い履歴レコードが上書きされます。

例

グローバルパスワード管理機能を有効にします。

<Switch> system-view

[Switch] password-control enable

パスワード構成ポリシー機能を有効にします。

[Switch] password-control composition enable

パスワードの有効期限の機能を有効にします。

[Switch] password-control aging enable

最小パスワード長の設定を有効にします。

[Switch] password-control length enable

パスワード履歴の機能を有効にします。

[Switch] password-control history enable

関連コマンド

- **display password-control**
- **password-control enable**

7.1.4 password-control aging

Syntax

password-control aging *aging-time*

undo password-control aging

デフォルト

パスワードの有効期限は 90 日です。ユーザグループのパスワードの有効期限はグローバルの設定と同一です。ローカルユーザのパスワードの有効期限はローカルユーザが所属しているユーザグループのパスワードの有効期限と同一です。

View

System view

User group view

Local user view

定義済みユーザロール

network-admin

パラメータ

aging-time: パスワードの有効期限を指定します。設定範囲は 1～365 日です。

説明

password-control aging コマンドはパスワードの有効期限を設定します。

undo password-control aging コマンドはデフォルトに戻します。

パスワードの有効期限は各 view に依存します。

- system view のパスワードの有効期限はグローバルであり、すべてのユーザグループに適用します。
- user group view のパスワードの有効期限はユーザグループのすべてのローカルユーザに適用します。
- local user view のパスワードの有効期限はローカルユーザのみに適用します。

パスワードの有効期限は小さい範囲でのパスワードの設定が高い優先度を持ちます。システムはローカルユーザに local user view のパスワードの有効期限を使用します。

- ローカルユーザにパスワードの有効期限が設定されていない場合、システムはローカルユーザが所属しているユーザグループのパスワードの有効期限を使用します。

- ユーザグループにパスワードの有効期限が設定されていない場合、システムはグローバルのパスワードの有効期限を使用します。

例

グローバルのパスワードの有効期限を 80 日に設定します。

<Switch> system-view

[Switch] password-control aging 80

ユーザグループ **test** のパスワードの有効期限を 90 日に設定します。

[Switch] user-group test

[Switch-ugroup-test] password-control aging 90

[Switch-ugroup-test] quit

装置管理ユーザ **abc** のパスワードの有効期限を 100 日に設定します。

[Switch] local-user abc class manage

[Switch-luser-manage-abc] password-control aging 100

関連コマンド

- **display local-user**
- **display password-control**
- **display user-group**
- **password-control aging enable**

7.1.5 password-control alert-before-expire

Syntax

password-control alert-before-expire *alert-time*

undo password-control alert-before-expire

デフォルト

7 日

View

System view

定義済みユーザロール

network-admin

パラメータ

alert-time: ユーザのパスワードの有効期限が終了する前にユーザに通知するまでの日数を指定します。設定範囲は 1～30 日です。

説明

password-control alert-before-expire コマンドはユーザのパスワードの有効期限が終了する前に、ユーザに通知するまでの日数を設定します。

undo password-control alert-before-expire コマンドはデフォルトに戻します。

このコマンドは FTP ユーザ以外のユーザに適用されます。FTP ユーザは、管理者によってのみパスワードを変更することができます。

例

ユーザのパスワードの有効期限が終了する前に、ユーザに通知するまでの日数を 10 日に設定します。

<Switch> system-view

[Switch] password-control alert-before-expire 10

関連コマンド

display password-control

7.1.6 password-control change-password first-login enable

Syntax

password-control change-password first-login enable

undo password-control change-password first-login enable

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

password-control change-password first-login enable コマンドは、初回ログイン時のパスワード変更機能を有効にします。

undo password-control change-password first-login enable コマンドは、初回ログイン時のパスワード変更機能を無効にします。

初回ログイン時のパスワード変更機能を有効にするには、**password-control enable** コマンドと **password-control change-password first-login enable** コマンドの両方を設定する必要があります。

例

初回ログイン時のパスワード変更機能を有効に設定します。

<Switch> system-view

[Switch] password-control change-password first-login enable

関連コマンド

- **display password-control**
- **password-control enable**

7.1.7 password-control complexity

Syntax

password-control complexity { **same-character** | **user-name** } **check**

undo password-control complexity { **same-character** | **user-name** } **check**

デフォルト

ユーザグループのパスワードの複雑性のポリシーはグローバルの設定と同一です。ローカルユーザのパスワードの複雑性のポリシーはローカルユーザが所属しているユーザグループのパスワードの複雑性のポリシーと同一です。

グローバルのパスワードの複雑性のポリシーは、**user-name check** は有効、**same-character check** は無効です。

View

System view

User group view

Local user view

定義済みユーザロール

network-admin

パラメータ

same-character: パスワードに文字あるいは数字が 3 回以上連続して続くことを禁止します。たとえば、パスワード **aaabc** はポリシーに適合しません。

user-name: パスワードにユーザ名あるいはユーザ名の逆の順番を含むことを禁止します。たとえば、ユーザ名が **123** であるとき、**abc123** あるいは **321df** のパスワードはポリシーに適合しません。**password-control enable** コマンドを設定していなくても、本コマンドが有効な場合には有効になります。

説明

password-control complexity コマンドはパスワードの複雑性のポリシーを設定します。

undo password-control complexity コマンドはパスワードの複雑性のポリシーを削除します。

パスワードの複雑性のポリシーは各 view に依存します。

- system view のパスワードの複雑性のポリシーはグローバルであり、すべてのユーザグループに適用します。
- user group view のパスワードの複雑性のポリシーはユーザグループのすべてのローカルユーザに適用します。
- local user view のパスワードの複雑性のポリシーはローカルユーザのみに適用します。

パスワードの複雑性のポリシーは小さい範囲でのパスワードの設定が高い優先度を持ちます。システムはローカルユーザに local user view のパスワードの複雑性のポリシーを使用します。

- ローカルユーザにパスワードの複雑性のポリシーが設定されていない場合、システムはローカルユーザが所属しているユーザグループのパスワードの複雑性のポリシーを使用します。
- ユーザグループにパスワードの複雑性のポリシーが設定されていない場合、システムはグローバルのパスワードの複雑性のポリシーを使用します。

パスワード内のユーザ名の有無の確認と、パスワードの文字の反復回数の確認の両方を有効にすることができます。

例

パスワード内のユーザ名の有無の確認、あるいはパスワードの文字の反復回数の確認を禁止するパスワードの複雑性のポリシーを設定します。

<Switch> system-view

[Switch] password-control complexity user-name check

関連コマンド

- **display local-user**
- **display password-control**
- **display user-group**

7.1.8 password-control composition

Syntax

password-control composition type-number *type-number* [**type-length** *type-length*]

undo password-control composition

デフォルト

グローバルのパスワード構成ポリシーは、少なくとも 2 種類の文字タイプと、各タイプに 1 文字以上を含む必要があります。

ユーザグループのパスワード構成ポリシーはグローバルの設定と同一です。ローカルユーザのパスワード構成ポリシーはローカルユーザが所属しているユーザグループのパスワード構成ポリシーと同一です。

View

System view

User group view

Local user view

定義済みユーザロール

network-admin

パラメータ

type-number *type-number*: パスワードに含まれる文字タイプの最小数を指定します。設定範囲は 1~4 です。

type-length *type-length*: パスワードの各タイプの最小文字数を指定します。設定範囲は 1～63 です。

説明

password-control composition コマンドはパスワード構成ポリシーを設定します。

undo password-control composition コマンドはデフォルトに戻します。

password-control enable コマンドを設定していなくても、本コマンドの設定が有効になります。

パスワード構成ポリシーは各 view に依存します。

- system view のパスワード構成ポリシーはグローバルであり、すべてのユーザグループに適用します。
- user group view のパスワード構成ポリシーはユーザグループのすべてのローカルユーザに適用します。
- local user view のパスワード構成ポリシーはローカルユーザのみに適用します。

パスワード構成ポリシーは小さい範囲でのパスワードの設定が高い優先度を持ちます。システムはローカルユーザに local user view のパスワード構成ポリシーを使用します。

- ローカルユーザにパスワード構成ポリシーが設定されていない場合、システムはローカルユーザが所属しているユーザグループのパスワード構成ポリシーを使用します。
- ユーザグループにパスワード構成ポリシーが設定されていない場合、システムはグローバルのパスワード構成ポリシーを使用します。

文字タイプの最小数と各タイプの最小文字数はパスワードの最大長より小さくする必要があります。

例

すべてのパスワードに少なくとも 4 種類の文字と各タイプに 5 文字以上を含むように指定します。

<Switch> system-view

[Switch] password-control composition type-number 4 type-length 5

ユーザグループ **test** のパスワードに少なくとも 4 種類の文字と各タイプに 5 文字以上を含むように指定します。

[Switch] user-group test

[Switch-ugroup-test] password-control composition type-number 4 type-length 5

[Switch-ugroup-test] quit

装置管理ユーザ **abc** のパスワードに少なくとも 4 種類の文字と各タイプに 5 文字以上を含むように指定します。

[Switch] local-user abc class manage

[Switch-luser-manage-abc] password-control composition type-number 4 type-length 5

関連コマンド

- **display local-user**
- **display password-control**
- **display user-group**
- **password-control composition enable**

7.1.9 password-control enable

Syntax

password-control enable

undo password-control enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

password-control enable コマンドはグローバルでパスワード管理機能を有効にします。

undo password-control enable コマンドはグローバルでパスワード管理機能を無効にします。

グローバルでパスワード管理機能を有効にしたのち、指定したパスワード管理機能が適用されます。

グローバルでパスワード管理機能を有効にしたのち、対応する **display** コマンドを使用して装置管理ユーザのパスワード設定と super パスワードの設定を表示することはできません。ネットワークアクセスユーザのパスワード設定が表示されます。装置管理ユーザの設定された初期パスワードは少なくとも 4 種類の文字を含む必要があります。

例

グローバルでパスワード管理機能を有効にします。

<Switch> system-view

[Switch] password-control enable

関連コマンド

- **display password-control**
- **password-control** { **aging** |**composition** | **history** | **length** } **enable**

7.1.10 password-control expired-user-login

Syntax

password-control expired-user-login delay *delay* **times** *times*

undo password-control expired-user-login

デフォルト

ユーザはパスワードの有効期限が終了したのち、30 日以内に 3 回ログインすることができます。すべてのログイン試行に失敗するか、30 日後にユーザがログイン試行を行うと、ユーザに新しいパスワードを設定するようプロンプトが表示されます。

View

System view

定義済みユーザロール

network-admin

パラメータ

delay *delay*: パスワードの有効期限が終了した後、ユーザがログインできる最大日時を設定します。設定範囲は 1～90 日です。

times *times*: パスワードの有効期限が終了した後、ユーザがログインできる最大回数を設定します。設定範囲は 0～10 です。パスワードの有効期限が終了した後、ユーザがシステムプロンプトで新しいパスワードを設定するには、値を 0 に設定します。

説明

password-control expired-user-login コマンドはパスワードの有効期限が終了した後、ユーザがログインできる最大日時と最大回数を設定します。

undo password-control expired-user-login コマンドはデフォルトに戻します。

このコマンドは、FTP 以外のログインユーザにのみ有効です。

FTP ユーザはパスワードの有効期限が終了した後、ログインすることができません。

例

パスワードの有効期限が終了した後、ユーザがログインできる最大日時を 60 日、最大回数を 5 回に設定します。

<Switch> system-view

[Switch] password-control expired-user-login delay 60 times 5

関連コマンド

display password-control

7.1.11 password-control history

Syntax

password-control history *max-record-number*

undo password-control history

デフォルト

4

View

System view

定義済みユーザロール

network-admin

パラメータ

max-record-number: 各ユーザのパスワード履歴の最大数を指定します。設定範囲は 2～15 です。

説明

password-control history コマンドは各ユーザのパスワード履歴の最大数を設定します。

undo password-control history コマンドはデフォルトに戻します。

パスワード履歴が最大数になったとき、後続のパスワード履歴はもっとも古いパスワードに上書きします。

システムは **undo password-control history enable** コマンドを実行した後、パスワードの記録を停止しますが、すでに記録されたパスワードを削除しません。

既存のパスワード履歴を削除する場合、以下のいずれかの方法を使用します。

- グローバルでパスワード管理機能を無効にするため、**undo password-control enable** コマンドを使用します。
- 手動でパスワードを削除するため、**reset password-control history-record** コマンドを使用します。

例

各ユーザのパスワード履歴の最大数を 10 に設定します。

<Switch> system-view

[Switch] password-control history 10

関連コマンド

- **display password-control**
- **password-control history enable**
- **reset password-control blacklist**

7.1.12 password-control length

Syntax

password-control length *length*

undo password-control length

デフォルト

グローバルの最小パスワード長は 10 文字です。

ユーザグループの最小パスワード長はグローバルの設定と同一です。ローカルユーザの最小パスワード長はローカルユーザが所属しているユーザグループの最小パスワード長と同一です。

View

System view

User group view

Local user view

定義済みユーザロール

network-admin

パラメータ

length: 最小パスワード長を指定します。設定範囲は 4～32 文字です。

説明

password-control length コマンドは最小パスワード長を設定します。

undo password-control length コマンドはデフォルトに戻します。

password-control enable コマンドを設定していなくても、本コマンドの設定が有効になります。

最小パスワード長の設定は各 view に依存します。

- system view の最小パスワード長の設定はグローバルであり、すべてのユーザグループに適用します。
- user group view の最小パスワード長の設定はユーザグループのすべてのローカルユーザに適用します。
- local user view の最小パスワード長の設定はローカルユーザのみに適用します。

最小パスワード長の設定は小さい範囲でのパスワードの設定が高い優先度を持ちます。システムはローカルユーザに local user view の最小パスワード長の設定を使用します。

- ローカルユーザに最小パスワード長が設定されていない場合、システムはローカルユーザが所属しているユーザグループの最小パスワード長の設定を使用します。
- ユーザグループに最小パスワード長が設定されていない場合、システムはグローバルの最小パスワード長の設定を使用します。

例

グローバルの最小パスワード長を 16 文字に設定します。

<Switch> system-view

[Switch] password-control length 16

ユーザグループ **test** の最小パスワード長を 16 文字に設定します。

[Switch] user-group test

[Switch-ugroup-test] password-control length 16

[Switch-ugroup-test] quit

装置管理ユーザ **abc** の最小パスワード長を 16 文字に設定します。

[Switch] local-user abc class manage

[Switch-luser-manage-abc] password-control length 16

関連コマンド

- **display local-user**
- **display password-control**
- **display user-group**
- **password-control length enable**

7.1.13 password-control login idle-time

Syntax

password-control login idle-time *idle-time*

undo password-control login idle-time

デフォルト

90 日

View

System view

定義済みユーザロール

network-admin

パラメータ

idle-time: アカウントアイドルタイムの最大日数を指定します。設定範囲は 0～365 日です。0 はアカウントアイドルタイムの制限を行いません。

説明

password-control login idle-time コマンドはアカウントアイドルタイムの最大日数を設定します。

undo password-control login idle-time コマンドはデフォルトに戻します。

ユーザが最後にログインしてから指定した期間内にログインしない場合、ユーザアカウントは無効になります。

例

アカウントアイドルタイムの最大日数を 30 日に設定します。

<Switch> system-view

[Switch] password-control login idle-time 30

関連コマンド

display password-control

7.1.14 password-control login-attempt

Syntax

password-control login-attempt *login-times* [**exceed** { **lock** | **lock-time** *time* | **unlock** }]

undo password-control login-attempt

デフォルト

グローバルのログイン試行の設定は以下です。

- 連続してログインに失敗できる最大数は 3 です。
- 3 回ログインに失敗した後、ログインの試行を無効にする時間は 1 分です。

ユーザグループのログイン試行の設定はグローバルの設定と同一です。ローカルユーザのログイン試行の設定はローカルユーザが所属しているユーザグループのログイン試行の設定と同一です。

View

System view

User group view

Local user view

定義済みユーザロール

network-admin

パラメータ

login-times: 連続してログインに失敗できる最大数を指定します。設定範囲は 2～10 です。

exceed: ユーザが試行回数後にログインに失敗した後のアクションを指定します。

- **lock**: FTP または VTY ユーザの場合、ユーザアカウントとユーザの IP アドレスは両方ともロックされます。このロックされた IP アドレスからは、このユーザアカウントを使用してログインできません。 コンソールユーザの場合、ユーザアカウントがロックされます。ユーザは、このユーザアカウントを使用してコンソール回線経由でログインできません。
- **lock-time** *time*: 設定範囲は 1～360 分です。
  ロックタイマが期限切れになると、FTP または VTY ユーザはこのユーザアカウントを使用して、IP アドレスから再度ログインできます。ロックタイマが期限切れになると、コンソールユーザはこのユーザアカウントを使用して再度ログインできます。
- **unlock**: ユーザが試行回数後にログインに失敗した後もユーザアカウントを使用することができます。

説明

password-control login-attempt コマンドはログイン試行の制限を設定します。ログイン最大試行回数と、ユーザが試行回数後にログインに失敗したときのアクションを設定できます。

undo password-control login-attempt コマンドはデフォルトに戻します。

ログイン試行の制限の設定は各 view に依存します。

- system view のログイン試行の制限の設定はグローバルであり、すべてのユーザグループに適用します。
- user group view のログイン試行の制限の設定はユーザグループのすべてのローカルユーザに適用します。
- local user view のログイン試行の制限の設定はローカルユーザのみに適用します。

ログイン試行の制限の設定は小さい範囲でのパスワードの設定が高い優先度を持ちます。システムはローカルユーザに local user view のログイン試行の制限の設定を使用します。

- ローカルユーザにログイン試行の制限が設定されていない場合、システムはローカルユーザが所属しているユーザグループのログイン試行の制限の設定を使用します。
- ユーザグループにログイン試行の制限が設定されていない場合、システムはグローバルのログイン試行の制限の設定を使用します。

FTP あるいは VTY ユーザが最大ログイン試行後にログインに失敗した場合、システムはユーザアカウントとユーザの IP アドレスをパスワード管理ブラックリストに追加します。

コンソールユーザも同様の操作でパスワード管理ブラックリストに追加します

アカウントは、ブラックリストに追加されたユーザのみロックされます。他のユーザはアカウントを使用することができます。ブラックリストに記載されているユーザは他のユーザアカウントを使用することができます。ロックされた IP アドレスのユーザに対してのみロックされます。ロック解除された IP アドレスのユーザはこのアカウントを使用でき、ロックされた IP アドレスのユーザは他のロック解除されたユーザアカウントを使用できます。

- ユーザのユーザアカウントが永久にロックされた場合、パスワード管理ブラックリストからアカウントを削除しない限り、ユーザはこのアカウントを使用することができません。ユーザアカウントを削除する場合、**reset password-control blacklist** コマンドを使用します。
- 一時的にロックされたユーザアカウントを使用する場合、以下のいずれかの処理を行うことができます。
  - □　ロックしているタイマが終了するまで待ちます。
  - □　パスワード管理ブラックリストからアカウントを削除します。
- ユーザアカウントとユーザがブラックリストに登録されているが、ロックされていない場合、ユーザは、このアカウントを使用してログインを行うことができます。ユーザがユーザアカウントを使用して装置に正常にログインしたとき、パスワード管理ブラックリストからアカウントとユーザの IP アドレスが削除されます。

password-control login-attempt コマンドは、コマンドが設定されたのち、すぐに適用されます。パスワード管理ブラックリストにすでに存在するユーザも適用されます。

例

ユーザアカウントのログイン最大試行回数を 4 に設定し、ユーザが試行回数後にログインに失敗した後、ユーザアカウントを無効にします。

<Switch> system-view

[Switch] password-control login-attempt 4 exceed lock

装置にログインするユーザアカウント **test** を使用し、4 回間違ったパスワードを入力します。

パスワード管理ブラックリストを表示します。出力は、ブラックリストのユーザアカウントに存在し、アクションが **lock** であることを示します。

[Switch] display password-control blacklist

```
Username: test
   IP: 192.168.44.1       Login failures: 4     Lock flag: lock

Blacklist items matched: 1.
```

192.168.44.1 のユーザが、このユーザアカウントを使用してログインできないことを確認します。

ユーザアカウントのログイン試行回数を 2 に設定し、ユーザが試行回数後にログインに失敗した後、3 分間、ユーザアカウントを無効にします。

<Switch> system-view

[Switch] password-control login-attempt 2 exceed lock-time 3

装置にログインするユーザアカウント **test** を使用し、2 回間違ったパスワードを入力します。

パスワード管理ブラックリストを表示します。出力は、ブラックリストのユーザアカウントに存在し、アクションが **lock** であることを示します。

[Switch] display password-control blacklist

```
Username: test
   IP: 192.168.44.1       Login failures: 2     Lock flag: lock

Blacklist items matched: 1.
```

3 分後、ユーザアカウントがパスワード管理ブラックリストから削除され、192.168.44.1 のユーザが、このユーザアカウントを使用してログインできることを確認します。

関連コマンド

- **display local-user**
- **display password-control**
- **display password-control blacklist**
- **display user-group**

- **reset password-control blacklist**

7.1.15 password-control super aging

Syntax

password-control super aging *aging-time*

undo password-control super aging

デフォルト

90 日

View

System view

定義済みユーザロール

network-admin

パラメータ

aging-time: super パスワードの有効期限を指定します。設定範囲は 1～365 日です。

説明

password-control super aging コマンドは super パスワードの有効期限を設定します。

undo password-control super aging コマンドはデフォルトに戻します。

例

super パスワードの有効期限を 10 日に設定します。

<Switch> system-view

[Switch] password-control super aging 10

関連コマンド

- **display password-control**
- **password-control aging**

7.1.16 password-control super composition

Syntax

password-control super composition type-number *type-number* [**type-length** *type-length*]

undo password-control super composition

デフォルト

superパスワード構成ポリシーは少なくとも 2種類の文字と各タイプに 1文字以上を含む必要があります。

View

System view

定義済みユーザロール

network-admin

パラメータ

type-number *type-number*: superパスワードに含まれる文字タイプの最小数を指定します。設定範囲は 1～4 文字です。

type-length *type-length*: パスワードの各タイプの最小数を指定します。設定範囲は 1～63 です。

説明

password-control super composition コマンドは super パスワードの複雑性のポリシーを設定します。

undo password-control super composition コマンドはデフォルトに戻します。

password-control enable コマンドを設定していなくても、本コマンドの設定が有効になります。

文字タイプの最小数と各タイプの最小文字数は super パスワードの最大長より小さくする必要があります。

例

superパスワードに少なくとも 4 種類の文字と各タイプに 5文字以上を含むように指定します。

<Switch> system-view

[Switch] password-control super composition type-number 4 type-length 5

関連コマンド

- **display password-control**
- **password-control composition**

7.1.17 password-control super length

Syntax

password-control super length *length*

undo password-control super length

デフォルト

10 文字

View

System view

定義済みユーザロール

network-admin

パラメータ

length: super パスワードの最小パスワード長を指定します。設定範囲は 4～63 です。

説明

password-control super length コマンドは super パスワードの最小パスワード長を設定します。

undo password-control super length コマンドはデフォルトに戻します。

password-control enable コマンドを設定していなくても、本コマンドの設定が有効になります。

例

super パスワードの最小パスワード長を 16 文字に設定します。

<Switch> system-view

[Switch] password-control super length 16

関連コマンド

- **display password-control**
- **password-control length**

7.1.18 password-control update-interval

Syntax

password-control update-interval *interval*

undo password-control update-interval

デフォルト

24 時間

View

System view

定義済みユーザロール

network-admin

パラメータ

interval: パスワードアップデートの最小間隔を指定します。設定範囲は 0～168 時間です。0 はパスワードのアップデートを行わないことを示します。

説明

password-control update-interval コマンドはパスワードアップデートの最小間隔を設定します。パスワードアップデートの最小間隔はユーザがパスワードを変更できる最小間隔です。

undo password-control update-interval コマンドはデフォルトに戻します。

設定された最小間隔は、最初のログイン時またはパスワードの有効期限が切れた後にパスワードの変更を求められる装置管理ユーザでは有効ではありません。

例

パスワードアップデートの最小間隔を 36 時間に設定します。

<Switch> system-view

[Switch] password-control update-interval 36

関連コマンド

display password-control

7.1.19 reset password-control blacklist

Syntax

reset password-control blacklist [**user-name** *user-name*]

View

User view

定義済みユーザロール

network-admin

パラメータ

user-name *user-name*: パスワード管理ブラックリストから削除するユーザを指定します。設定範囲は 1～55 文字です。大文字、小文字を区別します。

説明

reset password-control blacklist コマンドはパスワード管理ブラックリストからユーザを削除します。

ログイン試行を超過したためにブラックリストに記録されたユーザが再度ログインできるようにするため、このコマンドを使用して、パスワード管理ブラックリストからユーザを削除します。

例

パスワード管理ブラックリストからユーザ **test** を削除します。

<Switch> reset password-control blacklist user-name test

```
Are you sure to delete the specified user in blacklist? [Y/N]:
```

関連コマンド

display password-control blacklist

7.1.20 reset password-control history-record

Syntax

reset password-control history-record [**super** [**role** *role-name*] | **user-name** *user-name*]

View

User view

定義済みユーザロール

network-admin

パラメータ

super: 指定された、あるいはすべての super パスワードの履歴の記録を削除します。

role *role name*: ユーザロールを指定します。設定範囲は 1～63 文字です。大文字、小文字を区別します。このオプションを指定しないと、すべての super パスワードの履歴の記録が削除されます。

user-name *user-name*: パスワード履歴を削除するユーザのユーザ名を指定します。設定範囲は 1～55 文字です。大文字、小文字を区別します。

説明

reset password-control history-record コマンドはパスワード履歴の記録を削除します。

パラメータを指定しない場合、すべてのローカルユーザのパスワード履歴の記録を削除します。

例

すべてのローカルユーザのパスワード履歴の記録を削除します。

<Switch> reset password-control history-record

```
Are you sure to delete all local user's history records? [Y/N]:y
```

関連コマンド

password-control history

目次

このセクションのページは **9-x-x** です。

8 章 公開鍵 8-1
8.1 公開鍵設定コマンド 8-1
8.1.1 display public-key local public 8-1
8.1.2 display public-key peer 8-4
8.1.3 peer-public-key end 8-6
8.1.4 public-key local create 8-7
8.1.5 public-key local destroy 8-10
8.1.6 public-key local export dsa 8-12
8.1.7 public-key local export rsa 8-14
8.1.8 public-key peer 8-17
8.1.9 public-key peer import sshkey 8-18

8章 公開鍵

8.1 公開鍵設定コマンド

8.1.1 display public-key local public

Syntax

display public-key local { **dsa** | **rsa** } **public** [**name** *key-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

dsa: DSA 鍵ペアタイプを指定します。

rsa: RSA 鍵ペアタイプを指定します。

name *key-name*: ローカル非対称鍵ペアの名前を指定します。設定範囲は 1～64 文字です。英字、数字、ハイフン（-）を含みます。名前を指定しない場合、指定されたタイプのすべてのローカル非対称鍵ペアの公開鍵を表示します。

説明

display public-key local public コマンドはローカル鍵ペアを表示します。

例

すべてのローカル RSA 鍵ペアの公開鍵を表示します。

<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:
   30819F300D06092A864886F70D010101050003818D0030818902818100DEBC46F217DDF11D
   426E7095AA45CD6BF1F87343D952569AC223A01365E0D8C91D49D347C143C5D8FAADA896AA
   1A827E580F2502F1926F52197230E1DE391A64015C43DD79DC4E9E171BAEA1DEB4C71DAED7
   9A6EDFD460D8945D27D39B7C9822D56AEA5B7C2CCFF1B6BC524AD498C3B87D4BD6EB36AF03
   92D8C6D940890BF4290203010001
```

すべてのローカル DSA 鍵ペアの公開鍵を表示します。

<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
   585DA7F42519718CC9B09EEF038184000281804191 2CE34D12BCD2157E7AB1C2F03B3EF395
   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
   7811C7DA33021500C773218C737EC8EE993B4F2DED30F48EDACE915F028181008226900 9E1
   4EC474BAF2932E69D3B1F18517AD9594184CCDFCEAE96EC4D5EF93133E84B47093C52B20CD
   35D02492B3959EC6499625BC4FA5082E22C5B374E16DD00132CE71B020217091AC717B6123
   91C76C1FB2E88317C1BD8171D41ECB83E210C03CC9B32E810561C21621C73D6DAAC028F4B1
   585DA7F42519718CC9B09EEF03818500028181 00A1E456C8DA2AD1BB83B1BDF2A1A6B5A6E8
   3642B460402445DA7E4036715F468F76655E114D460B7112F57143EE020AEF4A5BFAD07B74
   0FBCB1C64DA8A2BCE619283421445EEC77D3CF0D11866E9656AD6511F4926F8376967B0AB7
   15F9FB7B514BC1174155DD6E073B1FCB3A2749E6C5FEA81003E16729497D0EAD9105E3E76A
```

ローカル DSA 鍵ペア dsa1 の公開鍵を表示します。

<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
   7811C7DA33021500C773218C737EC8EE993B4F2DED30F48EDACE915F028181008226900 9E1
   4EC474BAF2932E69D3B1F18517AD9594184CCDFCEAE96EC4D5EF93133E84B47093C52B20CD
   35D02492B3959EC6499625BC4FA5082E22C5B374E16DD00132CE71B020217091AC717B6123
   91C76C1FB2E88317C1BD8171D41ECB83E210C03CC9B32E810561C21621C73D6DAAC028F4B1
   585DA7F42519718CC9B09EEF03818500028181 00A1E456C8DA2AD1BB83B1BDF2A1A6B5A6E8
   3642B460402445DA7E4036715F468F76655E114D460B7112F57143EE020AEF4A5BFAD07B74
   0FBCB1C64DA8A2BCE619283421445EEC77D3CF0D11866E9656AD6511F4926F8376967B0AB7
   15F9FB7B514BC1174155DD6E073B1FCB3A2749E6C5FEA81003E16729497D0EAD9105E3E76A
```

表 8-1 コマンド出力

フィールド	説明
Key name	ローカル鍵ペアの名前です。 鍵ペアを作成したとき、名前を指定しない場合、以下の鍵ペア名の後ろに（default）が追加されます。 以下に各鍵アルゴリズムのデフォルト鍵ペアを示します。 ● **hostkey**—デフォルトRSAホスト鍵ペア名です。 ● **serverkey**—デフォルトRSAサーバ鍵ペア名です。 ● **dsakey**—デフォルトDSAホスト鍵ペア名です。
Key type	オプションです。 ● **RSA** ● **DSA**
Time when key pair created	ローカル鍵ペアが作成された日時です。
Key code	公開鍵の文字列です。

関連コマンド

public-key local create

8.1.2 display public-key peer

Syntax

display public-key peer [**brief** | **name** *publickey-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

brief: すべてのピアのホスト公開鍵の概要を表示します。鍵タイプ、鍵モジュール、鍵名のみ表示します。

name *publickey-name*: ピアのホスト公開鍵の詳細情報を表示します。鍵コードが含まれます。*publickey-name* はピアのホスト公開鍵の名前を指定します。設定範囲は 1～64 文字です。大文字、小文字を区別します。

説明

display public-key peer コマンドはピアのホスト公開鍵の情報を表示します。

パラメータを指定しない場合、ローカル装置で設定したすべてのピアのホスト公開鍵の詳細情報を表示します。

ローカル装置のピアのホスト公開鍵を設定する場合、**public-key peer** コマンドあるいは **public-key peer import sshkey** コマンドを使用します。

例

ピアのホスト公開鍵 idrsa の詳細情報を表示します。

<Switch> display public-key peer name idrsa

```
==========================================
Key name: idrsa
Key type: RSA
Key modulus: 1024
Key code:
   30819F300D06092A864886F70D010101050003818D0030818902818100C5971581A78B5388
   B3C9063EC6B53D395A6704D9752B6F9B7B1F734EEB5DD509F0B050662C46FFB8D27F797E37
   918F6270C5793F1FC63638970A0E4D51A3CEF7CFF6E92BFAFD73F530E0BDE27056E81F2525
   6D0883836FD8E68031B2C272FE2EA75C87734A7B8F85B8EBEB3BD51CC26916AF3B3FDC32C3
   42C142D41BB4884FEB0203010001
```

表 8-2 コマンド出力

フィールド	説明
Key name	ピアのホスト公開鍵の名前です。
Key type	鍵タイプです。RSA、DSAがあります。
Key modulus	鍵モジュール長です。単位はビットです。
Key code	公開鍵の文字列です。

すべてのピアのホスト公開鍵の概要情報を表示します。

<Switch> display public-key peer brief

```
Type  Modulus  Name
----------------------------
RSA   1024    idrsa
DSA   1024    10.1.1.1
```

表 8-3 コマンド出力

フィールド	説明
Type	鍵タイプです。RSA、DSAがあります。
Modulus	鍵モジュール長です。単位はビットです。
Name	ピアの公開鍵の名前です。

関連コマンド

- **public-key peer**
- **public-key peer import sshkey**

8.1.3 peer-public-key end

Syntax

peer-public-key end

View

Public key view

定義済みユーザロール

network-admin

説明

peer-public-key end コマンドは public key view から system view に戻り、設定されたピアのホスト公開鍵を保存します。

ローカル装置でピアのホスト公開鍵を入力した後、このコマンドを使用し、public key view から system view に戻り、ホスト公開鍵を保存します。

システムは公開鍵を保存する前に確認します。鍵が正しい形式でない場合、システムは鍵を廃棄し、エラーメッセージを表示します。鍵が正常である場合、鍵を保存します。鍵はたとえば、**display public-key local public** コマンドで表示することができます。

例

public key view から system view に戻り、設定されたピアのホスト公開鍵を保存します。

<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]30819F300D06092A864886F70D010101050003818D003
0818902818100C0EC8014F82515F6335A0A

[Switch-pkey-public-key-key1]EF8F999C01EC94E5760A079BD73E4F4D97F3500EDB3
08C29481B77E719D1643135877E13B1C531B4

[Switch-pkey-public-key-key1]FF1877A5E2E7B1FA4710DB0744F66F6600EEFE166F1B
854E2371D5B952ADF6B80EB5F52698FCF3D6

[Switch-pkey-public-key-key1]1F0C2EAAD9813ECB16C5C7DC09812D4EE3E9A0B074
276FFD4AF2050BD4A9B1DDE675AC30CB020301

[Switch-pkey-public-key-key1]0001

[Switch-pkey-public-key-key1] peer-public-key end

[Switch]

関連コマンド

- **display public-key local public**
- **display public-key peer**
- **public-key peer**

8.1.4 public-key local create

Syntax

public-key local create { **dsa** | **rsa** } [**name** *key-name*]

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

dsa: DSA 鍵ペアを作成します。

rsa: RSA 鍵ペアを作成します。

name *key-name*: ローカル非対称鍵ペアの名前を割り当てます。設定範囲は 1～64 文字です。英字、数字、ハイフン（-）を含みます。名前を割り当てない場合、デフォルト名を適用します。

表 8-4 デフォルトのローカル鍵ペア名

タイプ	デフォルト名
RSA	• **ホスト鍵ペア**：hostkey • **サーバ鍵ペア**：serverkey
DSA	dsakey

説明

public-key local create コマンドはローカル非対称鍵ペアを作成します。

鍵アルゴリズムはセキュリティアプリケーションで要求されたアルゴリズムと同一にする必要があります。

鍵の長さは適切に設定する必要があります。鍵の長さが長いと高いセキュリティとなりますが、鍵を作成する時間も長くなります。

鍵の長さは表 8-5 に示すように非対称鍵アルゴリズムの異なるタイプの比較を示します。

鍵ペアの名前を割り当てない場合、デフォルトの名前を割り当て、鍵ペアを default としてマーキングします。デフォルトの名前を別の鍵ペアに割り当てることができますが、鍵ペアを default としてマーキングしません。鍵ペアの名前は、同じ鍵アルゴリズムを使用する鍵ペア間で一意にする必要がありますが、異なる鍵アルゴリズムを使用する鍵ペアでは同じ名前を使用することができます。もし名前が重複している場合、存在する鍵ペアに上書きしていいか確認メッセージが表示されます。

鍵ペアは自動で保存され、装置の再起動が行われても削除されません。

表 8-5 非対称鍵アルゴリズムの異なるタイプの比較

タイプ	鍵ペア数	モジュール長	推奨
RSA	• 鍵ペアの名前を指定する場合、ホスト鍵ペアを作成します。 • 鍵ペアの名前を指定しない場合、1つのサーバ鍵ペアと1つのホスト鍵ペアを作成し、デフォルト名を使用します。	設定範囲は512～4096ビットです。 デフォルトは1024ビットです。	少なくとも768ビットにしてください。
DSA	1つのホスト鍵ペアを作成します。	設定範囲は512～2048ビットです。 デフォルトは1024ビットです。	少なくとも768ビットにしてください。

🕮 メモ：

・SSH 1.5 のみが RSA サーバ鍵ペアを使用します。・

例

デフォルト名のローカル RSA 鍵ペアを作成します。

<Switch> system-view

[Switch] public-key local create rsa

```
The range of public key modulus is (512 ~ 4096).
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.
```

デフォルト名のローカル DSA 鍵ペアを作成します。

<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.
```

名前が rsa1 のローカル RSA 鍵ペアを作成します。

<Switch> system-view

[Switch] public-key local create rsa name rsa1

```
The range of public key modulus is (512 ~ 4096).
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.
```

名前が dsa1 のローカル DSA 鍵ペアを作成します。

<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.
```

関連コマンド

- **display public-key local public**
- **public-key local destroy**

8.1.5 public-key local destroy

Syntax

public-key local destroy { **dsa** | **rsa** } [**name** *key-name*]

View

System view

定義済みユーザロール

network-admin

パラメータ

dsa: DSA タイプを指定します。

rsa: RSA タイプを指定します。

name *key-name*: ローカル非対称鍵ペアの名前を指定します。設定範囲は 1～64 文字です。英字、数字、ハイフン（-）を含みます。名前を指定しない場合、デフォルト名のローカル鍵ペアの指定されたタイプを削除します。

説明

public-key local destroy コマンドはローカル鍵ペアを削除します。

以下の状況が発生した場合、鍵を正常に保つため、ローカル非対称鍵ペアを削除し、新しいペアを生成する必要があります。

- 不正侵入が発生した場合。
- 装置の記憶媒体を交換した場合。
- ローカル証明書が期限切れとなった場合。ローカル証明書の詳細は、オペレーションマニュアルのセクション 9 *セキュリティ*を参照してください。

例

デフォルト名のローカル RSA 鍵ペアを削除します。

<Switch> system-view

[Switch] public-key local destroy rsa

```
Confirm to destroy the key pair? [Y/N]:y
```

デフォルト名のローカル DSA 鍵ペアを削除します。

<Switch> system-view

[Switch] public-key local destroy dsa

```
Confirm to destroy the key pair? [Y/N] :y
```

名前が rsa1 のローカル RSA 鍵ペアを削除します。

<Switch> system-view

[Switch] public-key local destroy rsa name rsa1

```
Confirm to destroy the key pair? [Y/N]:y
```

名前が dsa1 のローカル DSA 鍵ペアを削除します。

<Switch> system-view

[Switch] public-key local destroy dsa name dsa1

```
Confirm to destroy the key pair? [Y/N] :y
```

関連コマンド

public-key local create

8.1.6 public-key local export dsa

Syntax

public-key local export dsa [**name** *key-name*] { **openssh** | **ssh2** } [*filename*]

View

System view

定義済みユーザロール

network-admin

パラメータ

name *key-name*: ローカル DSA 鍵ペアの名前を指定します。設定範囲は 1～64 文字です。英字、数字、ハイフン（-）を含みます。指定しない場合、デフォルト名のローカル DSA 鍵ペアのホスト公開鍵を表示あるいはエクスポートします。

openssh: OpenSSH の形式を使用します。

ssh2: SSH2.0 の形式を使用します。

filename: 保存するローカルホスト公開鍵の名前を指定します。設定範囲は 1～128 文字です。大文字、小文字を区別しません。”./”、”../” を除いて指定します。名前は、ドット（.）、hostkey、serverkey、dsakey、ecdsakey を使用することができません。また先頭をスラッシュにすることができません。ファイル名の詳細は、オペレーションマニュアルのセクション 1 *はじめに*”*ファイルシステム管理*”を参照してください。

説明

public-key local export dsa コマンドは指定した形式のローカル DSA ホスト公開鍵を表示あるいはファイルにエクスポートします。

filename が指定されている場合、ローカル DSA ホスト公開鍵をエクスポートします。指定されていない場合、ローカル DSA ホスト公開鍵を表示します。

ローカル DSA ホスト公開鍵をピアの装置に分配する前に、コマンドを使用して表示あるいはエクスポートすることができます。

1) ローカルホスト公開鍵を以下のいずれかの方法でファイルに保存します。
   - **public-key local export dsa** [**name** *key-name*] { **openssh** | **ssh2** }コマンドを使用し、指定した形式のローカルホスト公開鍵を表示します。内容をコピーし、ファイルにペーストします。
   - **public-key local export dsa** [**name** *key-name*] { **openssh** | **ssh2** } *filename* コマンドを使用し、ファイルにローカルホスト公開鍵をエクスポートします。ホスト公開鍵をフォルダ pkey あるいはサブフォルダにエクスポートすることはできません。
2) バイナリモードの FTP あるいは TFTP などを使用してファイルのコピーをピアの装置に転送します。FTP、TFTP の詳細は、オペレーションマニュアルのセクション 1 *はじめに* “*FTP*”、“*TFTP*”を参照してください。

3) ピアの装置でファイルから **public-key peer import sshkey** コマンドを使用してホスト公開鍵をインポートします。

SSH2.0 と OpenSSH は異なる公開鍵形式です。ホスト公開鍵をインポートする装置でサポートされる形式に従って適切に選択してください。

例

OpenSSH 形式のデフォルト名のローカル DSA 鍵ペアのホスト公開鍵をファイル key.pub にエクスポートします。

<Switch> system-view

[Switch] public-key local export dsa openssh key.pub

SSH2.0 形式のデフォルト名のローカル DSA 鍵ペアのホスト公開鍵を表示します。

<Switch> system-view

[Switch] public-key local export dsa ssh2

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "dsa-key-2011/05/12"
AAAAB3NzaC1kc3MAAACBANdXJixFhMRMIR8YvZbl8GHE8KQj9/5ra4WzTO9yzhSg06UiL+CM7OZb5
sJlhUiJ3B7b0T7IsnTan3W6Jsy5h3I2Anh+kiuoRCHyLDyJy5sG/WD+AZQd3Xf+axKJPadu68HRKN
l/BnjXcitTQchQbzWCFLFqL6xLNolQOHgRx9ozAAAAFQDHcyGMc37I7pk7Ty3tMPSO2s6RXwAAAIE
AgiaQCeFOxHS68pMuadOx8YUXrZWUGEzN/OrpbsTV75MTPoS0cJPFKyDNNdAkkrOVnsZJliW8T6UI
LiLFs3ThbdABMs5xsCAhcJGscXthI5HHbB+y6IMXwb2BcdQey4PiEMA8ybMugQVhwhYhxz1tqsAo9
LFYXaf0JRlxjMmwnu8AAACAQZEs400SvNIVfnqxwvA7PvOVEA89tKni/f6GDBvWY9Z2Q499pAqUBt
YcqQea8T4zBInxx2eF3lLaZJrIvAS205zXxSzQoU9190kakdMdasIjQLWYGyepFc3sTwmIflQeweU
wLVAPaOesKaCERjxg+e4maYWlAvySGT4c9NJlxLo=
---- END SSH2 PUBLIC KEY ----
```

OpenSSH 形式のデフォルト名のローカル DSA 鍵ペアのホスト公開鍵を表示します。

<Switch> system-view

[Switch] public-key local export dsa openssh

```
ssh-dss
AAAAB3NzaC1kc3MAAACBANdXJixFhMRMIR8YvZbl8GHE8KQj9/5ra4WzTO9yzhSg06UiL+CM7OZb5
sJlhUiJ3B7b0T7IsnTan3W6Jsy5h3I2Anh+kiuoRCHyLDyJy5sG/WD+AZQd3Xf+axKJPadu68HRKN
l/BnjXcitTQchQbzWCFLFqL6xLNolQOHgRx9ozAAAAFQDHcyGMc37I7pk7Ty3tMPSO2s6RXwAAAIE
AgiaQCeFOxHS68pMuadOx8YUXrZWUGEzN/OrpbsTV75MTPoS0cJPFKyDNNdAkkrOVnsZJliW8T6UI
LiLFs3ThbdABMs5xsCAhcJGscXthI5HHbB+y6IMXwb2BcdQey4PiEMA8ybMugQVhwhYhxz1tqsAo9
LFYXaf0JRlxjMmwnu8AAACAQZEs400SvNIVfnqxwvA7PvOVEA89tKni/f6GDBvWY9Z2Q499pAqUBt
YcqQea8T4zBInxx2eF3lLaZJrIvAS205zXxSzQoU9190kakdMdasIjQLWYGyepFc3sTwmIflQeweU
wLVAPaOesKaCERjxg+e4maYWlAvySGT4c9NJlxLo= dsa-key
```

OpenSSH 形式のローカル DSA 鍵ペア dsa1 のホスト公開鍵をファイル dsa1.pub にエクスポートします。

<Switch> system-view

[Switch] public-key local export dsa name dsa1 openssh dsa1.pub

SSH2.0 形式のローカル DSA 鍵ペア dsa1 のホスト公開鍵を表示します。

<Switch> system-view

[Switch] public-key local export dsa name dsa1 ssh2

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "dsa-key-2011/05/12"
AAAAB3NzaC1kc3MAAACBANdXJixFhMRMIR8YvZbl8GHE8KQj9/5ra4WzTO9yzhSg06UiL+CM7OZb5
sJlhUiJ3B7b0T7IsnTan3W6Jsy5h3I2Anh+kiuoRCHyLDyJy5sG/WD+AZQd3Xf+axKJPadu68HRKN
l/BnjXcitTQchQbzWCFLFqL6xLNolQOHgRx9ozAAAAFQDHcyGMc37I7pk7Ty3tMPSO2s6RXwAAAIE
AgiaQCeFOxHS68pMuadOx8YUXrZWUGEzN/OrpbsTV75MTPoS0cJPFKyDNNdAkkrOVnsZJliW8T6UI
LiLFs3ThbdABMs5xsCAhcJGscXthI5HHbB+y6IMXwb2BcdQey4PiEMA8ybMugQVhwhYhxz1tqsAo9
LFYXaf0JRlxjMmwnu8AAACBAKHkVsjaKtG7g7G98qGmtaboNkK0YEAkRdp+QDZxX0aPdmVeEU1GC3
ES9XFD7gIK70pb+tB7dA+8scZNqKK85hkoNCFEXux3088NEYZullatZRH0km+DdpZ7CrcV+ft7UUv
BF0FV3W4HOx/LOidJ5sX+qBAD4WcpSX0OrZEF4+dq
---- END SSH2 PUBLIC KEY ----
```

OpenSSH 形式のローカル DSA 鍵ペア dsa1 のホスト公開鍵を表示します。

<Switch> system-view

[Switch] public-key local export dsa name dsa1 openssh

```
ssh-dss
AAAAB3NzaC1kc3MAAACBANdXJixFhMRMIR8YvZbl8GHE8KQj9/5ra4WzTO9yzhSg06UiL+CM7OZb5
sJlhUiJ3B7b0T7IsnTan3W6Jsy5h3I2Anh+kiuoRCHyLDyJy5sG/WD+AZQd3Xf+axKJPadu68HRKN
l/BnjXcitTQchQbzWCFLFqL6xLNolQOHgRx9ozAAAAFQDHcyGMc37I7pk7Ty3tMPSO2s6RXwAAAIE
AgiaQCeFOxHS68pMuadOx8YUXrZWUGEzN/OrpbsTV75MTPoS0cJPFKyDNNdAkkrOVnsZJliW8T6UI
LiLFs3ThbdABMs5xsCAhcJGscXthI5HHbB+y6IMXwb2BcdQey4PiEMA8ybMugQVhwhYhxz1tqsAo9
LFYXaf0JRlxjMmwnu8AAACBAKHkVsjaKtG7g7G98qGmtaboNkK0YEAkRdp+QDZxX0aPdmVeEU1GC3
ES9XFD7gIK70pb+tB7dA+8scZNqKK85hkoNCFEXux3088NEYZullatZRH0km+DdpZ7CrcV+ft7UUv
BF0FV3W4HOx/LOidJ5sX+qBAD4WcpSX0OrZEF4+dq dsa-key
```

関連コマンド

- **public-key local create**
- **public-key peer import sshkey**

8.1.7 public-key local export rsa

Syntax

public-key local export rsa [**name** *key-name*] { **openssh** | **ssh1** | **ssh2** } [*filename*]

View

System view

定義済みユーザロール

network-admin

パラメータ

name *key-name*: ローカル RSA 鍵ペアの名前を指定します。設定範囲は 1～64 文字です。英字、数字、ハイフン（-）を含みます。名前を指定しない場合、デフォルト名のローカル鍵 RSA ペアのホスト公開鍵を表示あるいはエクスポートします。

openssh: OpenSSH の形式を使用します。

ssh1: SSH1.5 の形式を使用します。

ssh2: SSH2.0 の形式を使用します。

filename: 保存するローカルホスト公開鍵の名前を指定します。設定範囲は 1～128 文字です。大文字、小文字を区別しません。”./”、”../”を除いて指定します。名前は、ドット（.）、hostkey、serverkey、dsakey、ecdsakey を使用することができません。また先頭をスラッシュにすることができません。ファイル名の詳細は、オペレーションマニュアルのセクション 1 *はじめに*”*ファイルシステム管理*”を参照してください。

説明

public-key local export rsa コマンドは指定した形式のローカル RSA ホスト公開鍵を表示あるいはファイルにエクスポートします。

filename が指定されている場合、ローカル RSA ホスト公開鍵をエクスポートします。指定されていない場合、ローカル RSA ホスト公開鍵を表示します。

ローカル DSA ホスト公開鍵をピアの装置に分配する前に、コマンドを使用して表示あるいはエクスポートすることができます。

1) ローカルホスト公開鍵を以下のいずれかの方法でファイルに保存します。
   - **public-key local export rsa** [**name** *key-name*] { **openssh** | **ssh2** }コマンドを使用し、指定した形式のローカルホスト公開鍵を表示します。内容をコピーし、ファイルにペーストします。
   - **public-key local export rsa** [**name** *key-name*] { **openssh** | **ssh2** } *filename* コマンドを使用し、ファイルにローカルホスト公開鍵をエクスポートします。ホスト公開鍵をフォルダ pkey あるいはサブフォルダにエクスポートすることはできません。
2) バイナリモードの FTP あるいは TFTP などを使用してファイルのコピーをピアの装置に転送します。FTP、TFTP の詳細は、オペレーションマニュアルのセクション 1 *はじめに* “*FTP*”、“*TFTP*”を参照してください。
3) ピアの装置でファイルから **public-key peer import sshkey** コマンドを使用してホスト公開鍵をインポートします。

SSH1.5、SSH2.0、OpenSSH は異なる公開鍵形式です。ホスト公開鍵をインポートする装置でサポートされる形式に従って適切に選択してください。

例

OpenSSH 形式のデフォルト名のローカル RSA 鍵ペアのホスト公開鍵をファイル key.pub にエクスポートします。

<Switch> system-view

[Switch] public-key local export rsa openssh key.pub

SSH2.0 形式のデフォルト名のローカル RSA 鍵ペアのホスト公開鍵を表示します。

<Switch> system-view

[Switch] public-key local export rsa ssh2

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "rsa-key-2011/05/12"
AAAAB3NzaC1yc2EAAAADAQABAAAAgQDapKr+/gTCyWZyabuCJuJjMeMPQaj/kixzOCCAl+hDMmEGM
rSfddq/bYcbgM7Buit1AgB3x0dFyTPi85DcCznTW4goPXAKFjuzCbGfj4chakSr+/aj1k3rM+XOvy
vPJilneKJqhPT0xdv4tlas+mLNloY0dImbwS2kwE71rgg1CQ==
---- END SSH2 PUBLIC KEY ----
```

OpenSSH 形式のデフォルト名のローカル RSA 鍵ペアのホスト公開鍵を表示します。

<Switch> system-view

[Switch] public-key local export rsa openssh

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAAAgQDapKr+/gTCyWZyabuCJuJjMeMPQaj/kixzOCCAl+hDMmEGM
rSfddq/bYcbgM7Buit1AgB3x0dFyTPi85DcCznTW4goPXAKFjuzCbGfj4chakSr+/aj1k3rM+XOvy
vPJilneKJqhPT0xdv4tlas+mLNloY0dImbwS2kwE71rgg1CQ== rsa-key
```

OpenSSH 形式のローカル RSA 鍵ペア rsa1 のホスト公開鍵をファイル rsa1.pub にエクスポートします。

<Switch> system-view

[Switch] public-key local export rsa name rsa1 openssh rsa1.pub

SSH2.0 形式のローカル RSA 鍵ペア rsa1 のホスト公開鍵を表示します。

<Switch> system-view

[Switch] public-key local export rsa name rsa1 ssh2

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "rsa-key-2011/05/12"
AAAAB3NzaC1yc2EAAAADAQABAAAAgQDevEbyF93xHUJucJWqRc1r8fhzQ9lSVprCI6ATZeDYyR1J0
0fBQ8XY+q2olqoagn5YDyUC8ZJvUhlyMOHeORpkAVxD3XncTp4XG66h3rTHHa7Xmm7f1GDYlF0n05
t8mCLVaupbfCzP8ba8UkrUmMO4fUvW6zavA5LYxtlAiQv0KQ==
---- END SSH2 PUBLIC KEY ----
```

OpenSSH 形式のローカル RSA 鍵ペア rsa1 のホスト公開鍵を表示します。

<Switch> system-view

[Switch] public-key local export rsa name rsa1 openssh

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAAAgQDevEbyF93xHUJucJWqRc1r8fhzQ9lSVprCI6ATZeDYyR1J0
0fBQ8XY+q2olqoagn5YDyUC8ZJvUhlyMOHeORpkAVxD3XncTp4XG66h3rTHHa7Xmm7f1GDYlF0n05
t8mCLVaupbfCzP8ba8UkrUmMO4fUvW6zavA5LYxtlAiQv0KQ== rsa-key
```

関連コマンド

- **public-key local create**
- **public-key peer import sshkey**

8.1.8 public-key peer

Syntax

public-key peer *keyname*

undo public-key peer *keyname*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

keyname: ピアの公開鍵の名前を指定します。設定範囲は 1～64 文字です。大文字、小文字を区別します。

説明

public-key peer コマンドはピアの公開鍵の名前を指定し、public key view に移行します。

undo public-key peer コマンドはピアの公開鍵を削除します。

public key view に移行するため、コマンドを実行した後、公開鍵を入力します。半角スペースと改行は入力できますが、保存されません。

ローカル装置でピアの公開鍵を手動で指定するため、最初に 16 進数のピアの公開鍵を取得し、ローカル装置で以下の処理を行ってください。

1) public key view に移行するため、**public-key peer** コマンドを実行します。
2) 公開鍵を入力します。
3) **peer-public-key end** コマンドを実行し、公開鍵を保存し、system view に戻ります。

public key view で正しい形式の公開鍵を入力してください。ピアの装置が QX シリーズである場合、公開鍵を記録するため、**display public-key local public** コマンドを使用することを推奨します。

例

ピアの公開鍵 key1 を指定し、public key view に移行します。

<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]

関連コマンド

- **display public-key local public**
- **display public-key peer**
- **peer-public-key end**

8.1.9 public-key peer import sshkey

Syntax

public-key peer *keyname* **import sshkey** *filename*

undo public-key peer *keyname*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

keyname: ピアの公開鍵の名前を指定します。設定範囲は 1～64 文字です。大文字、小文字を区別します。

filename: 保存するピアの公開鍵の名前を指定します。設定範囲は 1～128 文字です。大文字、小文字を区別しません。"./"、"../"を除いて指定します。名前は、ドット(.)、hostkey、serverkey、dsakey、ecdsakey を使用することができません。また先頭をスラッシュにすることができません。ファイル名の詳細は、オペレーションマニュアルのセクション 1 *はじめに*" *ファイルシステム管理*"を参照してください。

説明

public-key peer import sshkey コマンドは公開鍵ファイルからピアのホスト公開鍵をインポートします。

undo public-key peer コマンドは指定したピアのホスト公開鍵を削除します。

このコマンドを設定した後、システムは自動的に PKCS（Public Key Cryptography Standards）形式にホスト公開鍵を変換し、保存します。

ピアのホスト公開鍵をインポートする前に、バイナリモードで FTP または TFTP を使用してピアの装置から公開鍵のファイルのコピーの取得を行ってください。

装置は SSH1.5、SSH2.0、OpenSSH の形式の公開鍵をインポートすることができます。

例

公開鍵ファイル key.pub からピアのホスト公開鍵 key2 をインポートします。

<Switch> system-view

[Switch] public-key peer key2 import sshkey key.pub

関連コマンド

- **display public-key peer**
- **public-key local export dsa**
- **public-key local export rsa**

目次

このセクションのページは **9-x-x** です。

9 章 PKI..... 9-1

9章 PKI

PKIの設定に関するコンフィグについては、別紙の共通マニュアル“*QX シリーズ Ethernet スイッチ Web 認証コマンドマニュアル*（V7）”の“*PKI*”を参照してください。

目次

このセクションのページは **9-x-x** です。

10 章 SSH 10-1
10.1 SSH サーバ設定コマンド 10-1
10.1.1 display ssh server 10-1
10.1.2 display ssh user-information 10-3
10.1.3 free ssh 10-4
10.1.4 scp server enable 10-6
10.1.5 sftp server enable 10-6
10.1.6 sftp server idle-timeout 10-7
10.1.7 ssh server acl 10-8
10.1.8 ssh server authentication-retries 10-9
10.1.9 ssh server authentication-timeout 10-10
10.1.10 ssh server compatible-ssh1x enable 10-11
10.1.11 ssh server dscp 10-12
10.1.12 ssh server enable 10-12
10.1.13 ssh server ipv6 acl 10-13
10.1.14 ssh server ipv6 dscp 10-14
10.1.15 ssh server rekey-interval 10-15
10.1.16 ssh user 10-16
10.2 SSH クライアント設定コマンド 10-19
10.2.1 bye 10-19
10.2.2 cd 10-20
10.2.3 cdup 10-20
10.2.4 delete 10-21
10.2.5 dir 10-22
10.2.6 display sftp client source 10-23
10.2.7 display ssh client source 10-23
10.2.8 exit 10-24
10.2.9 get 10-25
10.2.10 help 10-25
10.2.11 ls 10-26
10.2.12 mkdir 10-27
10.2.13 put 10-28
10.2.14 pwd 10-29
10.2.15 quit 10-29
10.2.16 remove 10-30
10.2.17 rename 10-30

10.2.18 rmdir 10-31
10.2.19 scp 10-31
10.2.20 scp ipv6 10-35
10.2.21 sftp 10-38
10.2.22 sftp client ipv6 source 10-40
10.2.23 sftp client source 10-41
10.2.24 sftp ipv6 10-42
10.2.25 ssh client ipv6 source 10-45
10.2.26 ssh client source 10-46
10.2.27 ssh2 10-47
10.2.28 ssh2 ipv6 10-49

10章 SSH

10.1 SSHサーバ設定コマンド

10.1.1 display ssh server

Syntax

display ssh server { **session** | **status** }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

session: SSH サーバのセッションを表示します。

status: SSH サーバの状態を表示します。

説明

display ssh server コマンドは SSH サーバで SSH サーバのセッションあるいは状態を表示します。

例

SSH サーバの状態を表示します。

<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
```

表 10-1 コマンド出力

フィールド	説明
Stelnet server	Stelnetサーバ機能が有効かどうかを示します。
SSH version	SSHプロトコルのバージョンです。 SSH1をサポートしている場合、プロトコルバージョンは1.99です。その他の場合、プロトコルバージョンは2です。
SSH authentication-timeout	認証タイムアウトタイマです。
SSH server key generating interval	SSHサーバ鍵ペアのアップデート間隔です。
SSH authentication retries	SSHユーザの認証の最大試行回数です。
SFTP server	SFTPサーバ機能が有効かどうかを示します。
SFTP server Idle-Timeout	SFTP接続アイドルタイムアウトタイマです。
Netconf server	NETCONF over SSHが有効かどうかを示します。 NETCONF over SSHはサポートしていません。
SCP server	SCPサーバ機能が有効かどうかを示します。 SCPサーバ機能はサポートしていません。
SSH Server PKI domain name	SSHサーバで指定したPKIドメインの名前です。

SSH サーバのセッションを表示します。

<Switch> display ssh server session

```
UserPid   SessID Ver   Encrypt    State        Retries  Serv     Username
 184       0     2.0   aes128-cbc Established   1       Stelnet  abc@123
```

表 10-2 コマンド出力

フィールド	説明
UserPid	ユーザプロセスIDです。
SessID	セッションIDです。
Ver	SSHサーバのプロトコルバージョンです。
Encrypt	SSHサーバで使用される暗号化アルゴリズムです。

フィールド	説明
State	セッション状態です。 ● **Init**–初期化状態です。 ● **Ver-exchange**–バージョンのネゴシエーション状態です。 ● **Keys-exchange**–鍵交換状態です。 ● **Auth-request**–認証要求状態です。 ● **Serv-request**–セッションサービス要求状態です。 ● **Established**–セッションが確立されています。 ● **Disconnected**–セッションが切断されています。
Retries	認証に失敗した数です。
Serv	サービスタイプです。 ● SCPです。 ● SFTPです。 ● Stelnetです。 ● NETCONFです。
Username	サーバにログインしているユーザ名です。

10.1.2 display ssh user-information

Syntax

display ssh user-information [*username*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

username: SSH ユーザ名を指定します。設定範囲は 1～80 文字です。大文字、小文字を区別します。指定しない場合、すべての SSH ユーザの情報を表示します。

説明

display ssh user-information コマンドは SSH サーバの SSH ユーザの情報を表示します。

このコマンドは、SSH サーバ上で **ssh user** コマンドを使用して設定された SSH ユーザのみの情報を表示します。

例

すべての SSH ユーザの情報を表示します。

<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
```

表 10-3 コマンド出力

フィールド	説明
Total ssh users	SSHユーザの総数です。
Authentication-type	認証方式です。 ● パスワード認証です。 ● 公開鍵認証です。 ● パスワード-公開鍵認証です。 ● 他の認証です。
User-public-key-name	ユーザの公開鍵名です。パスワード認証が使用される場合、表示されません。
Service-type	サービスタイプです。 ● Stelnetです。 ● SFTPです。 ● SCPです。 ● NETCONFです。 SSHユーザで複数のサービスタイプが有効である場合、垂直バー（|）で区切られます。

関連コマンド

ssh user

10.1.3 free ssh

Syntax

free ssh { **user-ip** { *ip-address* | **ipv6** *ipv6-address* } [**port** *port-number*] | **user-pid** *pid-number* | **username** *username* }

View

User view

定義済みユーザロール

network-admin

パラメータ

user-ip: 接続を解除する SSH セッションのユーザ IP アドレスを指定します。

ip-address: 接続を解除する SSH セッションのユーザ IPv4 アドレスを指定します。

ipv6 *ipv6-address:* 接続を解除する SSH セッションのユーザ IPv6 アドレスを指定します。

port *port-number*: 接続を解除する SSH セッションの送信元ポートを指定します。設定範囲は 1～65535 です。送信元ポートを指定しない場合、指定された IP アドレスを使用してすべての SSH セッションを切断します。

user-pid *pid-number*: 接続を解除する SSH セッションのユーザプロセス ID を指定します。設定範囲は 1~2147483647 です。SSH セッションのユーザプロセス ID を表示するには、**display ssh server session** コマンドを使用します。

username *username*: 接続を解除する SSH セッションのユーザ名を指定します。SSH セッションのユーザ名を表示するには、**display ssh server session** コマンドを使用します。

説明

free ssh コマンドは SSH セッションを切断します。

例

ユーザ IPv4 アドレス 192.168.15.45 の SSH セッションを切断します。

<Switch> free ssh user-ip 192.168.15.45

```
Releasing SSH connection. Continue? [Y/N]:y
```

ユーザ IPv6 アドレス 2000 :: 11 を持つ SSH セッションを切断します。

<Switch> free ssh user-ip ipv6 2000::11

```
Releasing SSH connection. Continue? [Y/N]:y
```

ユーザプロセス ID417 の SSH セッションを切断します。

<Switch> free ssh user-pid 417

```
Releasing SSH connection. Continue? [Y/N]:y
```

ユーザ名 **sshuser** で SSH セッションを切断します。

<Switch> free ssh username sshuser

```
Releasing SSH connection. Continue? [Y/N]:y
```

関連コマンド

display ssh server session

10.1.4 scp server enable

Syntax

scp server enable

undo scp server enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

scp server enable コマンドは SCP サーバを有効にします。

undo scp server enable コマンドは SCP サーバを無効にします。

例

SCP サーバを有効にします。

<Switch> system-view

[Switch] scp server enable

関連コマンド

display ssh server

10.1.5 sftp server enable

Syntax

sftp server enable

undo sftp server enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

sftp server enable コマンドは SFTP サーバ機能を有効にします。

undo sftp server enable コマンドは SFTP サーバ機能を無効にします。

例

SFTP サーバ機能を有効にします。

<Switch> system-view

[Switch] sftp server enable

関連コマンド

display ssh server

10.1.6 sftp server idle-timeout

Syntax

sftp server idle-timeout *time-out-value*

undo sftp server idle-timeout

デフォルト

10 分

View

System view

定義済みユーザロール

network-admin

パラメータ

time-out-value: タイムアウトタイマを指定します。設定範囲は 1～35791 分です。

説明

sftp server idle-timeout コマンドは SFTP サーバの SFTP ユーザ接続のアイドルタイムアウトタイマを設定します。

undo sftp server idle-timeout コマンドはデフォルトに戻します。

アイドルタイムアウトタイマが終了したとき、SFTP 接続がアイドルである場合、システムは自動的に接続を切断します。多くの SFTP 接続が確立されている場合、接続リソースを即座に開放できるように、タイマを小さい値に設定することができます。

例

SFTP ユーザ接続のアイドルタイムアウトタイマを 500 分に設定します。

<Switch> system-view

[Switch] sftp server idle-timeout 500

関連コマンド

display ssh server

10.1.7 ssh server acl

Syntax

ssh server acl { *advanced-acl-number* | *basic-acl-number* | **mac** *mac-acl-number* }

undo ssh server acl

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

advanced-acl-number: 拡張 IPv4 ACL を指定します。設定範囲は 3000～3999 です。

basic-acl-number: 標準 IPv4 ACL を指定します。設定範囲は 2000～2999 です。

mac *mac-acl-number:* L2 ACL を指定します。設定範囲は 4000～4999 です。

説明

ssh server acl コマンドは IPv4 SSH サーバへのアクセスを制御します。

undo ssh server acl コマンドはデフォルトに戻します。

ACL を使用して IPv4 SSH クライアントの要求パケットをフィルタするために使用します。

- ACL ルールが設定されている場合、ACL の permit 条件に一致する IPv4 SSH クライアントの要求パケットのみがサーバにアクセスすることができます。

- ACL ルールが存在しない、あるいは ACL に条件がない場合、すべての IPv4 SSH クライアントがサーバにアクセスすることができます。

この設定は、設定した後に SSH 接続を行った要求パケットから有効になります。

このコマンドを複数実行した場合、最後に行われた設定が適用されます。

例

IPv4 SSH クライアント 1.1.1.1 のみサーバにアクセスできるように ACL 2001 を設定します。

<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

関連コマンド

display ssh server

10.1.8 ssh server authentication-retries

Syntax

ssh server authentication-retries *retries*

undo ssh server authentication-retries

デフォルト

3

View

System view

定義済みユーザロール

network-admin

パラメータ

retries: SSH ユーザの認証を試行する最大数を指定します。設定範囲は 1～5 です。

説明

ssh server authentication-retries コマンドは SSH ユーザの認証を試行する最大数を指定します。

undo ssh server authentication-retries コマンドはデフォルトに戻します。

偽のユーザ名とパスワードの攻撃を防ぐため、最大数を設定することができます。

- 認証が使用されたとき、公開鍵とパスワード認証の合計の試行回数が設定した上限を超えることができません。
- 認証方式がパスワード-公開鍵である場合、SSH ユーザを認証するため、最初にサーバは公開鍵認証を使用し、ユーザパスワード認証を使用します。プロセスは 1 つの認証を行うものとして扱います。

この設定はログインユーザには適用されません。新しい SSH ユーザのみ適用されます。

例

SSH ユーザの認証を試行する最大数を 4 に設定します。

<Switch> system-view

[Switch] ssh server authentication-retries 4

関連コマンド

display ssh server

10.1.9 ssh server authentication-timeout

Syntax

ssh server authentication-timeout *time-out-value*

undo ssh server authentication-timeout

デフォルト

60 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

time-out-value: 認証タイムアウトタイマを指定します。設定範囲は 1～120 秒です。

説明

ssh server authentication-timeout コマンドは SSH サーバで SSH ユーザ認証のタイムアウトタイマを設定します。

undo ssh server authentication-timeout コマンドはデフォルトに戻します。

タイムアウトタイマが終了したとき、ユーザが認証を終了しない場合、接続は確立することができません。

タイムアウトタイマの値を小さくすることで、認証が中断される間に、偽の TCP 接続による占有を防ぐことができます。

例

SSH ユーザ認証のタイムアウトタイマを 10 秒に設定します。

<Switch> system-view

[Switch] ssh server authentication-timeout 10

関連コマンド

display ssh server

10.1.10 ssh server compatible-ssh1x enable

Syntax

ssh server compatible-ssh1x enable

undo ssh server compatible-ssh1x

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

network-operator

説明

ssh server compatible-ssh1x enable コマンドは SSH1 クライアントをサポートする SSH サーバを有効にします。

undo ssh server compatible-ssh1x コマンドは SSH サーバで SSH1 クライアントのサポートを無効にします。

この設定はログインユーザには適用されません。次回ログインしたユーザのみ適用します。

例

SSH1 クライアントをサポートする SSH サーバを有効にします。

<Switch> system-view

[Switch] ssh server compatible-ssh1x enable

関連コマンド

display ssh server

10.1.11 ssh server dscp

Syntax

ssh server dscp *dscp-value*

undo ssh server dscp

デフォルト

48

View

System view

定義済みユーザロール

network-admin

パラメータ

dscp-value: 送信 IPv4 パケットの DHCP を指定します。設定範囲は 0～63 です。DSCP の値が大きくなると、プライオリティが高くなります。

説明

ssh server dscp コマンドは SSH サーバが SSH クライアントに IPv4 パケットを送信する DHCP を設定します。

undo ssh server dscp コマンドはデフォルトに戻します。

DHCP パケットの DSCP の値はパケットのプライオリティを指定します。パケットを送信するプライオリティに影響します。

例

SSH サーバによって送信される IPv4 パケットの DSCP を 30 に設定します。

<Switch> system-view

[Switch] ssh server dscp 30

10.1.12 ssh server enable

Syntax

ssh server enable

undo ssh server enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

ssh server enable コマンドは Stelnet サーバ機能を有効にします。

undo ssh server enable コマンドは Stelnet サーバ機能を無効にします。

例

Stelnet サーバ機能を有効にします。

<Switch> system-view

[Switch] ssh server enable

関連コマンド

display ssh server

10.1.13 ssh server ipv6 acl

Syntax

ssh server ipv6 acl { **ipv6** { *advanced-acl-number* | *basic-acl-number* } | **mac** *mac-acl-number* }

undo ssh server ipv6 acl

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

ipv6: IPv6 ACL を指定します。

advanced-acl-number: 拡張 IPv4 ACL を指定します。設定範囲は 3000～3999 です。

basic-acl-number: 標準 IPv4 ACL を指定します。設定範囲は 2000～2999 です。

mac *mac-acl-number:* L2 ACL を指定します。設定範囲は 4000～4999 です。

説明

ssh server ipv6 acl コマンドは IPv6 SSH サーバへのアクセスを制御します。

undo ssh server ipv6 acl コマンドはデフォルトに戻します。

IPv6 ACL を使用して IPv6 SSH クライアントの要求パケットをフィルタするために使用します。

- ACL ルールが設定されている場合、ACL の permit 条件に一致する IPv6 SSH クライアントの要求パケットのみがサーバにアクセスすることができます。
- ACL ルールが存在しない、あるいは ACL に条件がない場合、すべての IPv6 SSH クライアントがサーバにアクセスすることができます。

この設定は、設定した後に SSH 接続を行った要求パケットから有効になります。

このコマンドを複数実行した場合、最後に行われた設定が適用されます。

例

サブネット 1::1/64 の IPv6 SSH クライアントのみサーバにアクセスできるように ACL 2001 を設定します。

<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

関連コマンド

display ssh server

10.1.14 ssh server ipv6 dscp

Syntax

ssh server ipv6 dscp *dscp-value*

undo ssh server ipv6 dscp

デフォルト

48

View

System view

定義済みユーザロール

network-admin

パラメータ

dscp-value: 送信 IPv6 パケットの DHCP を指定します。設定範囲は 0～63 です。DSCP の値が大きくなると、プライオリティが高くなります。

説明

ssh server ipv6 dscp コマンドは SSH サーバが SSH クライアントに IPv6 パケットを送信する DHCP を設定します。

undo ssh server ipv6 dscp コマンドはデフォルトに戻します。

DHCP パケットの DSCP の値は IPv6 パケットのプライオリティを指定します。IPv6 パケットを送信するプライオリティに影響します。

例

SSH サーバが SSH クライアントに IPv6 パケットを送信する DHCP を 30 に設定します。

<Switch> system-view

[Switch] ssh server ipv6 dscp 30

10.1.15 ssh server rekey-interval

Syntax

ssh server rekey-interval *interval*

undo ssh server rekey-interval

デフォルト

アップデート間隔の値は 0 時間です。RSA サーバ鍵ペアのアップデートを行いません。

View

System view

定義済みユーザロール

network-admin

パラメータ

interval: RSA サーバ鍵ペアのアップデート間隔を指定します。設定範囲は 1～24 時間です。

説明

ssh server rekey-interval コマンドは RSA サーバ鍵ペアのアップデート間隔を設定します。

undo ssh server rekey-interval コマンドはデフォルトに戻します。

RSA サーバ鍵ペアを定期的にアップデートすることで、鍵ペアのハッキングを防ぎ、SSH 接続のセキュリティを強化することができます。

システムは SSH1 ユーザがサーバにログイン後にアップデート最小間隔を数え始めます。新しい SSH1 ユーザがアップデート最小間隔後にサーバにログインする場合、システムは以下の操作をします。

1) RSA サーバ鍵ペアをアップデートします。
2) 新しいユーザの鍵ペアネゴシエーションにアップデートされた RSA サーバ鍵ペアを使用します。
3) アップデート最小間隔を再び数え始めます。

このコマンドは、SSH1 クライアントソフトウェアを使用する SSH クライアントのみ適用します。

例

RSA サーバ鍵ペアのアップデート間隔を 3 時間に設定します。

<Switch> system-view

[Switch] ssh server rekey-interval 3

関連コマンド

display ssh server

10.1.16 ssh user

Syntax

ssh user *username* **service-type** { **all** | **scp** | **sftp** | **stelnet** } **authentication-type** { **password** | { **any** | **password-publickey** | **publickey** } [**assign publickey** *keyname*&<1-6>] }

undo ssh user *username*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

username: SSH ユーザ名を指定します。設定範囲は 1～80 文字です。大文字、小文字を区別します。ユーザ名には、a、al、または all は使用できません。また、ユーザ名に縦棒(|)、コロン(:)、アスタリスク(*)、疑問符(?)または山かっこ(<>)を使用できます。アットマーク(@)、スラッシュ(/)、バックスラッシュは、pureusername@domain、pureusername/domain、domain¥pureusername の形式でユーザ名に ISP ドメイン名を付加する場合にのみ使用できます。SCP ユーザのユーザ名にハイフン(-)を含めない。そうしないと、そのユーザ名を使用した SCP ログインは失敗します。

service-type: SSH ユーザのサービスタイプを指定します。

- **all**: Stelnet、SFTP、SCP を指定します。
- **scp**: scp のサービスタイプを指定します。
- **sftp**: SFTP のサービスタイプを指定します。
- **stelnet**: Stelnet のサービスタイプを指定します。

authentication-type: SSH ユーザの認証方法を指定します。

- **password**: パスワード認証を指定します。認証方式は容易で暗号時間が早くなりますが、セキュリティ強度は脆弱です。ユーザ認証、許可、アカウンティングを実行する AAA と同時に使用することができます。
- **any**: パスワード認証あるいは公開鍵認証のどちらかを指定します。
- **password-publickey**: SSH2 クライアントのパスワード認証と公開鍵認証の両方を指定します。SSH2 クライアントでは、**password-publickey** 認証方式は高いセキュリティを提供します。SSH1 クライアントではパスワード認証あるいは公開鍵認証のどちらかを指定します。
- **publickey**: 公開鍵認証を指定します。認証方式は複雑で暗号時間が遅いですが、セキュリティ強度は強くなり、総当たり攻撃（ブルートフォース攻撃）に対して防御することができます。この認証方式は、使用しやすいです。一度設定すると、パスワードを記憶しておくことやパスワードを入力することなく、認証プロセスが自動で完了します。

assign: クライアントを確認するために使用するパラメータを指定します。

- **publickey** *keyname*&<1-6>: SSH クライアントの公開鍵を最大 6 つまで指定します。*keyname* はサーバで設定される SSH クライアントの公開鍵を示します。設定範囲は 1～64 文字です。大文字、小文字を区別します。サーバはクライアントの確認を行うため、クライアントの公開鍵を使用します。もしクライアントの公開鍵のファイルが変更されている場合、すぐにサーバのクライアントの公開鍵をアップデートする必要があります。複数のクライアントの公開鍵を指定した場合、装置は指定し

た順番で公開鍵を使用してユーザを識別し、確認します。1 つの公開鍵にパスした場合、ユーザが正当であることが確認されます。

説明

ssh user コマンドは SSH ユーザを作成し、サービスタイプと認証方式を指定します。

undo ssh user コマンドは SSH ユーザを削除します。

SSH ユーザを設定するため、認証方式に従ってコマンドを使用します。

認証方式が公開鍵である場合、SSH ユーザとローカルユーザを作成する必要があります。SSH ユーザが正しい作業ディレクトリとユーザロールを割り当てられるように、ローカルユーザは SSH ユーザのユーザ名と同一にする必要があります。

認証方式がパスワードである場合、SSH ユーザは以下の処理のどちらか 1 つを実行する必要があります。

- ローカル認証用に、**local-user** コマンドを使用してローカルユーザを設定します。
- リモート認証用に、RADIUS サーバのようなリモート認証サーバの SSH ユーザを設定します。

ssh user コマンドを使用して SSH ユーザを作成する必要がありません。しかし、集中管理のため、すべての SSH ユーザ（パスワード認証のみの SSH ユーザを含みます）を表示する場合、このコマンドを使用することができます。SSH ユーザが作成された場合、正しいサービスタイプと認証方式であることを確認してください。

- 認証方式が **password-publickey** あるいは **any** である場合、SSH ユーザは以下の処理のどちらか 1 つを実行する必要があります。
  - ローカル認証用に、**local-user** コマンドを使用してローカルユーザを設定します。
  - リモート認証用に、RADIUS サーバのようなリモート認証サーバの SSH ユーザを設定します。

どちらの場合でも、ローカルユーザあるいはリモート認証サーバで設定される SSH ユーザは SSH ユーザと同じユーザ名を使用する必要があります。

SFTP または SCP ユーザでは、作業ディレクトリは認証方式に依存します。

- 認証方式が **publickey** あるいは **password-publickey** である場合、作業ディレクトリは、関連した local user view で **authorization-attribute** コマンドを使用して指定されます。
- 認証方式がパスワードである場合、作業ディレクトリは AAA によって許可されます。

SSH ユーザでは、ユーザロールは認証方式に依存します。

- 認証方式が **publickey** あるいは **password-publickey** である場合、ユーザロールは関連した local user view で **authorization-attribute** コマンドを使用して指定されます。
- 認証方式がパスワードである場合、ユーザロールはリモート AAA サーバあるいはローカル装置によって許可されます。

ホスト公開鍵を指定するため、このコマンドを複数回使用した場合、最後に行った設定が適用されます。ホスト公開鍵を指定しない場合、ユーザはログインを行うために証明書認証を使用します。

ユーザが SSH サーバと通信しているとき、SSH ユーザの認証方式、サービスタイプ、ホスト公開鍵を変更することができますが、設定の変更は次回ログインのクライアントのみ適用されます。

例

SSH ユーザ user1 を作成します。ユーザにサービスタイプ sftp、認証方式 password-publickey を指定します。ユーザにホスト公開鍵 key1 を割り当てます。

<Switch> system-view

[Switch] ssh user user1 service-type sftp authentication-type password-publickey assign publickey key1

ローカル装置管理ユーザ user1 を作成します。プレーンテキストでパスワード 123456TESTplat&!を指定し、ユーザのサービスタイプ ssh を指定します。作業ディレクトリ flash:を割り当て、ユーザにユーザロール network-admin を割り当てます。

[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

関連コマンド

- **authorization-attribute**
- **display ssh user-information**
- **local-user**
- **pki domain**

10.2 SSHクライアント設定コマンド

10.2.1 bye

Syntax

bye

View

SFTP client view

定義済みユーザロール

network-admin

説明

bye コマンドは SFTP サーバとの通信を終了し、user view に戻ります。

このコマンドは **exit** コマンド、**quit** コマンドと同一です。

例

SFTP サーバとの通信を終了し、user view に戻ります。

sftp> bye

```
<Switch>
```

10.2.2 cd

Syntax

cd [*remote-path*]

View

SFTP client view

定義済みユーザロール

network-admin

パラメータ

remote-path: サーバのパスの名前を指定します。

説明

cd コマンドは SFTP サーバの作業パスを変更します。

上位のディレクトリに戻るため、**cd ..**コマンドを使用できます。

ルートディレクトリに戻るため、**cd /**コマンドを使用できます。

例

作業パスを new1 に変更します。

sftp> cd new1

```
Current Directory is:/new1
```

sftp> pwd

```
Remote working directory: /new1
sftp>
```

10.2.3 cdup

Syntax

cdup

View

SFTP client view

定義済みユーザロール

network-admin

説明

cdup コマンドは上位のディレクトリに戻ります。

例

現在の作業ディレクトリ/test1 から上位のディレクトリに戻ります。

sftp> cd test1

```
Current Directory is:/test1
```

sftp> pwd

```
Remote working directory: /test1
```

sftp> cdup

```
Current Directory is:/
```

sftp> pwd

```
Remote working directory: /
sftp>
```

10.2.4 delete

Syntax

delete *remote-file*

View

SFTP client view

定義済みユーザロール

network-admin

パラメータ

remote-file: サーバから削除するファイルを指定します。

説明

delete コマンドはサーバからファイルを削除します。

このコマンドは **remove** コマンドと同一です。

例

サーバからファイル temp.c を削除します。

sftp> delete temp.c

```
Removing /temp.c
```

10.2.5 dir

Syntax

dir [**-a** | **-l**] [*remote-path*]

View

SFTP client view

定義済みユーザロール

network-admin

パラメータ

-a: リストのディレクトリの下にあるファイルとサブディレクトリの詳細情報を表示します。ドット（.）で始まる名前のファイルとサブディレクトリも含みます。

-l: リストのディレクトリの下にあるファイルとサブディレクトリの詳細情報を表示します。ドット（.）で始まる名前のファイルとサブディレクトリは除きます。

remote-path: ディレクトリの名前を指定します。指定しない場合、現在の作業ディレクトリの下にあるファイルとディレクトリの詳細情報を表示します。

説明

dir コマンドはディレクトリの下にあるファイルとサブディレクトリの情報を表示します。

-a あるいは**-l** のいずれも指定しない場合、ディレクトリの下にあるファイルとサブディレクトリの詳細情報を表示します。

このコマンドは **ls** コマンドと同一です。

例

リストのディレクトリの下にあるファイルとサブディレクトリの詳細情報を表示します。ドット（.）で始まる名前のファイルとサブディレクトリも含みます。

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
```

リストのディレクトリの下にあるファイルとサブディレクトリの詳細情報を表示します。

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.pu
```

10.2.6 display sftp client source

Syntax

display sftp client source

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display sftp client source コマンドは SFTP クライアントの送信元 IP アドレスを表示します。

例

SFTP クライアントの送信元 IP アドレスを表示します。

<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.
```

関連コマンド

- **sftp client ipv6 source**
- **sftp client source**

10.2.7 display ssh client source

Syntax

display ssh client source

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display ssh client source コマンドは Stelnet クライアントの送信元 IP アドレスを表示します。

例

Stelnet クライアントの送信元 IP アドレスを表示します。

<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.
```

関連コマンド

- **ssh client ipv6 source**
- **ssh client source**

10.2.8 exit

Syntax

exit

View

SFTP client view

定義済みユーザロール

network-admin

説明

exit コマンドは SFTP サーバとの通信を終了し、user view に戻ります。

このコマンドは **bye** コマンド、**quit** コマンドと同一です。

例

SFTP サーバとの通信を終了し、user view に戻ります。

sftp> exit

```
<Switch>
```

10.2.9 get

Syntax

get *remote-file* [*local-file*]

View

SFTP client view

定義済みユーザロール

network-admin

パラメータ

remote-file: SFTP サーバの名前を指定します。

local-file: ローカルファイルの名前を指定します。指定しない場合、ファイルはサーバのファイルと同一の名前で保存されます。

説明

get コマンドは FTP サーバからファイルをダウンロードし、ローカルにファイルを保存します。

例

ファイル temp1.c をダウンロードし、ローカルにファイル temp.c として保存します。

sftp> get temp1.c temp.c

```
Fetching /temp1.c to temp.c
/temp.c                                       100% 1424     1.4KB/s   00:00
```

10.2.10 help

Syntax

help

View

SFTP client view

定義済みユーザロール

network-admin

説明

help コマンドは SFTP クライアントコマンドのヘルプ情報を表示します。

このコマンドはクォーテーションマーク（?）を入力した場合と同一です。

例

SFTP クライアントでヘルプ情報を表示します。

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
```

10.2.11 ls

Syntax

ls [**-a** | **-l**] [*remote-path*]

View

SFTP client view

定義済みユーザロール

network-admin

パラメータ

-a: リストのディレクトリの下にあるファイルとサブディレクトリの詳細情報を表示します。ドット（.）で始まる名前のファイルとサブディレクトリも含みます。

-l: リストのディレクトリの下にあるファイルとサブディレクトリの詳細情報を表示します。ドット（.）で始まる名前のファイルとサブディレクトリは除きます。

remote-path: ディレクトリの名前を指定します。指定しない場合、現在の作業ディレクトリの下にあるファイルとディレクトリの詳細情報を表示します。

説明

ls コマンドはディレクトリの下にあるファイルとサブディレクトリの情報を表示します。

-a あるいは**-l** のいずれも指定しない場合、ディレクトリの下にあるファイルとサブディレクトリの詳細情報を表示します。

このコマンドは **dir** コマンドと同一です。

例

リストのディレクトリの下にあるファイルとサブディレクトリの詳細情報を表示します。ドット（.）で始まる名前のファイルとサブディレクトリも含みます。

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
```

リストのディレクトリの下にあるファイルとサブディレクトリの詳細情報を表示します。

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
```

10.2.12 mkdir

Syntax

mkdir *remote-path*

View

SFTP client view

定義済みユーザロール

network-admin

パラメータ

remote-path: SFTP サーバのディレクトリ名を指定します。

説明

mkdir コマンドは SFTP サーバ上にディレクトリを作成します。

例

SFTP サーバ上にディレクトリを作成します。

sftp> mkdir test

10.2.13 put

Syntax

put *local-file* [*remote-file*]

View

SFTP client view

定義済みユーザロール

network-admin

パラメータ

local-file: ローカルファイルの名前を指定します。

remote-file: SFTP サーバの名前を指定します。指定しない場合、ファイルはローカルファイルと同一の名前で保存されます。

説明

put コマンドは SFTP サーバにローカルファイルをアップロードします。

例

SFTP サーバにローカルファイル startup.bak をアップロードし、startup01.bak として保存します。

sftp> put startup.bak startup01.bak

```
Uploading startup.bak to /startup01.bak
startup01.bak                              100% 1424     1.4KB/s   00:00
```

10.2.14 pwd

Syntax

pwd

View

SFTP client view

定義済みユーザロール

network-admin

説明

pwd コマンドは SFTP サーバの現在の作業ディレクトリを表示します。

例

SFTP サーバの現在の作業ディレクトリを表示します。

sftp> pwd

```
Remote working directory: /
The output shows that the current working directory is the root directory.
```

10.2.15 quit

Syntax

quit

View

SFTP client view

定義済みユーザロール

network-admin

説明

quit コマンドは SFTP サーバとの通信を終了し、user view に戻ります。

このコマンドは **bye** コマンド、**exit** コマンドと同一です。

例

SFTP サーバとの通信を終了し、user view に戻ります。

sftp> quit

<Switch>

10.2.16 remove

Syntax

remove *remote-file*

View

SFTP client view

定義済みユーザロール

network-admin

パラメータ

remote-file: ファイルを指定します。

説明

remove コマンドは SFTP サーバからファイルを削除します。

このコマンドは **delete** コマンドと同一です。

例

SFTP サーバからファイル temp.c を削除します。

sftp> remove temp.c

```
Removing /temp.c
```

10.2.17 rename

Syntax

rename *old-name new-name*

View

SFTP client view

定義済みユーザロール

network-admin

パラメータ

old-name: 既存のファイルあるいはディレクトリの名前を指定します。

new-name: 新しいファイルあるいはディレクトリの名前を指定します。

説明

rename コマンドは SFTP サーバのファイルあるいはディレクトリの名前を変更します。

例

SFTP サーバのファイルの名前を temp1.c から temp2.c に変更します。

sftp> dir

```
aa.pub  temp1.c
```

sftp> rename temp1.c temp2.c

sftp> dir

```
aa.pub  temp2.c
```

10.2.18 rmdir

Syntax

rmdir *remote-path*

View

SFTP client view

定義済みユーザロール

network-admin

パラメータ

remote-path: ディレクトリを指定します。

説明

rmdir コマンドは SFTP サーバからディレクトリを削除します。

例

SFTP サーバの現在のディレクトリの下のサブディレクトリ temp1 を削除します。

sftp> rmdir temp1

10.2.19 scp

Syntax

scp *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] { **put** | **get** } *source-file-name* [*destination-file-name*] [**identity-key** { **dsa** | **ecdsa-sha2-nistp256** | **ecdsa-sha2-nistp384** | **rsa** | { **x509v3-ecdsa-sha2-nistp256** | **x509v3-ecdsa-sha2-nistp384** } } | **prefer-compress zlib** | **prefer-ctos-cipher** { **3des-cbc** | **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** | **des-cbc** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** |

sha1-96 | **sha2-256** | **sha2-512** } | **prefer-kex** { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** | **ecdh-sha2-nistp256** | **ecdh-sha2-nistp384** } | **prefer-stoc-cipher** { **3des-cbc** | **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** | **des-cbc** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** }] * [**public-key** *keyname* | **source** { **interface** *interface-type interface-number* | **ip** *ip-address* }] * [**user** *username* [**password** *password*]]

View

User view

定義済みユーザロール

network-admin

パラメータ

server: IPv4 アドレスまたはホスト名でサーバを指定します。設定範囲は 1～253 文字です。大文字、小文字を区別しません。

port-number: サーバのポート番号を指定します。設定範囲は 1～65535 です。デフォルトは 22 です。

vpn-instance *vpn-instance-name*: サーバが属する VPN インスタンスを指定します。大文字、小文字を区別し、設定範囲は 1～31 文字です。

get: ファイルをダウンロードします。

put: ファイルをアップロードします。

source-file-name: ソースファイル名を指定します。大文字、小文字を区別し、設定範囲は 1～255 文字です。

destination-file-name: ターゲットファイル名を指定します。大文字、小文字を区別し、設定範囲は 1～255 文字です。指定しない場合、ターゲットファイルはソースファイルと同じファイル名を使用します。

identity-key: クライアントの公開鍵認証用の公開鍵アルゴリズムを指定します。デフォルトは dsa です。サーバが公開鍵認証を使用する場合、指定する必要があります。ローカルプライベート鍵を使用してクライアントはデジタル署名を作成します。

- **dsa**: 公開鍵アルゴリズム dsa を指定します。
- **ecdsa-sha2-nistp256**: 256 ビットの鍵強度を持つ ECDSA アルゴリズムを指定します。
- **ecdsa-sha2-nistp384**: 384 ビットの鍵強度を持つ ECDSA アルゴリズムを指定します。
- **rsa**: 公開鍵アルゴリズム rsa を指定します。
- **x509v3-ecdsa-sha2-nistp256**: 公開鍵アルゴリズム x509v3-ecdsa-sha2-nistp256 を指定します。
- **x509v3-ecdsa-sha2-nistp384**: 公開鍵アルゴリズム x509v3-ecdsa-sha2-nistp384 を指定します。

prefer-compress: サーバとクライアント間のデータ圧縮に推奨される圧縮アルゴリズムを指定します。デフォルトでは、圧縮はサポートされていません。

zlib: 圧縮アルゴリズム zlib を指定します。

prefer-ctos-cipher: クライアントからサーバへの優先暗号化アルゴリズムを指定します。デフォルトは AES128-CTR です。サポートされているアルゴリズムは、セキュリティ強度と計算時間の昇順で、DES-CBC、3DES-CBC、AES128-CBC、AES128-CTR、AES128-GCM、AES192-CTR、AES256-CBC、AES256-CTR、および AES256-GCM です。

- **3des-cbc**: 暗号化アルゴリズム 3DES-CBC を指定します。
- **aes128-cbc**: 暗号化アルゴリズム AES128-CBC を指定します。
- **aes128-ctr**: 暗号化アルゴリズム AES128-CTR を指定します。
- **aes128-gcm**: 暗号化アルゴリズム AES128-GCM を指定します。
- **aes192-ctr**: 暗号化アルゴリズム AES192-CTR を指定します。
- **aes256-cbc**: 暗号化アルゴリズム AES256-CBC を指定します。
- **aes256-ctr**: 暗号化アルゴリズム AES256-CTR を指定します。
- **aes256-gcm**: 暗号化アルゴリズム AES256-GCM を指定します。
- **des-cbc**: 暗号化アルゴリズム DES-CBC を指定します。

prefer-ctos-hmac: クライアントからサーバへの優先 HMAC アルゴリズムを指定します。デフォルトは SHA2-256 です。サポートされているアルゴリズムは、セキュリティ強度と計算時間の昇順で、MD5、MD5-96、SHA1、SHA1-96、SHA2-256、SHA2-512 です。

- **md5**: HMAC アルゴリズム HMAC-MD5 を指定します。
- **md5-96**: HMAC アルゴリズム HMAC-MD5-96 を指定します。
- **sha1**: HMAC アルゴリズム HMAC-SHA1 を指定します。
- **sha1-96**: HMAC アルゴリズム HMAC-SHA1-96 を指定します。
- **sha2-256**: HMAC アルゴリズム HMAC-SHA2-256 を指定します。
- **sha2-512**: HMAC アルゴリズム HMAC-SHA2-512 を指定します。

prefer-kex: 優先鍵交換アルゴリズムを指定します。デフォルトは ecdh-sha2-nistp256 です。サポートされるアルゴリズムは、セキュリティ強度と計算時間の昇順で、difie-hellman-group-exchange-sha1、difie-hellman-group1-sha1、difie-hellman-group14-sha1、ecdh-sha2-nistp256、および ecdh-sha2-nistp384 です。

- **dh-group-exchange-sha1**: 鍵交換アルゴリズム difi-hellman-group-exchange-sha1 を指定します。
- **dh-group1-sha1**: 鍵交換アルゴリズム difie-hellman-group1-sha1 を指定します。
- **dh-group14-sha1**: 鍵交換アルゴリズム difie-hellman-group14-sha1 を指定します。
- **ecdh-sha2-nistp256**: 鍵交換アルゴリズム ecdh-sha2-nistp256 を指定します。
- **ecdh-sha2-nistp384**: 鍵交換アルゴリズム ecdh-sha2-nistp384 を指定します。

prefer-stoc-cipher: サーバからクライアントへの優先暗号化アルゴリズムを指定します。デフォルトは AES128-CTR です。サポートされるアルゴリズムは、クライアントからサーバへの暗号化アルゴリズム(**prefer-ctos-cipher** キーワードを参照)と同じです。

prefer-stoc-hmac: サーバからクライアントへの優先 HMAC アルゴリズムを指定します。デフォルトは SHA2-256 です。サポートされるアルゴリズムは、クライアントからサーバへの HMAC アルゴリズム(**prefer-ctos-hmac** キーワードを参照)と同じです。

public-key *keyname*: クライアントがサーバの認証に使用するサーバのホスト公開鍵を指定します。設定範囲は 1～64 文字です。大文字、小文字を区別しないストリングを指定します。

source: SCP パケットの送信元 IPv4 アドレスまたは送信元インタフェースを指定します。デフォルトでは、装置は SCP パケットの送信元アドレスとしてルーティングエントリの出力インタフェースのプライマリ IPv4 アドレスを使用します。SCP 接続を成功させるための最善の方法として、送信元インタフェースとしてループバックインタフェースを指定するか、送信元アドレスとしてループバックインタフェースの IPv4 アドレスを指定します。

- **interface** *interface-type interface-number*: ソースインタフェースをタイプと番号で指定します。このインタフェースの IPv4 アドレスは SCP パケットの送信元 IPv4 アドレスです。
- **ip** *ip-address*: 送信元 IPv4 アドレスを指定します。

user *username*: SCP ユーザ名を指定します。大文字、小文字を区別し、設定範囲は 1～80 文字です。ユーザ名に ISP ドメイン名が含まれている場合は、*pureusername@domain*、*pureusername/domain*、または *domain¥pureusername* の形式を使用します。

password *password*: パスワードをプレーンテキスト形式で指定します。大文字と小文字を区別し、設定範囲は 1~63 文字です。

説明

scp コマンドは IPv4 SCP サーバへの接続を確立し、サーバとファイルを転送します。

コマンドでユーザ名とパスワードを指定しない場合は、対話形式でユーザ名とパスワードを指定する必要があります。

SCP サーバが公開鍵認証を使用する場合、このコマンドによって指定されたパスワードは無視されます。

例

SCP クライアントを SCP サーバ **200.1.1.1** に接続します。サーバの公開鍵を **svkey** として指定し、サーバからファイル **abc.txt** をダウンロードします。SCP クライアントは、公開鍵認証を使用します。次のアルゴリズムを使用します。

- 優先される鍵交換アルゴリズムは **dh-group14-sha1** です。
- サーバからクライアントへの優先される暗号化アルゴリズムは **aes128-cbc** です。
- クライアントからサーバへの優先される HMAC アルゴリズムは **sha1** です。
- サーバからクライアントへの優先される HMAC アルゴリズムは **sha1-96** です。
- サーバとクライアント間で優先される圧縮アルゴリズムは **zlib** です。

<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:
```

10.2.20 scp ipv6

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** | **ecdsa-sha2-nistp256** | **ecdsa-sha2-nistp384** | **rsa** | { **x509v3-ecdsa-sha2-nistp256** | **x509v3-ecdsa-sha2-nistp384** } } | **prefer-compress zlib** | **prefer-ctos-cipher** { **3des-cbc** | **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** | **des-cbc** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** } | **prefer-kex** { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** | **ecdh-sha2-nistp256** | **ecdh-sha2-nistp384** } | **prefer-stoc-cipher** { **3des-cbc** | **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** | **des-cbc** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** }] * [**public-key** *keyname* | **source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }] * [**user** *username* [**password** *password*]]

View

User view

定義済みユーザロール

network-admin

パラメータ

server: IPv6 アドレスまたはホスト名でサーバを指定します。設定範囲は 1～253 文字です。大文字、小文字を区別しません。

port-number: サーバのポート番号を指定します。設定範囲は 1～65535 です。デフォルトは 22 です。

vpn-instance *vpn-instance-name*: サーバが属する VPN インスタンスを指定します。大文字小文字を区別し、設定範囲は 1～31 文字です。

-i *interface-type interface-number*: SCP パケットのタイプと数によって出力インタフェースを指定します。このオプションは、サーバがリンクローカルアドレスを使用してクライアントに SCP サービスを提供する場合にのみ使用されます。SCP クライアント上の指定された出力インタフェースはリンクローカルアドレスを持たなければなりません。

get: ファイルをダウンロードします。

put: ファイルをアップロードします。

source-file-name: ソースファイル名を指定します。大文字、小文字を区別し、設定範囲は 1～255 文字です。

destination-file-name: ターゲットファイル名を指定します。大文字、小文字を区別し、設定範囲は 1～255 文字です。指定しない場合、ターゲットファイルはソースファイルと同じファイル名を使用します。

identity-key: クライアントの公開鍵認証用の公開鍵アルゴリズムを指定します。デフォルトは dsa です。サーバが公開鍵認証を使用する場合、指定する必要があります。ローカルプライベート鍵を使用してクライアントはデジタル署名を作成します。

- **dsa**: 公開鍵アルゴリズム dsa を指定します。
- **ecdsa-sha2-nistp256**: 256 ビットの鍵強度を持つ ECDSA アルゴリズムを指定します。
- **ecdsa-sha2-nistp384**: 384 ビットの鍵強度を持つ ECDSA アルゴリズムを指定します。
- **rsa**: 公開鍵アルゴリズム rsa を指定します。
- **x509v3-ecdsa-sha2-nistp256**: 公開鍵アルゴリズム x509v3-ecdsa-sha2-nistp256 を指定します。
- **x509v3-ecdsa-sha2-nistp384**: 公開鍵アルゴリズム x509v3-ecdsa-sha2-nistp384 を指定します。

prefer-compress: サーバとクライアント間のデータ圧縮に推奨される圧縮アルゴリズムを指定します。デフォルトでは、圧縮はサポートされていません。

zlib: 圧縮アルゴリズム **zlib** を指定します。

prefer-ctos-cipher: クライアントからサーバへの優先暗号化アルゴリズムを指定します。デフォルトは AES128-CTR です。サポートされているアルゴリズムは、セキュリティ強度と計算時間の昇順で、DES-CBC、3DES-CBC、AES128-CBC、AES128-CTR、AES128-GCM、AES192-CTR、AES256-CBC、AES256-CTR、および AES256-GCM です。

- **3des-cbc**: 暗号化アルゴリズム 3DES-CBC を指定します。
- **aes128-cbc**: 暗号化アルゴリズム AES128-CBC を指定します。
- **aes128-ctr**: 暗号化アルゴリズム AES128-CTR を指定します。
- **aes128-gcm**: 暗号化アルゴリズム AES128-GCM を指定します。
- **aes192-ctr**: 暗号化アルゴリズム AES192-CTR を指定します。
- **aes256-cbc**: 暗号化アルゴリズム AES256-CBC を指定します。
- **aes256-ctr**: 暗号化アルゴリズム AES256-CTR を指定します。
- **aes256-gcm**: 暗号化アルゴリズム AES256-GCM を指定します。
- **des-cbc**: 暗号化アルゴリズム DES-CBC を指定します。

prefer-ctos-hmac: クライアントからサーバへの優先 HMAC アルゴリズムを指定します。デフォルトは SHA2-256 です。サポートされているアルゴリズムは、セキュリティ強度と計算時間の昇順で、MD5、MD5-96、SHA1、SHA1-96、SHA2-256、SHA2-512 です。

- **md5**: HMAC アルゴリズム HMAC-MD5 を指定します。
- **md5-96**: HMAC アルゴリズム HMAC-MD5-96 を指定します。
- **sha1**: HMAC アルゴリズム HMAC-SHA1 を指定します。
- **sha1-96**: HMAC アルゴリズム HMAC-SHA1-96 を指定します。
- **sha2-256**: HMAC アルゴリズム HMAC-SHA2-256 を指定します。

- **sha2-512**: HMAC アルゴリズム HMAC-SHA2-512 を指定します。

prefer-kex: 優先鍵交換アルゴリズムを指定します。デフォルトは ecdh-sha2-nistp256 です。サポートされるアルゴリズムは、セキュリティ強度と計算時間の昇順で、difie-hellman-group-exchange-sha1 、 difie-hellman-group1-sha1 、 difie-hellman-group14-sha1、ecdh-sha2-nistp256、および ecdh-sha2-nistp384 です。

- **dh-group-exchange-sha1**: 鍵交換アルゴリズム difi-hellman-group-exchange-sha1 を指定します。
- **dh-group1-sha1**: 鍵交換アルゴリズム difie-hellman-group1-sha1 を指定します。
- **dh-group14-sha1**: 鍵交換アルゴリズム difie-hellman-group14-sha1 を指定します。
- **ecdh-sha2-nistp256**: 鍵交換アルゴリズム ecdh-sha2-nistp256 を指定します。
- **ecdh-sha2-nistp384**: 鍵交換アルゴリズム ecdh-sha2-nistp384 を指定します。

prefer-stoc-cipher: サーバからクライアントへの優先暗号化アルゴリズムを指定します。デフォルトは AES128-CTR です。サポートされるアルゴリズムは、クライアントからサーバへの暗号化アルゴリズム(**prefer-ctos-cipher** キーワードを参照)と同じです。

prefer-stoc-hmac: サーバからクライアントへの優先 HMAC アルゴリズムを指定します。デフォルトは SHA2-256 です。サポートされるアルゴリズムは、クライアントからサーバへの HMAC アルゴリズム(**prefer-ctos-hmac** キーワードを参照)と同じです。

public-key *keyname*: クライアントがサーバの認証に使用するサーバのホスト公開鍵を指定します。設定範囲は 1～64 文字です。大文字、小文字を区別しないストリングを指定します。

source: IPv6 SCP パケットの送信元 IPv6 アドレスまたは送信元インタフェースを指定します。デフォルトで、装置は RFC3484 に従って IPv6 SCP パケットのソースアドレスを自動的に選択します。SCP 接続を成功させるための最善の方法として、ループバックインタフェースを送信元インタフェースとして指定するか、ループバックインタフェースの IPv6 アドレスを送信元アドレスとして指定します。

- **interface** *interface-type interface-number*: ソースインタフェースをタイプと番号で指定します。このインタフェース IPv6 アドレスは IPv6SCP パケットの送信元 IPv6 アドレスです。
- **ipv6** *ipv6-address*: 送信元 IPv6 アドレスを指定します。

user *username*: SCP ユーザ名を指定します。大文字と小文字を区別し、設定範囲は 1~80 文字です。ユーザ名に ISP ドメイン名が含まれている場合は、*pureusername@domain*、*pureusername/domain*、または *domain¥pureusername* の形式を使用します。

password *password*: パスワードをプレーンテキスト形式で指定します。大文字と小文字を区別し、設定範囲は 1～63 文字です。

説明

scp ipv6 コマンドは IPv6 SCP サーバへの接続を確立し、サーバとファイルを転送します。

コマンドでユーザ名とパスワードを指定しない場合は、対話形式でユーザ名とパスワードを指定する必要があります。

SCP サーバが公開鍵認証を使用する場合、このコマンドによって指定されたパスワードは無視されます。

例

SCP クライアントを SCP サーバ **2000::1.**に接続します。サーバの公開鍵を **svkey** として指定し、サーバからファイル **abc.txt** をダウンロードします。SCP クライアントは、公開鍵認証を使用します。次のアルゴリズムを使用します。

- 優先される鍵交換アルゴリズムは **dh-group14-sha1** です。
- サーバからクライアントへの優先される暗号化アルゴリズムは **aes128-cbc** です。
- クライアントからサーバへの優先される HMAC アルゴリズムは **sha1** です。
- サーバからクライアントへの優先される HMAC アルゴリズムは **sha1-96** です。
- サーバとクライアント間で優先される圧縮アルゴリズムは **zlib** です。

<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:
```

10.2.21 sftp

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* }] *

View

User view

定義済みユーザロール

network-admin

パラメータ

server: IPv4 アドレスあるいはホスト名でサーバを指定します。設定範囲は 1～253 文字です。大文字、小文字を区別しません。

port-number: サーバのポート番号を指定します。設定範囲は 1～65535 です。デフォルトは 22 です。

vpn-instance *vpn-instance-name*: サーバが属する VPN インスタンスを指定します。大文字小文字を区別し、設定範囲は 1～31 文字です。

identity-key: クライアントの公開鍵アルゴリズムを指定します。サーバが公開鍵認証を使用する場合、指定する必要があります。クライアントはアルゴリズムに関連したローカル秘密鍵を使用してデジタル署名を作成します。

- **dsa**: 公開鍵アルゴリズム dsa を指定します。
- **rsa**: 公開鍵アルゴリズム rsa を指定します。

prefer-compress: サーバとクライアント間で優先される圧縮アルゴリズムを指定します。

zlib: 圧縮アルゴリズム zlib を指定します。

prefer-ctos-cipher: クライアントからサーバへの優先される暗号化アルゴリズムを指定します。アルゴリズム **des-cbc**、**3des-cbc**、**aes128-cbc** の順番でセキュリティの強度が強くなり、計算時間が長くなります。

- **3des-cbc**: 暗号化アルゴリズム 3des-cbc を指定します。
- **aes128-cbc**: 暗号化アルゴリズム aes128-cbc を指定します。
- **des-cbc**: 暗号化アルゴリズム des-cbc を指定します。

prefer-ctos-hmac: クライアントからサーバへの優先される HMAC アルゴリズムを指定します。アルゴリズム **md5**、**md5-96**、**sha1**、**sha1-96** の順番でセキュリティの強度が強くなり、計算時間が長くなります。

- **md5:** HMAC アルゴリズム hmac-md5 を指定します。
- **md5-96:** HMAC アルゴリズム hmac-md5-96 を指定します。
- **sha1:** HMAC アルゴリズム hmac-sha1 を指定します。
- **sha1-96:** HMAC アルゴリズム hmac-sha1-96 を指定します。

prefer-kex: 優先される鍵交換アルゴリズムを指定します。アルゴリズム **dh-group-exchange-sha1**、**dh-group1-sha1**、**dh-group14-sha1** の順番でセキュリティの強度が強くなり、計算時間が長くなります。

- **dh-group-exchange-sha1**: 鍵交換アルゴリズム diffie-hellman-group-exchange-sha1 を指定します。
- **dh-group1-sha1**: 鍵交換アルゴリズム diffie-hellman-group1-sha1 を指定します。
- **dh-group14-sha1**: 鍵交換アルゴリズム diffie-hellman-group14-sha1 を指定します。

prefer-stoc-cipher: サーバからクライアントへの優先される暗号化アルゴリズムを指定します。サポートするアルゴリズムは **prefer-ctos-cipher** 暗号化アルゴリズムと同一にしてください。

prefer-stoc-hmac: サーバからクライアントへの優先される HMAC アルゴリズムを指定します。サポートするアルゴリズムは **prefer-ctos-hmac** 暗号化アルゴリズムと同一にしてください。

dscp *dscp-value*: SFTP クライアントによって送信される IPv4 SFTP パケットの DSCP を指定します。設定範囲は 0～63 です。デフォルトは 48 です。DSCP の値はパケットを送信するプライオリティに影響します。

public-key *keyname*: サーバを認証するためにクライアントが使用するサーバのホスト公開鍵を指定します。設定範囲は 1～64 文字です。

source: SFTP パケットの送信元 IP アドレスあるいは送信元インタフェースを指定します。デフォルトで SFTP パケットは送信元アドレスとして、ルーティングエントリで指定された送信インタフェースのプライマリ IP アドレスを使用します。SFTP 接続を正しく行うため、送信元インタフェースとしてループバックインタフェースを指定する、あるいは送信元 IPv4 アドレスとしてループバックインタフェースの IPv4 アドレスを指定します。

- **interface** *interface-type interface-number*: 送信元インタフェースのタイプと番号を指定します。インタフェースのプライマリ IPv4 アドレスは SFTP パケットの送信元 IPv4 アドレスです。
- **ip** *ip-address*: 送信元 IPv4 アドレスを指定します。

説明

sftp コマンドは IPv4 SFTP サーバとの接続を確立し、SFTP client view に移行します。

公開鍵認証では、クライアントはデジタル認証のローカルプライベート鍵を取得する必要があります。公開鍵アルゴリズムは RSA あるいは DSA アルゴリズムを使用するため、identity-key を使用して公開鍵アルゴリズムを指定する必要があります。クライアントは正しいローカルプライベート鍵を取得することができます。

例

IPv4 SFTP サーバ 10.1.1.2 に SFTP クライアントを接続し、サーバの公開鍵として svkey を指定します。SFTP クライアントは公開鍵認証を使用します。以下のアルゴリズムを使用します。

- 優先される鍵交換アルゴリズムは dh-group14-sha1 です。
- サーバからクライアントへの優先される暗号化アルゴリズムは aes128-cbc です。
- クライアントからサーバへの優先される HMAC アルゴリズムは sha1 です。
- サーバからクライアントへの優先される HMAC アルゴリズムは sha1-96 です。
- サーバとクライアント間で優先される圧縮アルゴリズムは zlib です。

<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

10.2.22 sftp client ipv6 source

Syntax

sftp client ipv6 source { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }

undo sftp client ipv6 source

デフォルト

SFTP パケットの送信元 IPv6 アドレスは設定されていません。SFTP パケットは RFC3484 で定義された送信元アドレスとして、自動で選択された IPv6 アドレスを選択します。

View

System view

定義済みユーザロール

network-admin

パラメータ

interface *interface-type interface-number*: 送信元インタフェースのタイプと番号を指定します。SFTP パケットは送信元アドレスとして指定されたインタフェースで、ロンゲストマッチの IPv6 アドレスを使用します。

ipv6 *ipv6-address*: 送信元 IPv6 アドレスを指定します。

説明

sftp client ipv6 source コマンドは SFTP パケットの送信元 IPv6 アドレスを指定します。

undo sftp client ipv6 source コマンドはデフォルトに戻します。

このコマンドはすべての IPv6 SFTP 接続に適用します。**sftp ipv6** コマンドで指定された送信元 IPv6 アドレスは、現在の IPv6 SFTP 接続のみ適用します。このコマンドと **sftp ipv6** コマンドの両方で送信元 IPv6 アドレスが指定された場合、**sftp ipv6** コマンドで指定された送信元 IPv6 アドレスが適用されます。

このコマンドを複数実行した場合、最後に行われた設定が適用されます。

例

SFTP パケットの送信元 IPv6 アドレスとして 2:2::2:2 を指定します。

<Switch> system-view

[Switch] sftp client ipv6 source ipv6 2:2::2:2

関連コマンド

display sftp client source

10.2.23 sftp client source

Syntax

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

undo sftp client source

デフォルト

SFTP パケットの送信元 IP アドレスは設定されていません。SFTP パケットは送信元アドレスとして、ルーティングエントリで指定された送信インタフェースのプライマリ IP アドレスを使用します。

View

System view

定義済みユーザロール

network-admin

パラメータ

interface *interface-type interface-number*: 送信元インタフェースのタイプと番号を指定します。SFTP パケットは送信元アドレスとしてインタフェースのプライマリ IP アドレスを使用します。

ip *ip-address*: 送信元 IPv4 アドレスを指定します。

説明

sftp client source コマンドは SFTP パケットの送信元 IPv4 アドレスを指定します。

undo sftp client source コマンドはデフォルトに戻します。

このコマンドはすべての SFTP 接続に適用します。**sftp** コマンドで指定された送信元 IP アドレスは、現在の SFTP 接続のみ適用します。このコマンドと **sftp** コマンドの両方で送信元 IP アドレスが指定された場合、**sftp** コマンドで指定された送信元 IP アドレスが適用されます。

このコマンドを複数実行した場合、最後に行われた設定が適用されます。

例

SFTP パケットの送信元 IP アドレスとして 192.168.0.1 を指定します。

<Switch> system-view

[Switch] sftp client source ip 192.168.0.1

関連コマンド

display sftp client source

10.2.24 sftp ipv6

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* }] *

View

User view

定義済みユーザロール

network-admin

パラメータ

server: IPv6 アドレスあるいはホスト名でサーバを指定します。設定範囲は 1～253 文字です。大文字、小文字を区別しません。

port-number: サーバのポート番号を指定します。設定範囲は 1～65535 です。デフォルトは 22 です。

vpn-instance *vpn-instance-name*: サーバが属する VPN インスタンスを指定します。大文字小文字を区別し、設定範囲は 1～31 文字です。

-i *interface-type interface-number*: IPv6 SFTP パケットを送信するインタフェースのタイプと番号を指定します。指定された送信インタフェースはリンクローカルにする必要があります。このパラメータはサーバがクライアントの SFTP サービスを提供するため、リンクローカルアドレスを使用しているときのみ使用します。

identity-key: クライアントの公開鍵アルゴリズムを指定します。サーバが公開鍵認証を使用する場合、指定する必要があります。クライアントはアルゴリズムに関連したローカル秘密鍵を使用してデジタル署名を作成します。

- **dsa**: 公開鍵アルゴリズム dsa を指定します。
- **rsa**: 公開鍵アルゴリズム rsa を指定します。

prefer-compress: サーバとクライアント間で優先される圧縮アルゴリズムを指定します。

zlib: 圧縮アルゴリズム zlib を指定します。

prefer-ctos-cipher: クライアントからサーバへの優先される暗号化アルゴリズムを指定します。アルゴリズム **des-cbc**、**3des-cbc**、**aes128-cbc** の順番でセキュリティの強度が強くなり、計算時間が長くなります。

- **3des-cbc**: 暗号化アルゴリズム 3des-cbc を指定します。
- **aes128-cbc**: 暗号化アルゴリズム aes128-cbc を指定します。
- **des-cbc**: 暗号化アルゴリズム des-cbc を指定します。

prefer-ctos-hmac: クライアントからサーバへの優先される HMAC アルゴリズムを指定します。アルゴリズム **md5**、**md5-96**、**sha1**、**sha1-96** の順番でセキュリティの強度が強くなり、計算時間が長くなります。

- **md5:** HMAC アルゴリズム hmac-md5 を指定します。

- **md5-96:** HMAC アルゴリズム hmac-md5-96 を指定します。
- **sha1:** HMAC アルゴリズム hmac-sha1 を指定します。
- **sha1-96:** HMAC アルゴリズム hmac-sha1-96 を指定します。

prefer-kex: 優先される鍵交換アルゴリズムを指定します。アルゴリズム **dh-group-exchange-sha1**、**dh-group1-sha1**、**dh-group14-sha1** の順番でセキュリティの強度が強くなり、計算時間が長くなります。

- **dh-group-exchange-sha1**: 鍵交換アルゴリズム diffie-hellman-group-exchange-sha1 を指定します。
- **dh-group1-sha1**: 鍵交換アルゴリズム diffie-hellman-group1-sha1 を指定します。
- **dh-group14-sha1**: 鍵交換アルゴリズム diffie-hellman-group14-sha1 を指定します。

prefer-stoc-cipher: サーバからクライアントへの優先される暗号化アルゴリズムを指定します。サポートするアルゴリズムは **prefer-ctos-cipher** 暗号化アルゴリズムと同一にしてください。

prefer-stoc-hmac: サーバからクライアントへの優先される HMAC アルゴリズムを指定します。サポートするアルゴリズムは **prefer-ctos-hmac** 暗号化アルゴリズムと同一にしてください。

dscp *dscp-value*: SFTP クライアントによって送信される IPv4 SFTP パケットの DSCP を指定します。設定範囲は 0～63 です。デフォルトは 48 です。DSCP の値はパケットを送信するプライオリティに影響します。

public-key *keyname*: サーバを認証するためにクライアントが使用するサーバのホスト公開鍵を指定します。設定範囲は 1～64 文字です。

source: IPv6 SFTP パケットの送信元 IPv6 アドレスあるいは送信元インタフェースを指定します。デフォルトで SFTP パケットは RFC3484 で定義された送信元アドレスとして、自動で選択された IPv6 アドレスを選択します。IPv6 SFTP 接続を正しく行うため、送信元インタフェースとしてループバックインタフェースを指定する、あるいは送信元 IPv6 アドレスとしてループバックインタフェースの IPv6 アドレスを指定します。

- **interface** *interface-type interface-number*: 送信元インタフェースのタイプと番号を指定します。インタフェースの IPv6 アドレスは SFTP パケットの送信元 IPv6 アドレスです。
- **ipv6** *ipv6-address*: 送信元 IPv6 アドレスを指定します。

説明

sftp ipv6 コマンドは IPv6 SFTP サーバとの接続を確立し、SFTP client view に移行します。

公開鍵認証では、クライアントはデジタル認証のローカルプライベート鍵を取得する必要があります。公開鍵アルゴリズムは RSA あるいは DSA アルゴリズムを使用するため、**identity-key** を使用して公開鍵アルゴリズムを指定する必要があります。クライアントは正しいローカルプライベート鍵を取得することができます。

例

IPv6 SFTP サーバ 2000::1 へ接続を確立し、サーバの公開鍵として svkey を指定します。SFTP クライアントは公開鍵認証を使用します。以下のアルゴリズムを使用します。

- 優先される鍵交換アルゴリズムは dh-group14-sha1 です。
- サーバからクライアントへの優先される暗号化アルゴリズムは aes128-cbc です。
- クライアントからサーバへの優先される HMAC アルゴリズムは sha1 です。
- サーバからクライアントへの優先される HMAC アルゴリズムは sha1-96 です。
- サーバとクライアント間で優先される圧縮アルゴリズムは zlib です。

<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

10.2.25 ssh client ipv6 source

Syntax

ssh client ipv6 source { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }

undo ssh client ipv6 source

デフォルト

SSH パケットの送信元 IPv6 アドレスは設定されていません。SSH パケットは RFC3484 で定義された送信元アドレスとして、自動で選択された IPv6 アドレスを選択します。

View

System view

定義済みユーザロール

network-admin

パラメータ

interface *interface-type interface-number*: 送信元インタフェースのタイプと番号を指定します。SSH パケットは送信元アドレスとして指定されたインタフェースで、ロンゲストマッチの IPv6 アドレスを使用します。

ipv6 *ipv6-address*: 送信元 IPv6 アドレスを指定します。

説明

ssh client ipv6 source コマンドは Stelnet クライアントが送信する SSH パケットの送信元 IPv6 アドレスを指定します。

undo ssh client ipv6 source コマンドはデフォルトに戻します。

このコマンドはすべての IPv6 Stelnet 接続に適用します。**ssh2 ipv6** コマンドで指定された送信元 IPv6 アドレスは、現在の IPv6 Stelnet 接続のみ適用します。このコマンドと **ssh2**

ipv6 コマンドの両方で送信元 IPv6 アドレスが指定された場合、**ssh2 ipv6** コマンドで指定された送信元 IPv6 アドレスが適用されます。

このコマンドを複数実行した場合、最後に行われた設定が適用されます。

例

Stelnet クライアントが SSH パケットの送信元 IPv6 アドレスとして 2:2::2:2 を指定します。

<Switch> system-view

[Switch] ssh client ipv6 source ipv6 2:2::2:2

関連コマンド

display ssh client source

10.2.26 ssh client source

Syntax

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

undo ssh client source

デフォルト

SSH パケットの送信元 IP アドレスは設定されていません。SSH パケットは送信元アドレスとして、ルーティングエントリで指定された送信インタフェースのプライマリ IP アドレスを使用します。

View

System view

定義済みユーザロール

network-admin

パラメータ

interface *interface-type interface-number*: 送信元インタフェースのタイプと番号を指定します。SSH パケットは送信元アドレスとしてインタフェースのプライマリ IP アドレスを使用します。

ip *ip-address*: 送信元 IPv4 アドレスを指定します。

説明

ssh client source コマンドは Stelnet クライアントが送信する SSH パケットの送信元 IPv4 アドレスを指定します。

undo ssh client source コマンドはデフォルトに戻します。

このコマンドはすべての Stelnet 接続に適用します。**ssh2** コマンドで指定された送信元 IP アドレスは、現在の Stelnet 接続のみ適用します。このコマンドと **ssh2** コマンドの両方で送信元 IP アドレスが指定された場合、**ssh2** コマンドで指定された送信元 IP アドレスが適用されます。

このコマンドを複数実行した場合、最後に行われた設定が適用されます。

例

SSH パケットの送信元 IPv4 アドレスとして 192.168.0.1 を指定します。

<Switch> system-view

[Switch] ssh client source ip 192.168.0.1

関連コマンド

display ssh client source

10.2.27 ssh2

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* }] *

View

User view

定義済みユーザロール

network-admin

パラメータ

server: IPv4 アドレスあるいはホスト名でサーバを指定します。設定範囲は 1～253 文字です。大文字、小文字を区別しません。

port-number: サーバのポート番号を指定します。設定範囲は 1～65535 です。デフォルトは 22 です。

vpn-instance *vpn-instance-name*: サーバが属する VPN インスタンスを指定します。大文字小文字を区別し、設定範囲は 1～31 文字です。

identity-key: クライアントの公開鍵アルゴリズムを指定します。サーバが公開鍵認証を使用する場合、指定する必要があります。クライアントはアルゴリズムに関連したローカル秘密鍵を使用してデジタル署名を作成します。

- **dsa**: 公開鍵アルゴリズム dsa を指定します。
- **rsa**: 公開鍵アルゴリズム rsa を指定します。

prefer-compress: サーバとクライアント間で優先される圧縮アルゴリズムを指定します。

zlib: 圧縮アルゴリズム zlib を指定します。

prefer-ctos-cipher: クライアントからサーバへの優先される暗号化アルゴリズムを指定します。アルゴリズム **des-cbc**、**3des-cbc**、**aes128-cbc** の順番でセキュリティの強度が強くなり、計算時間が長くなります。

- **3des-cbc**: 暗号化アルゴリズム 3des-cbc を指定します。
- **aes128-cbc**: 暗号化アルゴリズム aes128-cbc を指定します。
- **des-cbc**: 暗号化アルゴリズム des-cbc を指定します。

prefer-ctos-hmac: クライアントからサーバへの優先される HMAC アルゴリズムを指定します。アルゴリズム **md5**、**md5-96**、**sha1**、**sha1-96** の順番でセキュリティの強度が強くなり、計算時間が長くなります。

- **md5:** HMAC アルゴリズム hmac-md5 を指定します。
- **md5-96:** HMAC アルゴリズム hmac-md5-96 を指定します。
- **sha1:** HMAC アルゴリズム hmac-sha1 を指定します。
- **sha1-96:** HMAC アルゴリズム hmac-sha1-96 を指定します。

prefer-kex: 優先される鍵交換アルゴリズムを指定します。アルゴリズム **dh-group-exchange-sha1**、**dh-group1-sha1**、**dh-group14-sha1** の順番でセキュリティの強度が強くなり、計算時間が長くなります。

- **dh-group-exchange-sha1**: 鍵交換アルゴリズム diffie-hellman-group-exchange-sha1 を指定します。
- **dh-group1-sha1**: 鍵交換アルゴリズム diffie-hellman-group1-sha1 を指定します。
- **dh-group14-sha1**: 鍵交換アルゴリズム diffie-hellman-group14-sha1 を指定します。

prefer-stoc-cipher: サーバからクライアントへの優先される暗号化アルゴリズムを指定します。サポートするアルゴリズムは **prefer-ctos-cipher** 暗号化アルゴリズムと同一にしてください。

prefer-stoc-hmac: サーバからクライアントへの優先される HMAC アルゴリズムを指定します。サポートするアルゴリズムは **prefer-ctos-hmac** 暗号化アルゴリズムと同一にしてください。

dscp *dscp-value*: IPv4 SSH パケットの DSCP を指定します。設定範囲は 0～63 です。デフォルトは 48 です。DSCP の値はパケットを送信するプライオリティに影響します。

escape *character*: Stelnet 接続を切断するための文字を指定します。デフォルトはチルダ（~）です。

public-key *keyname*: サーバのホスト公開鍵を指定します。サーバを認証するために使用します。設定範囲は 1～64 です。大文字、小文字を区別しません。

source: SSH パケットの送信元 IP アドレスあるいは送信元インタフェースを指定します。デフォルトで SSH パケットは送信元アドレスとして、ルーティングエントリで指定された送信インタフェースのプライマリ IP アドレスを使用します。Stelnet 接続を正しく行うため、送信元インタフェースとしてループバックインタフェースを指定する、あるいは送信元 IPv4 アドレスとしてループバックインタフェースの IPv4 アドレスを指定します。

- **interface** *interface-type interface-number*: 送信元インタフェースのタイプと番号を指定します。インタフェースのプライマリ IPv4 アドレスは SSH パケットの送信元 IP アドレスです。
- **ip** *ip-address*: 送信元 IPv4 アドレスを指定します。

説明

ssh2 コマンドは IPv4 Stelnet サーバとの接続を確立します。

escape *character* パラメータとドット（.）の組み合わせは、エスケープシーケンスとして働きます。このエスケープシーケンスは、一般に、サーバが再起動や例外的な挙動をするときに SSH 接続を素早く切断します。

エスケープシーケンスを適用するには、ラインのその最初に入力しなければなりません。ラインに他の文字を入力したり、操作を実行した場合、次のラインにエスケープシーケンスを入力してください。

escape *character* パラメータにはデフォルトの（~）を使用することを推奨します。SSH ユーザ名として別の文字を使用しないでください。

例

IPv4 Stelnet サーバ 3.3.3.3 へ接続を確立し、サーバの公開鍵として svkey を指定します。Stelnet クライアントは公開鍵認証を使用します。**escape** *character* として（$）を指定します。以下のアルゴリズムを使用します。

- 優先される鍵交換アルゴリズムは dh-group14-sha1 です。
- サーバからクライアントへの優先される暗号化アルゴリズムは aes128-cbc です。
- クライアントからサーバへの優先される HMAC アルゴリズムは sha1 です。
- サーバからクライアントへの優先される HMAC アルゴリズムは sha1-96 です。
- サーバとクライアント間で優先される圧縮アルゴリズムは zlib です。

<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 $

10.2.28 ssh2 ipv6

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* }] *

View

User view

定義済みユーザロール

network-admin

パラメータ

server: IPv6 アドレスあるいはホスト名でサーバを指定します。設定範囲は 1～253 文字です。大文字、小文字を区別しません。

port-number: サーバのポート番号を指定します。設定範囲は 1～65535 です。デフォルトは 22 です。

vpn-instance *vpn-instance-name*: サーバが属する VPN インスタンスを指定します。大文字、小文字を区別し、設定範囲は 1～31 文字です。

-i *interface-type interface-number*: IPv6 SSH パケットを送信するインタフェースのタイプと番号を指定します。指定された送信インタフェースはリンクローカルにする必要があります。このパラメータはサーバが Stelnet クライアントの SSH サービスを提供するため、リンクローカルアドレスを使用しているときのみ使用します。

identity-key: クライアントの公開鍵アルゴリズムを指定します。サーバが公開鍵認証を使用する場合、指定する必要があります。クライアントはアルゴリズムに関連したローカル秘密鍵を使用してデジタル署名を作成します。

- **dsa**: 公開鍵アルゴリズム dsa を指定します。
- **rsa**: 公開鍵アルゴリズム rsa を指定します。

prefer-compress: サーバとクライアント間で優先される圧縮アルゴリズムを指定します。

zlib: 圧縮アルゴリズム zlib を指定します。

prefer-ctos-cipher: クライアントからサーバへの優先される暗号化アルゴリズムを指定します。アルゴリズム **des-cbc**、**3des-cbc**、**aes128-cbc** の順番でセキュリティの強度が強くなり、計算時間が長くなります。

- **3des-cbc**: 暗号化アルゴリズム 3des-cbc を指定します。
- **aes128-cbc**: 暗号化アルゴリズム aes128-cbc を指定します。
- **des-cbc**: 暗号化アルゴリズム des-cbc を指定します。

prefer-ctos-hmac: クライアントからサーバへの優先される HMAC アルゴリズムを指定します。アルゴリズム **md5**、**md5-96**、**sha1**、**sha1-96** の順番でセキュリティの強度が強くなり、計算時間が長くなります。

- **md5:** HMAC アルゴリズム hmac-md5 を指定します。
- **md5-96:** HMAC アルゴリズム hmac-md5-96 を指定します。
- **sha1:** HMAC アルゴリズム hmac-sha1 を指定します。
- **sha1-96:** HMAC アルゴリズム hmac-sha1-96 を指定します。

prefer-kex: 優先される鍵交換アルゴリズムを指定します。アルゴリズム **dh-group-exchange-sha1**、**dh-group1-sha1**、**dh-group14-sha1** の順番でセキュリティの強度が強くなり、計算時間が長くなります。

- **dh-group-exchange-sha1**: 鍵交換アルゴリズム diffie-hellman-group-exchange-sha1 を指定します。
- **dh-group1-sha1**: 鍵交換アルゴリズム diffie-hellman-group1-sha1 を指定します。
- **dh-group14-sha1**: 鍵交換アルゴリズム diffie-hellman-group14-sha1 を指定します。

prefer-stoc-cipher: サーバからクライアントへの優先される暗号化アルゴリズムを指定します。サポートするアルゴリズムは **prefer-ctos-cipher** 暗号化アルゴリズムと同一にしてください。

prefer-stoc-hmac: サーバからクライアントへの優先される HMAC アルゴリズムを指定します。サポートするアルゴリズムは **prefer-ctos-hmac** 暗号化アルゴリズムと同一にしてください。

dscp *dscp-value*: SFTP クライアントによって送信される IPv6 SSH パケットの DSCP を指定します。設定範囲は 0～63 です。デフォルトは 48 です。DSCP の値はパケットを送信するプライオリティに影響します。

escape *character*: Stelnet 接続を切断するための文字を指定します。デフォルトはチルダ（~）です。

public-key *keyname*: サーバのホスト公開鍵を指定します。サーバを認証するために使用します。設定範囲は 1～64 文字です。大文字、小文字を区別しません。

source: IPv6 SSH パケットの送信元 IPv6 アドレスあるいは送信元インタフェースを指定します。デフォルトで IPv6 SSH パケットは RFC3484 で定義された送信元アドレスとして、自動で選択された IPv6 アドレスを選択します。IPv6 Stelnet 接続を正しく行うため、送信元インタフェースとしてループバックインタフェースを指定する、あるいは送信元 IPv6 アドレスとしてループバックインタフェースの IPv6 アドレスを指定します。

- **interface** *interface-type interface-number*: 送信元インタフェースのタイプと番号を指定します。インタフェースの IPv6 アドレスは SSH パケットの送信元 IPv6 アドレスです。
- **ipv6** *ipv6-address*: 送信元 IPv6 アドレスを指定します。

説明

ssh2 ipv6 コマンドは IPv6 Stelnet サーバとの接続を確立します。

escape *character* パラメータとドット（.）の組み合わせは、エスケープシーケンスとして働きます。このエスケープシーケンスは、一般に、サーバが再起動や例外的な挙動をするときに SSH 接続を素早く切断します。

エスケープシーケンスを適用するには、ラインのその最初に入力しなければなりません。ラインに他の文字を入力したり、操作を実行した場合、次のラインにエスケープシーケンスを入力してください。

escape *character* パラメータにはデフォルトの（~）を使用することを推奨します。SSH ユーザ名として別の文字を使用しないでください。

例

IPv6 Stelnet サーバ 2000::1 へ接続を確立し、サーバの公開鍵として svkey を指定します。Stelnet クライアントは公開鍵認証を使用します。以下のアルゴリズムを使用します。エスケープ *character* パラメータは（$）を使用します。

- 優先される鍵交換アルゴリズムは dh-group14-sha1 です。
- サーバからクライアントへの優先される暗号化アルゴリズムは aes128-cbc です。
- クライアントからサーバへの優先される HMAC アルゴリズムは sha1 です。
- サーバからクライアントへの優先される HMAC アルゴリズムは sha1-96 です。
- サーバとクライアント間で優先される圧縮アルゴリズムは zlib です。

<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 $

目次

このセクションのページは **9-x-x** です。

11 章 SSL.....11-1
11.1 SSL 設定コマンド 11-1
11.1.1 security-enhanced level.....11-1

11章 SSL

SSL の設定に関するコンフィグについては、別紙の共通マニュアル“*QX シリーズ Ethernet スイッチ Web 認証コマンドマニュアル*（V7）”の“*SSL*”を参照してください。

11.1 SSL設定コマンド

11.1.1 security-enhanced level

Syntax

security-enhanced level 1

undo security-enhanced level

デフォルト

レベル 1

View

System view

定義済みユーザロール

network-admin

パラメータ

level-value: セキュリティ強化レベルを指定します。QX-S5100G シリーズはレベル 1 のみをサポートします。

説明

装置のセキュリティ強化レベルを 1 にすることができます。

- SSL クライアントポリシーと SSL サーバポリシーは、DES、3 DES、MD 5、RC 4、RC 2 を含む暗号スイートをサポートします。
- SSL クライアントポリシーと SSL サーバポリシーは、TLS 1.1 より前の SSL プロトコルバージョンをサポートします。
- SSL セッションの再ネゴシエーションを有効にできます。

例

装置のセキュリティ強化レベルを 1 に設定する。

<Sysname> system-view

[Sysname] security-enhanced level 1

目次

このセクションのページは **9-x-x** です。

12 章 TCP フラグメントアタックプロテクション.....12-1
12.1 TCP フラグメントアタックプロテクション設定コマンド.....12-1
12.1.1 attack-defense tcp fragment enable 12-1

12章 TCP フラグメントアタックプロテクション

12.1 TCPフラグメントアタックプロテクション設定コマンド

12.1.1 attack-defense tcp fragment enable

Syntax

attack-defense tcp fragment enable

undo attack-defense tcp fragment enable

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

attack-defense tcp fragment enable コマンドは TCP フラグメントアタックプロテクションを有効にします。

undo attack-defense tcp fragment enable コマンドは TCP フラグメントアタックプロテクションを無効にします。

このコマンドは TCP フラグメント攻撃を防ぐために、パケットフィルタ機能で検出できない TCP フラグメント攻撃のパケットを廃棄します。RFC1858 で定義されています。TCP フラグメントアタックプロテクションは以下の TCP フラグメントを調査します。

- TCP ヘッダが 20 バイトよりも小さい、最初のフラグメント
- 8 バイトのフラグメントオフセット（FO=1）の 2 番目以降のフラグメント

例

TCP フラグメントアタックプロテクションを有効にします。

<Switch> system-view

[Switch] attack-defense tcp fragment enable

目次

このセクションのページは **9-x-x** です。

13 章 IP ソースガード.....13-1
13.1 IP ソースガード設定コマンド.....13-1
13.1.1 display ip source binding.....13-1
13.1.2 display ipv6 source binding.....13-3
13.1.3 ip source binding (interface view).....13-5
13.1.4 ip verify source.....13-7
13.1.5 ipv6 source binding (interface view).....13-8
13.1.6 ipv6 verify source.....13-9

13章 IP ソースガード

13.1 IPソースガード設定コマンド

13.1.1 display ip source binding

Syntax

display ip source binding [**static** | [**arp-snooping-vlan** | **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*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

static: スタティック IPv4 ソースガードバインディングエントリを表示します。

arp-snooping-vlan: VLAN の ARP snooping をもとにした IPv4 ソースガードバインディングを指定します。

dhcp-relay: DHCP リレーをもとにしたダイナミック IPv4 ソースガードバインディングエントリを指定します。

dhcp-server: DHCP サーバをもとにしたダイナミック IPv4 ソースガードバインディングエントリを指定します。

dhcp-snooping: DHCP snooping をもとにしたダイナミック IPv4 ソースガードバインディングエントリを指定します。

ip-address *ip-address*: IPv4 アドレスの IP ソースガードバインディングエントリを指定します。

mac-address *mac-address*: MAC アドレスの IP ソースガードバインディングエントリを指定します。MAC アドレスの形式は H-H-H です。

vlan *vlan-id*: VLAN の IP ソースガードバインディングエントリを指定します。VLAN ID の設定範囲は 1～4094 です。

interface *interface-type interface-number*: インタフェースの IPv4 ソースガードバインディングエントリを指定します。*interface-type* と *interface-number* はインタフェースのタイプと番号を指定します。

slot *slot-number*: IRF スタックメンバ装置の ID を指定します。指定しない場合、マスタ装置の IP ソースガードバインディングエントリを表示します。

説明

display ip source binding コマンドは IPv4 ソースガードバインディングエントリを表示します。

例

パブリックネットワークのすべての IPv4 ソースガードバインディングエントリを表示します。

<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
```

表 13-1 コマンド出力

フィールド	説明
Total entries found	IPv4ソースガードバインディングエントリの総数です。
IP Address	IPv4ソースガードバインディングエントリのIPv4アドレスです。エントリにIPv4アドレスが割り当てられていない場合、**N/A**と表示されます。
MAC Address	IPv4ソースガードバインディングエントリのMACアドレスです。エントリにMACアドレスが割り当てられていない場合、**N/A**と表示されます。
Interface	IPv4ソースガードバインディングエントリのインタフェースです。エントリがグローバルIPv4ソースガードバインディングエントリである場合、**N/A**と表示されます。
VLAN	IPv4ソースガードバインディングエントリのVLAN情報です。エントリにVLAN情報がない場合、**N/A**と表示されます。

フィールド	説明
Type	IPv4ソースガードバインディングエントリのタイプです。 ● **Static**—手動で設定されました。バインディングはIPソースガードのパケットフィルタリングに使われます。あるいはセキュリティサービスを提供するためほかのモジュールで使用されます。 ● **ARP snooping**— ARP snoopingエントリをもとにダイナミックに作成されました。バインディングはIPソースガードのパケットフィルタリングに使われます。 ● **802.1X**—802.1Xエントリをもとにダイナミックに作成されました。バインディングはIPソースガードのパケットフィルタリングに使われます。このフィールドはサポートしていません。 ● **DHCP relay**—DHCPリレーエントリをもとにダイナミックに作成されました。バインディングはIPソースガードのパケットフィルタリングに使われます。 ● **DHCP server**—DHCPサーバエントリをもとにダイナミックに作成されました。バインディングはIPソースガードのパケットフィルタリングに使われます。あるいはセキュリティサービスを提供するためほかのモジュールで使用されます。 ● **DHCP snooping**—DHCP snoopingエントリをもとにダイナミックに作成されました。バインディングはIPソースガードのパケットフィルタリングに使われます。

関連コマンド

- **ip source binding**
- **ip verify source**

13.1.2 display ipv6 source binding

Syntax

display ipv6 source binding [**static**] [**ip-address** *ipv6-address*] [**mac-address** *mac-address*] [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

static: スタティック IPv6 ソースガードバインディングエントリを表示します。

ip-address *ipv6-address*: IPv6 アドレスの IPv6 ソースガードバインディングエントリを表示します。

mac-address *mac-address*: MAC アドレスの IPv6 ソースガードバインディングエントリを表示します。MAC アドレスの形式は H-H-H です。

vlan *vlan-id*: VLAN の IPv6 ソースガードバインディングエントリを表示します。VLAN ID の設定範囲は 1～4094 です。

interface *interface-type interface-number*: インタフェースの IPv6 ソースガードバインディングエントリを表示します。*interface-type* と *interface-number* はインタフェースのタイプと番号を指定します。

slot *slot-number*: IRF スタックメンバ装置の ID を指定します。指定しない場合、マスタ装置の IPv6 ソースガードバインディングエントリを表示します。

説明

display ipv6 source binding コマンドは IPv6 ソースガードバインディングエントリを表示します。

例

パブリックネットワークのすべての IPv6 ソースガードバインディングエントリを表示します。

<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
```

表 13-2 コマンド出力

フィールド	説明
Total entries found	IPv6ソースガードバインディングエントリの総数です。
IPv6 Address	IPv6ソースガードバインディングエントリのIPv6アドレスです。エントリにIPv6アドレスが割り当てられていない場合、**N/A**と表示されます。

フィールド	説明
MAC Address	IPv6ソースガードバインディングエントリのMACアドレスです。エントリにMACアドレスが割り当てられていない場合、**N/A**と表示されます。
Interface	IPv6ソースガードバインディングエントリのインタフェースです。エントリがグローバルIPv6ソースガードバインディングエントリである場合、**N/A**と表示されます。
VLAN	IPv6ソースガードバインディングエントリのVLAN情報です。エントリにVLAN情報がない場合、**N/A**と表示されます。
Type	IPv6ソースガードバインディングエントリのタイプです。 • **Static**—手動で設定されました。バインディングはIPソースガードのパケットフィルタリングに使われます。あるいはセキュリティサービスを提供するためほかのモジュールで使用されます。 • **DHCPv6 snooping**—DHCPv6 snoopingエントリをもとにダイナミックに作成されました。バインディングはIPソースガードのパケットフィルタリングに使われます。 • **802.1X**—802.1Xエントリをもとにダイナミックに作成されました。バインディングはIPソースガードのパケットフィルタリングに使われます。このフィールドはサポートしていません。

関連コマンド

- **ipv6 source binding**
- **ipv6 verify source**

13.1.3 ip source binding (interface view)

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*]

デフォルト

設定なし

View

Layer 2 Ethernet interface view

VLAN interface view

定義済みユーザロール

network-admin

パラメータ

all: インタフェースのすべてのスタティック IPv4 ソースガードバインディングエントリを削除します。

ip-address *ip-address*: スタティックバインディングエントリの IPv4 アドレスを指定します。IPv4 アドレスは、クラス A、クラス B、クラス C にする必要があります。127.x.x.x、0.0.0.0 は指定することができません。

mac-address *mac-address*: スタティックバインディングエントリの MAC アドレスを指定します。MAC アドレスの形式は H-H-H です。すべてが 0 のアドレス、すべてが F のアドレス（ブロードキャスト MAC アドレス）、マルチキャスト MAC アドレスは指定することができません。

vlan *vlan-id*: スタティックバインディングエントリの VLAN ID を指定します。設定範囲は 1～4094 です。Layer 2 Ethernet interface view でのみサポートしています。

説明

ip source binding コマンドはインタフェースのスタティック IPv4 ソースガードバインディングエントリを設定します。

undo ip source binding コマンドはインタフェースのスタティック IPv4 ソースガードバインディングエントリを削除します。

IP ソースガードは、以下の機能を実装するため、インタフェースのスタティック IPv4 ソースガードバインディングエントリを使用することができます。

- インタフェースの受信 IPv4 パケットをフィルタします。
- ARP 検出機能と連携してユーザの妥当性を確認します。

例

IP アドレスが 192.168.0.1、MAC アドレスが 0001-0001-0001 のスタティック IPv4 ソースガードバインディングエントリを GigabitEthernet 1/0/1 に割り当てます。

<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

関連コマンド

display ip source binding

13.1.4 ip verify source

Syntax

ip verify source { **ip-address** | **ip-address mac-address** | **mac-address** }

undo ip verify source

デフォルト

無効

View

Layer 2 Ethernet interface view

VLAN interface view

定義済みユーザロール

network-admin

パラメータ

ip-address: 送信元 IPv4 アドレスによって受信パケットをフィルタします。

ip-address mac-address: 送信元 IPv4 アドレスと送信元 MAC アドレスによって受信パケットをフィルタします。

mac-address: 送信元 MAC アドレスによって受信パケットをフィルタします。

説明

ip verify source コマンドは IPv4 ソースガード機能を有効にします。

undo ip verify source コマンドはデフォルトに戻します。

インタフェースで IPv4 ソースガードを有効にしたのち、スタティック IPv4 ソースガードバインディングとダイナミック IPv4 ソースガードバインディングをインタフェースから受信したパケットに一致させます。IPv4 ソースガードバインディングに一致するパケットは転送され、一致しないパケットは廃棄されます。

このコマンドの一致条件は、ダイナミック IP ソースガードにのみ適用されます。スタティック IPv4 ソースガードは、**ip source binding** コマンドを使用することで設定されたスタティックバインディングエントリを使用します。

例

レイヤ 2 Ethernet インタフェース GigabitEthernet 1/0/1 で IPv4 ソースガード機能を有効にします。ダイナミック IP ソースガード機能で送信元 IPv4 アドレスと送信元 MAC アドレスによって受信パケットをフィルタします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] ip verify source ip-address mac-address

VLAN インタフェース 100 で IPv4 ソースガードを有効にします。ダイナミック IP ソースガード機能で送信元 IPv4 アドレスと送信元 MAC アドレスによって受信パケットをフィルタします。

<Switch> system-view

[Switch] interface vlan-interface 100

[Switch-Vlan-interface100] ip verify source ip-address mac-address

関連コマンド

display ip source binding

13.1.5 ipv6 source binding (interface view)

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*]

デフォルト

設定なし

View

Layer 2 Ethernet interface view

VLAN interface view

定義済みユーザロール

network-admin

パラメータ

all: インタフェースのすべてのスタティック IPv6 ソースガードバインディングエントリを削除します。

ip-address *ipv6-address*: スタティックバインディングエントリの IPv6 アドレスを指定します。すべてが 0 のアドレス、マルチキャストアドレス、ループバックアドレスは指定することができません。

mac-address *mac-address*: スタティックバインディングエントリの MAC アドレスを指定します。MAC アドレスの形式は H-H-H です。すべてが 0 のアドレス、すべてが F のアドレス（ブロードキャスト MAC アドレス）、マルチキャスト MAC アドレスは指定することができません。

vlan *vlan-id*: スタティックバインディングエントリの VLAN ID を指定します。設定範囲は 1～4094 です。Layer 2 Ethernet interface view でのみサポートしています。

説明

ipv6 source binding コマンドはインタフェースのスタティック IPv6 ソースガードバインディングエントリを設定します。

undo ipv6 source binding コマンドはインタフェースに設定されたスタティック IPv6 ソースガードバインディングエントリを削除します。

IP ソースガードは、インタフェースの受信 IPv6 パケットをフィルタするため、インタフェースのスタティック IPv6 ソースガードバインディングエントリを使用することができます。

例

IPv6 アドレスが 2001::1、MAC アドレスが 0002-0002-0002 のスタティック IPv6 ソースガードバインディングエントリを GigabitEthernet 1/0/1 に割り当てます。

<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

関連コマンド

display ipv6 source binding

13.1.6 ipv6 verify source

Syntax

ipv6 verify source { **ip-address** | **ip-address mac-address** | **mac-address** }

undo ipv6 verify source

デフォルト

無効

View

Layer 2 Ethernet interface view

VLAN interface view

定義済みユーザロール

network-admin

パラメータ

ip-address: 送信元 IPv6 アドレスによって受信パケットをフィルタします。

ip-address mac-address: 送信元 IPv6 アドレスと送信元 MAC アドレスによって受信パケットをフィルタします。

mac-address: 送信元 MAC アドレスによって受信パケットをフィルタします。

説明

ipv6 verify source コマンドは IPv6 ソースガード機能を有効にします。

undo ipv6 verify source コマンドはデフォルトに戻します。

インタフェースで IPv6 ソースガードを有効にしたのち、スタティック IPv6 ソースガードバインディングとダイナミック IPv6 ソースガードバインディングをインタフェースから受信したパケットに一致させます。IPv6 ソースガードバインディングに一致するパケットは転送され、一致しないパケットは廃棄されます。

このコマンドの一致条件は、ダイナミック IPv6 ソースガードにのみ適用されます。スタティック IPv6 ソースガードは、**ipv6 source binding** コマンドを使用することで設定されたスタティックバインディングエントリを使用します。

例

レイヤ 2 Ethernet インタフェース GigabitEthernet 1/0/1 で IPv6 ソースガード機能を有効にします。ダイナミック IPv6 ソースガード機能で送信元 IPv6 アドレスと送信元 MAC アドレスによって受信パケットをフィルタします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] ipv6 verify source ip-address mac-address

関連コマンド

display ipv6 source binding

目次

このセクションのページは **9-x-x** です。

14 章 ARP アタックプロテクション.....14-1
14.1 宛先不明の IP アタックプロテクション設定コマンド.....14-1
14.1.1 arp resolving-route enable.....14-1
14.1.2 arp resolving-route probe-count.....14-2
14.1.3 arp resolving-route probe-interval.....14-2
14.1.4 arp source-suppression enable.....14-3
14.1.5 arp source-suppression limit.....14-4
14.1.6 display arp source-suppression.....14-5
14.2 ARP パケットレートリミット設定コマンド.....14-6
14.2.1 arp rate-limit.....14-6
14.2.2 arp rate-limit log enable.....14-6
14.2.3 arp rate-limit log interval.....14-7
14.2.4 snmp-agent trap enable arp.....14-8
14.3 送信元 MAC ベース ARP アタック detection 設定コマンド.....14-9
14.3.1 arp source-mac.....14-9
14.3.2 arp source-mac aging-time.....14-10
14.3.3 arp source-mac exclude-mac.....14-11
14.3.4 arp source-mac threshold.....14-12
14.3.5 display arp source-mac.....14-12
14.4 ARP パケット送信元 MAC アドレス整合性チェック設定コマンド.....14-13
14.4.1 arp valid-check enable.....14-13
14.5 ARP 確認応答設定コマンド.....14-14
14.5.1 arp active-ack enable.....14-14
14.6 ARP アタック検出設定コマンド.....14-15
14.6.1 arp detection enable.....14-15
14.6.2 arp detection log enable.....14-16
14.6.3 arp detection trust.....14-16
14.6.4 arp detection validate.....14-17
14.6.5 arp restricted-forwarding enable.....14-18
14.6.6 display arp detection.....14-19
14.6.7 display arp detection statistics.....14-19
14.6.8 display arp detection statistics attack-source.....14-21
14.6.9 display arp detection statistics packet-drop.....14-22
14.6.10 reset arp detection statistics.....14-23
14.6.11 reset arp detection statistics attack-source.....14-24
14.6.12 reset arp detection statistics packet-drop.....14-25

14.7 ARP スキャンおよび固定 ARP 設定コマンド 14-25
14.7.1 arp scan 14-25
14.8 ARP ゲートウェイプロテクション設定コマンド 14-27
14.8.1 arp filter source 14-27
14.9 ARP フィルタリング設定コマンド 14-28
14.9.1 arp filter binding 14-28

14章 ARP アタックプロテクション

14.1 宛先不明のIPアタックプロテクション設定コマンド

14.1.1 arp resolving-route enable

Syntax

arp resolving-route enable

undo arp resolving-route enable

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

arp resolving-route enable コマンドは ARP ブラックホールルーティングを有効にします。

undo arp resolving-route enable コマンドは ARP ブラックホールルーティングを無効にします。

このコマンドはゲートウェイで設定します。

例

#ARP ブラックホールルーティングを有効にします。

<Switch> system-view

[Switch] arp resolving-route enable

関連コマンド

- **arp resolving-route probe-count**
- **arp resolving-route probe-interval**

14.1.2 arp resolving-route probe-count

Syntax

arp resolving-route probe-count *count*

undo arp resolving-route probe-count

デフォルト

1

View

System view

定義済みユーザロール

network-admin

パラメータ

count: 調査する回数を設定します。設定範囲は 1～25 です。

説明

arp resolving-route probe-count コマンドは、それぞれの宛先不明 IP アドレスに ARP ブラックホールのルートを調査する回数を設定します。

undo arp resolving-route probe-count コマンドは、デフォルトに戻します。

例

それぞれの宛先不明 IP アドレスに ARP ブラックホールのルートを 5 回調査するように設定します。

<Switch> system-view

[Switch] arp resolving-route probe-count 5

関連コマンド

- **arp resolving-route enable**
- **arp resolving-route probe-interval**

14.1.3 arp resolving-route probe-interval

Syntax

arp resolving-route probe-interval *interval*

undo arp resolving-route probe-interval

デフォルト

1 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

interval: 調査する周期を指定します。設定範囲は 1～5 秒です。

説明

arp resolving-route probe-interval コマンドは、ARP ブラックホールのルートを調査する周期を設定します。

undo arp resolving-route probe-interval コマンドは、デフォルトに戻します。

例

#ARP ブラックホールのルートを 3 秒周期で調査するよう設定します。

<Switch> system-view

[Switch] arp resolving-route probe-interval 3

関連コマンド

- **arp resolving-route enable**
- **arp resolving-route probe-count**

14.1.4 arp source-suppression enable

Syntax

arp source-suppression enable

undo arp source-suppression enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

arp source-suppression enable コマンドは ARP 送信元抑制機能を有効にします。

undo arp source-suppression enable コマンドはデフォルトに戻します。

このコマンドはゲートウェイで設定します。

例

ARP 送信元抑制機能を有効にします。

<Switch> system-view

[Switch] arp source-suppression enable

関連コマンド

display arp source-suppression

14.1.5 arp source-suppression limit

Syntax

arp source-suppression limit *limit-value*

undo arp source-suppression limit

デフォルト

10

View

System view

定義済みユーザロール

network-admin

パラメータ

limit-value: 5 秒以内に受信できる宛先不明のパケットの最大数を設定します。設定範囲は 2～1024 です。

説明

arp source-suppression limit コマンドは装置が 5 秒以内に受信できる宛先不明のパケットの最大数を設定します。

undo arp source-suppression limit コマンドはデフォルトに戻します。

ホストから 5 秒以内に宛先不明のパケットの最大数を受信した場合、装置は、5 秒が経過するまでホストからのパケットの受信を停止します。

例

5 秒以内に受信できる宛先不明のパケットの最大数を 100 に設定します。

<Switch> system-view

[Switch] arp source-suppression limit 100

関連コマンド

display arp source-suppression

14.1.6 display arp source-suppression

Syntax

display arp source-suppression

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display arp source-suppression コマンドは現在の ARP 送信元抑制機能の設定を表示します。

例

#現在の ARP 送信元抑制機能の設定を表示します。

<Switch> display arp source-suppression

```
ARP source suppression is enabled
Current suppression limit: 100
```

表 14-1 コマンド出力

フィールド	説明
Current suppression limit	5秒以内に受信できる宛先不明のパケットの最大数です。

14.2 ARPパケットレートリミット設定コマンド

14.2.1 arp rate-limit

Syntax

arp rate-limit [*pps*]

undo arp rate-limit

デフォルト

ARP パケットレートリミットは有効です。レートリミットは 100pps です。

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

pps: ARP パケットの上限を指定します。単位は pps です。設定範囲は 5～200pps です。

説明

arp rate-limit コマンドはインタフェースで ARP パケットのレートリミットを有効にし、上限を指定します。上限を超過したパケットは廃棄されます。

undo arp rate-limit コマンドは ARP パケットのレートリミットを無効にします。

arp rate-limit コマンドでパラメータを指定しない場合、デフォルトのレートリミットを適用します。

例

GigabitEthernet 1/0/1 で ARP パケットのレートリミットを有効にし、上限を 50pps に指定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] arp rate-limit 50

14.2.2 arp rate-limit log enable

Syntax

arp rate-limit log enable

undo arp rate-limit log enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

arp rate-limit log enable コマンドは ARP パケットレートリミットのロギングを有効にします。

undo arp rate-limit log enable コマンドは ARP パケットレートリミットのロギングを無効にします。

ARP パケットレートリミットのロギングが有効の場合、装置はログメッセージの送信間隔内で最大しきい値を超えた ARP パケットレートを information center に送信します。ログ出力ルールを設定するように information center モジュールを設定できます。詳細は、セクション 11 *システム管理 オペレーションマニュアル*を参照してください。

例

#ARP パケットレートリミットのロギングを有効にします。

<Switch> system-view

[Switch] arp rate-limit log enable

14.2.3 arp rate-limit log interval

Syntax

arp rate-limit log interval *interval*

undo arp rate-limit log interval

デフォルト

インタフェースで受信された ARP パケットのレートが制限を超えた場合、装置は 60 秒ごとに通知またはログメッセージを送信します。

View

System view

定義済みユーザロール

network-admin

パラメータ

interval: 設定範囲は 1～86400 秒です。

説明

arp rate-limit log interval コマンドは ARP パケットレートリミットの通知およびログメッセージ送信間隔を設定します。

undo arp rate-limit log interval コマンドはデフォルトに戻します。

デフォルトの間隔を変更してアクティブにするには、ARP パケットレートリミットを有効にし、ARP パケットレートリミットの通知またはログメッセージの送信を有効にする必要があります。

例

インタフェースで受信するARPパケットのレートが制限を超えた場合に120秒ごとに通知とログメッセージを送信するように装置を設定します。

<Switch> system-view

[Switch] arp rate-limit log interval 120

関連コマンド

- **arp rate-limit**
- **arp rate-limit log enable**
- **snmp-agent trap enable arp**

14.2.4 snmp-agent trap enable arp

Syntax

snmp-agent trap enable arp [**rate-limit**]

undo snmp-agent trap enable arp [**rate-limit**]

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

パラメータ

rate-limit: ARP パケットのレートリミット機能を指定します。

説明

snmp-agent trap enable arp コマンドは ARP の SNMP notification を有効にします。

undo snmp-agent trap enable arp コマンドは ARP の SNMP notification を無効にします。

ARP の SNMP notification が有効である場合、装置は送信間隔内で最大しきい値を超えた ARP パケットレートを含む notification を生成します。

ARP イベント notification を正しく送信するには、装置で SNMP も設定する必要があります。

SNMP 設定についての詳細は、オペレーションマニュアルのセクション 11 *システム管理* “*SNMP*”を参照してください。

例

#ARP パケットレートリミットの SNMP notification を有効にします。

<Switch> system-view

[Switch] snmp-agent trap enable arp rate-limit

14.3 送信元MACベースARPアタックdetection設定コマンド

14.3.1 arp source-mac

Syntax

arp source-mac { **filter** | **monitor** }

undo arp source-mac [**filter** | **monitor**]

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

パラメータ

filter: フィルタモードを指定します。

monitor: モニタモードを指定します。

説明

arp source-mac コマンドは送信元 MAC アドレスにもとづいた ARP 攻撃 detection を有効にし、処理方法を指定します。

undo arp source-mac コマンドはデフォルトに戻します。

このコマンドはゲートウェイで設定します。

この機能は、CPU に送信された ARP パケットの数を確認します。同一 MAC アドレスから 5 秒以内に受信された ARP パケットの数が上限を超えた場合、MAC アドレスの ARP アタックエントリを作成します。エントリがエージアウトする前、装置は以下の処理のどちらかの処理を行います。

- モニタ—ログメッセージを作成します。
- フィルタ—ログメッセージを作成し、同一 MAC アドレスからの後続の ARP パケットを廃棄します。

undo arp anti-attack source-mac コマンドで **filter** パラメータ、**monitor** パラメータの両方とも指定されない場合、両方の処理方法が無効となります。

例

送信元 MAC アドレスにもとづいた ARP 攻撃 detection を有効にし、処理方法を filter に指定します。

<Switch> system-view

[Switch] arp source-mac filter

14.3.2 arp source-mac aging-time

Syntax

arp source-mac aging-time *time*

undo arp source-mac aging-time

デフォルト

300 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

time: ARP 攻撃エントリのエージング時間を設定します。設定範囲は 60～6000 秒です。

説明

arp source-mac aging-time コマンドは ARP 攻撃エントリのエージング時間を設定します。

undo arp anti-attack source-mac aging-time コマンドはデフォルトに戻します。

例

ARP 攻撃エントリのエージング時間を 60 秒に設定します。

<Switch> system-view

[Switch] arp source-mac aging-time 60

14.3.3 arp source-mac exclude-mac

Syntax

arp source-mac exclude-mac *mac-address*&<1-10>

undo arp source-mac exclude-mac [*mac-address*&<1-10>]

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

mac-address&<1-10>: 除外する MAC アドレスのリストを指定します。形式は H-H-H です。&<1-10>は除外する MAC アドレスを 10 まで設定できることを示します。

説明

arp anti-attack source-mac exclude-mac コマンドは送信元 MAC アドレスにもとづいた ARP 攻撃 detection から指定された MAC アドレスを除外します。

undo arp anti-attack source-mac exclude-mac コマンドは除外する MAC アドレスを削除します。

undo arp source-mac exclude-mac コマンドで MAC アドレスを指定しない場合、除外されたすべての MAC アドレスを削除します。

例

送信元 MAC にもとづいた ARP 攻撃 detection から指定された MAC アドレスを除外します。

<Switch> system-view

[Switch] arp source-mac exclude-mac 001e-1200-0213

14.3.4 arp source-mac threshold

Syntax

arp source-mac threshold *threshold-value*

undo arp source-mac threshold

デフォルト

30

View

System view

定義済みユーザロール

network-admin

パラメータ

threshold-value: 送信元 MAC アドレスにもとづいた ARP 攻撃 detection のしきい値を指定します。設定範囲は 1～5000 です。

説明

arp source-mac threshold コマンドは送信元 MAC アドレスにもとづいた ARP 攻撃 detection のしきい値を指定します。同一 MAC アドレスから 5 秒以内に受信された ARP パケットの数が上限を超えた場合、装置は、設定されたパラメータに従い、攻撃に対する処理を実行します。

undo arp source-mac threshold コマンドはデフォルトに戻します。

例

送信元 MAC アドレスにもとづいた ARP 攻撃 detection のしきい値を 30 に指定します。

<Switch> system-view

[Switch] arp source-mac threshold 30

14.3.5 display arp source-mac

Syntax

display arp source-mac { **interface** *interface-type interface-number* | **slot** *slot-number* }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: インタフェースのタイプと番号を指定します。

slot *slot-number*: IRF スタックメンバ装置で検出された ARP 攻撃エントリを表示します。*slot-number* は IRF スタックメンバ装置の ID を指定します。指定しない場合、マスタ装置の ARP 攻撃エントリを表示します。

説明

display arp source-mac コマンドは送信元 MAC アドレスにもとづいた ARP 攻撃 detection によって検出された ARP 攻撃エントリを表示します。

例

GigabitEthernet 1/0/1 で送信元 MAC アドレスにもとづいた ARP 攻撃 detection によって検出された ARP 攻撃エントリを表示します。

<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
```

14.4 ARPパケット送信元MACアドレス整合性チェック設定コマンド

14.4.1 arp valid-check enable

Syntax

arp valid-check enable

undo arp valid-check enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

arp valid-check enable コマンドはゲートウェイで ARP パケット送信元 MAC アドレス整合性チェックを有効にします。

undo arp valid-check enable コマンドは ARP パケット送信元 MAC アドレス整合性チェックを無効にします。

このコマンドはゲートウェイで設定します。ゲートウェイはイーサネットヘッダの送信元 MAC アドレスが ARP メッセージの送信 MAC アドレスと異なる場合、フィルタします。

例

#ARP パケット送信元 MAC アドレス整合性チェックを有効にします。

<Switch> system-view

[Switch] arp valid-check enable

14.5 ARP確認応答設定コマンド

14.5.1 arp active-ack enable

Syntax

arp active-ack enable

undo arp active-ack enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

arp active-ack enable コマンドは ARP 確認応答機能を有効にします。

undo arp active-ack enable コマンドはデフォルトに戻します。

このコマンドはゲートウェイでユーザのなりすましを防御します。

例

ARP 確認応答機能を有効にします。

<Switch> system-view

[Switch] arp active-ack enable

14.6 ARPアタック検出設定コマンド

14.6.1 arp detection enable

Syntax

arp detection enable

undo arp detection enable

デフォルト

無効

View

VLAN view

定義済みユーザロール

network-admin

説明

arp detection enable コマンドは ARP アタック検出を有効にします。

undo arp detection enable コマンドはデフォルトに戻します。

例

VLAN 2 で ARP アタック検出を有効にします。

<Switch> system-view

[Switch] vlan 2

[Switch-vlan2] arp detection enable

関連コマンド

- **arp detection rule**
- **display arp detection**
- **display arp detection statistics attack-source**
- **reset arp detection statistics attack-source**

14.6.2 arp detection log enable

Syntax

arp detection log enable [**interval** *interval*]

undo arp detection log enable

デフォルト

無効

Views

System view

定義済みユーザロール

network-admin

パラメータ

interval *interval*: ARP 検出ログをインフォセンターに送る間隔を指定します。

0 または、10～3600(秒)の範囲で指定が可能です。デフォルトは 60(秒)です。

0 に設定した場合は、装置は直ちに ARP 検出ログをインフォセンターに送ります。

説明

arp detection log enable コマンドは、ARP 検出時の LOG 出力を有効にします。

undo arp detection log enable コマンドは、ARP 検出時の LOG 出力を無効にします。

例

ARP 検出時のログ記録機能を有効にします。

<QX> system-view

[QX] arp detection log enable

14.6.3 arp detection trust

Syntax

arp detection trust

undo arp detection trust

デフォルト

インタフェースは非 ARP トラステッドポートです。

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

arp detection trust コマンドはインタフェースを ARP トラステッドポートとして設定します。

undo arp detection trust コマンドはデフォルトに戻します。

例

GigabitEthernet 1/0/1 を ARP トラステッドポートとして設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] arp detection trust

14.6.4 arp detection validate

Syntax

arp detection validate { **dst-mac** | **ip** | **src-mac** } *

undo arp detection validate [**dst-mac** | **ip** | **src-mac**] *

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

パラメータ

dst-mac: ARP 応答の宛先 MAC アドレスを確認します。宛先 MAC アドレスがすべて 0、すべて 1、イーサネットヘッダ内の送信先 MAC アドレスに矛盾があった場合、パケットは無効と見なされ、破棄されます。

ip: ARP 応答の送信元 IP アドレスと宛先 IP アドレスを確認します。ARP 要求の送信元 IP アドレスがすべて 0、すべて 1、マルチキャスト IP アドレスである場合、パケットは無効と見なされ、破棄されます。

src-mac: ARP パケットの送信元 MAC アドレスがイーサネットヘッダ内の送信元 MAC アドレスと同一かどうかをチェックします。同一だった場合、パケットは有効と見なされ、同一でなかった場合は、パケットは破棄されます。

説明

arp detection validate コマンドは ARP パケットの正当性の確認を有効にします。

undo arp detection validate コマンドは ARP パケットの正当性の確認を無効にします。

1 つのコマンドで確認する 1 つあるいは複数のオブジェクトを指定することができます。**undo arp detection validate** コマンドでパラメータを指定しない場合、すべてのオブジェクトを削除します。

例

ARP パケットの MAC アドレスと IP アドレスを確認する ARP パケットの正当性の確認を有効にします。

<Switch> system-view

[Switch] arp detection validate dst-mac ip src-mac

14.6.5 arp restricted-forwarding enable

Syntax

arp restricted-forwarding enable

undo arp restricted-forwarding enable

デフォルト

無効

View

VLAN view

定義済みユーザロール

network-admin

説明

arp restricted-forwarding enable コマンドは ARP 制限転送を有効にします。

undo arp restricted-forwarding enable コマンドは ARP 制限転送を無効にします。

例

VLAN 2 で ARP 制限転送を有効にします。

<Switch> system-view

[Switch] vlan 2

[Switch-vlan2] arp restricted-forwarding enable

14.6.6 display arp detection

Syntax

display arp detection

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display arp detection コマンドは ARP アタック検出が有効な VLAN を表示します。

例

#ARP アタック検出が有効な VLAN を表示します。

<Switch> display arp detection

```
ARP detection is enabled in the following VLANs:
1-2, 4-5
```

関連コマンド

arp detection enable

14.6.7 display arp detection statistics

Syntax

display arp detection statistics [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: インタフェースの ARP detection の統計情報を表示します。指定しない場合、すべてのインタフェースの統計情報を表示します

説明

display arp detection statistics コマンドは ARP アタック検出の統計情報を表示します。

このコマンドはユーザの正当性の確認と ARP パケットの正当性の確認で廃棄されたパケットの数を表示します。

例

すべてのインタフェースの ARP アタック検出の統計情報を表示します。

<Switch> display arp detection statistics

```
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
```

表 14-2 コマンド出力

フィールド	説明
State	インタフェースの状態です。 ● **U**—非ARPトラステッドインタフェースです。 ● **T**—ARPトラステッドインタフェースです。
Interface(State)	ARPパケットの受信インタフェースです。Stateはポートの状態を示します。トラステッドあるいは非トラステッドがあります。
IP	送信元IPアドレスと宛先IPアドレスが無効であるため、廃棄されたARPパケットの数です。
Src-MAC	送信元MACアドレスが無効であるため、廃棄されたARPパケットの数です。
Dst-MAC	宛先MACアドレスが無効であるため、廃棄されたARPパケットの数です。
Inspect	ユーザの正当性の確認が無効であるため、廃棄されたARPパケットの数です。

関連コマンド

reset arp detection statistics

14.6.8 display arp detection statistics attack-source

Syntax

display arp detection statistics attack-source slot *slot-number*

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

slot *slot-number*: IRF スタックメンバ装置を ID で指定します。メンバ装置を指定しない場合、このコマンドはマスタ装置の ARP アタックの送信元統計情報を表示します。

説明

display arp detection statistics attack-source コマンドは、ARP アタックの送信元統計情報を表示します。

例

slot 1 の ARP アタックの送信元統計情報を表示します。

<Switch> display arp detection statistics attack-source slot 1

```
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
```

表 14-3 コマンド出力

フィールド	説明
Interface	ARPアタックパケットのインタフェースを受信します。
VLAN	ARPアタックパケットが属するVLANです。
MAC address	ARPアタックパケットの送信元MACアドレスです。
IP address	ARPアタックパケットの送信元IPアドレスです。

フィールド	説明
Number	ARPアタック検出によって破棄されたARPアタックパケットの数です。
Time	ARPアタック検出がARPアタックパケットを破棄した最新の時刻です。

関連コマンド

arp detection enable

14.6.9 display arp detection statistics packet-drop

Syntax

display arp detection statistics packet-drop [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: インタフェースをタイプと番号で指定します。インタフェースを指定しない場合、このコマンドは、すべてのインタフェースの破棄されたパケット統計情報を表示します。

説明

display arp detection statistics packet-drop を使用して、ARP アタック detection で破棄されたパケットの統計情報を表示します。

このコマンドは、インタフェースのユーザ妥当性チェックおよび ARP パケット妥当性チェックによって破棄されたパケットの数を表示します。

例

#ARP アタック detection によって破棄されたパケットの統計情報を表示します。

<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
```

表 14-4 コマンド出力

フィールド	説明
State	インタフェースの状態です。 • **U**–ARP の untrusted インタフェースまたは AC です。 • **T**–ARP トラステッドインタフェースまたは AC です。
Interface(State)	ARPパケットの着信インタフェースまたはACです。Stateは、ポートまたはACの状態 (trustedまたはuntrusted) を指定します。
IP	無効な送信元およびターゲットIPアドレスが原因で破棄されたARPパケットの数です。
Src-MAC	無効な送信元MACアドレスが原因で破棄されたARPパケットの数です。
Dst-MAC	無効な宛先MACアドレスが原因で破棄されたARPパケットの数です。
Inspect	ユーザ妥当性チェックにパスしなかったARPパケットの数です。

関連コマンド

reset arp detection statistics packet-drop

14.6.10 reset arp detection statistics

Syntax

reset arp detection statistics [**interface** *interface-type interface-number*]

View

User view

定義済みユーザロール

network-admin

パラメータ

interface *interface-type interface-number*: インタフェースの ARP アタック検出の統計情報を削除します。指定しない場合、すべてのインタフェースの ARP アタック検出の統計情報を削除します。

説明

reset arp detection statistics コマンドは ARP アタック検出の統計情報を削除します。

例

すべてのインタフェースの ARP アタック検出の統計情報を削除します。

<Switch> reset arp detection statistics

関連コマンド

display arp detection statistics

14.6.11 reset arp detection statistics attack-source

Syntax

reset arp detection statistics attack-source [**slot** *slot-number*]

View

User view

定義済みユーザロール

network-admin

パラメータ

slot *slot-number*: IRF スタックメンバ装置を ID で指定します。メンバ装置を指定しない場合、このコマンドはマスタ装置の ARP アタックの送信元統計情報を削除します。

説明

reset arp detection statistics attack-source コマンドは、ARP アタックの送信元統計情報を削除します。

例

#ARP アタックの送信元統計情報を削除します。

<Switch> reset arp detection statistics attack-source

関連コマンド

- **arp detection enable**
- **display arp detection statistics attack-source**

14.6.12 reset arp detection statistics packet-drop

Syntax

reset arp detection statistics packet-drop [interface *interface-type interface-number*]

View

User view

定義済みユーザロール

network-admin

パラメータ

interface *interface-type interface-number*: インタフェースをタイプと番号で指定します。インタフェースを指定しない場合、このコマンドは、インタフェース上のすべてのインタフェースおよびすべての Ethernet サービスインスタンスについて、破棄されたパケット統計情報を削除します。

説明

reset arp detection statistics packet-drop コマンドは、ARP アタック detection によって破棄されたパケットの統計情報を削除します。

例

#ARP アタック detection によって破棄されたパケットの統計情報を削除します。

<Switch> reset arp detection statistics packet-drop

関連コマンド

display arp detection statistics packet-drop

14.7 ARPスキャンおよび固定ARP設定コマンド

14.7.1 arp scan

Syntax

arp scan [*start-ip-address* **to** *end-ip-address*] [**send-rate** *pps*]

View

VLAN interface view

定義済みユーザロール

network-admin

パラメータ

start-ip-address: スキャン範囲の開始 IP アドレスを指定します。

end-ip-address: スキャン範囲の終了 IP アドレスを指定します。終了 IP アドレスは、開始 IP アドレス以上である必要があります。

send-rate: 装置が ARP スキャンの ARP 要求を送信するレートを指定します。

pps: ARP パケット送信レートをパケット/秒 (pps)で指定します。*pps* の設定範囲は 10~1000 で、10 の倍数である必要があります。

説明

arp scan コマンドは指定されたアドレス範囲内で ARP スキャンを開始します。

ARP スキャンは、指定されたアドレス範囲内の装置の ARP エントリを自動的に作成します。ARP テーブルに存在する IP アドレスはスキャンされません。

インタフェースのプライマリ IP アドレスとセカンダリ IP アドレスがアドレス範囲内にある場合、ARP 要求の送信元 IP アドレスは、最小ネットワークセグメントのアドレスになります。

アドレス範囲が指定されていない場合、装置はインタフェースのプライマリ IP アドレスが存在するサブネット上の装置の ARP エントリを学習します。ARP 要求の送信元 IP アドレスは、インタフェースのプライマリ IP アドレスです。

開始 IP アドレスと終了 IP アドレスは、インタフェースのプライマリ IP アドレスまたはセカンダリ IP アドレスと同じサブネット上にある必要があります。

ARP スキャンには時間がかかります。実行中のスキャンを停止するには、**Ctrl+C** を押します。ダイナミック ARP エントリは、スキャンが終了する前に受信した ARP 応答に基づいて作成されます。

スキャンする範囲に IP アドレスが多い場合は、ARP パケットの送信レートを設定できます。この設定により、ARP トラフィックのバーストが原因で CPU 使用率が高くなり、ネットワーク負荷が高くなるのを回避できます。

送信レートを大きな値に設定すると、装置のパフォーマンスを確保するために、指定されたレートよりも低いレートが使用される場合があります。

例

VLAN インタフェース 2 のプライマリ IP アドレスが存在するネットワーク上のネイバをスキャンします。

<Switch> system-view

[Switch] interface vlan-interface 2

[Switch-Vlan-interface2] arp scan

VLAN インタフェース 2 上のアドレス範囲内のネイバをスキャンします。

<Switch> system-view

[Switch] interface vlan-interface 2

[Switch-Vlan-interface2] arp scan 1.1.1.1 to 1.1.1.20

VLAN インタフェース 2 上のアドレス範囲内のネイバを送信レート 10pps の ARP パケットでスキャンします。

<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

🕮 メモ：

arp scan コマンドは Version7.1.4 を含む以降のソフトウェアからサポートしています。

14.8 ARPゲートウェイプロテクション設定コマンド

14.8.1 arp filter source

Syntax

arp filter source *ip-address*

undo arp filter source *ip-address*

デフォルト

無効

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

ip-address: ゲートウェイの IP アドレスを指定します。

説明

arp filter source コマンドは ARP ゲートウェイプロテクションを有効にします。

undo arp filter source コマンドは ARP ゲートウェイプロテクションを無効にします。

インタフェースで最大 8 つの ARP ゲートウェイプロテクションを有効にすることができます。

arp filter source コマンドと **arp filter binding** コマンドを同一インタフェースに設定することはできません。

例

IP アドレス 1.1.1.1 のゲートウェイに ARP ゲートウェイプロテクションを有効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] arp filter source 1.1.1.1

14.9 ARPフィルタリング設定コマンド

14.9.1 arp filter binding

Syntax

arp filter binding *ip-address mac-address*

undo arp filter binding *ip-address*

デフォルト

無効

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

ip-address: 許可された送信元 IP アドレスを指定します。

mac-address: 許可された送信元 MAC アドレスを指定します。

説明

arp filter binding コマンドは ARP フィルタリングを有効にし、許可される ARP フィルタリングエントリを設定します。

undo arp filter binding コマンドは ARP フィルタリングエントリを削除します。

ARP パケットの送信元 IP アドレスと送信元 MAC アドレスが許可される ARP フィルタリングエントリに一致した場合、ARP パケットは許可されます。ARP パケットの送信元 IP アドレスと送信元 MAC アドレスが許可される ARP フィルタリングエントリに一致しない場合、ARP パケットは廃棄されます。

インタフェースで最大 8 つの ARP フィルタリングエントリを設定することができます。

arp filter binding コマンドと **arp filter source** コマンドを同一インタフェースに設定することはできません。

例

#ARP フィルタリングを有効にし、許可される ARP フィルタリングエントリを設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] arp filter binding 1.1.1.1 0e10-0213-1023

目次

このセクションのページは **9-x-x** です。

15 章 uRPF 15-1
15.1 IPv4 uRPF 設定コマンド 15-1
15.1.1 display ip urpf 15-1
15.1.2 ip urpf 15-2

15章 uRPF

15.1 IPv4 uRPF設定コマンド

15.1.1 display ip urpf

Syntax

display ip urpf [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

slot *slot-number*: IRF スタックメンバ装置を ID で指定します。指定しない場合、すべてのメンバ装置の uRPF 設定を表示します。

説明

display ip urpf コマンドは、uRPF の設定を表示します。

例

指定されたスロットの uRPF の設定を表示します。

<Switch> display ip urpf slot 1

```
Global uRPF configuration information(failed):
   Check type: strict
   Allow default route
```

表 15-1 コマンド出力

フィールド	説明
(failed)	リソース不足のため転送チップにuRPF設定の配信に失敗します。このフィールドがない場合、配信は成功しています。
Check type	uRPFチェックモードです。strictがあります。

15.1.2 ip urpf

Syntax

ip urpf { **strict** }

undo ip urpf

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

パラメータ

strict: strict uRPF チェックを有効にします。strict uRPF にパスするため、パケットの送信元アドレスと受信インタフェースは FIB エントリの宛先アドレスと出力インタフェースに一致する必要があります。

説明

ip urpf コマンドは、uRPF を有効にします。

undo ip urpf コマンドは、uRPF を無効にします。

uRPF は、CE または ISP に接続した PE 上、または CE 上で展開できます。

例

グローバルに strict uRPF チェックを有効にします。

<Switch> system-view

[Switch] ip urpf strict

関連コマンド

display ip urpf

QX-S5100G シリーズ Ethernet スイッチ

コマンドマニュアル

10. 高可用性

本マニュアルは以下に示す章で構成されています。

01-Ethernet OAM

02-CFD

03-DLDP

04-RRPP

05-Smart Link

06-Monitor Link

07-VRRP

08-BFD

09-Track

目次

このセクションのページは **10-x-x** です。

1 章 Ethernet OAM 1-1
1.1 Ethernet OAM 設定コマンド 1-1
1.1.1 display oam 1-1
1.1.2 display oam configuration 1-6
1.1.3 display oam critical-event 1-8
1.1.4 display oam link-event 1-10
1.1.5 oam enable 1-14
1.1.6 oam errored-frame threshold 1-14
1.1.7 oam errored-frame window 1-15
1.1.8 oam errored-frame-seconds threshold 1-16
1.1.9 oam errored-frame-seconds window 1-17
1.1.10 oam global errored-frame threshold 1-18
1.1.11 oam global errored-frame window 1-19
1.1.12 oam errored-frame-period threshold 1-20
1.1.13 oam errored-frame-period window 1-21
1.1.14 oam global errored-frame-period threshold 1-22
1.1.15 oam global errored-frame-period window 1-23
1.1.16 oam global errored-frame-seconds threshold 1-24
1.1.17 oam global errored-frame-seconds window 1-25
1.1.18 oam global timer hello 1-26
1.1.19 oam global timer keepalive 1-27
1.1.20 oam mode 1-28
1.1.21 oam remote-failure action 1-29
1.1.22 oam remote-loopback 1-30
1.1.23 oam remote-loopback interface 1-31
1.1.24 oam remote-loopback reject-request 1-32
1.1.25 oam timer hello 1-33
1.1.26 oam timer keepalive 1-34
1.1.27 reset oam 1-35

1章 Ethernet OAM

1.1 Ethernet OAM設定コマンド

1.1.1 display oam

Syntax

display oam { **local** | **remote** } [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

local: ローカル装置の Ethernet OAM の接続情報を表示します。

remote: ローカル装置の Ethernet OAM の接続情報を表示します。

interface *interface-type interface-number*: ポートのタイプと番号を指定します。

説明

display oam コマンドは Ethernet OAM の接続情報を表示します。接続の状態、Ethernet OAM パケットヘッダに含まれる情報、Ethernet OAM パケットの統計情報が含まれます。

interface を指定しない場合、すべての Ethernet OAM の接続情報を表示します。

例

すべてのローカル装置の Ethernet OAM の接続情報を表示します。

<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
```

ローカル装置の GigabitEthernet 1/0/1 の Ethernet OAM の接続情報を表示します。

<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
```

表 1-1 コマンド出力

フィールド	説明
GigabitEthernet1/0/1	GigabitEthernet 1/0/1の情報です。
Enable status	Ethernet OAMの状態です。有効あるいは無効があります。
Loopback status	Ethernet OAMループバックの状態です。 ● **No loopback**ーループバックがありません。 ● **Remote loopback**ーリモートループバックです。 ● **Local loopback**ーローカルループバックです。
Link status	リンク状態です。UPあるいはDOWNがあります。
OAM mode	ローカルEthernet OAMモードです。 ● **Active**—ポートがアクティブEthernet OAMモードで動作することを示します。 ● **Passive**—ポートがパッシブEthernet OAMモードで動作することを示します。

フィールド	説明
PDU	ローカル装置でのEthernet OAMPDUの処理方法です。 ● **RX_INFO**—ポートはEthernet OAMPDU情報を受信のみ行い、送信を行わないことを示します。 ● **LF_INFO**—ポートは、TLVトリプレットの情報と設定したリンクエラーフラグを除いたOAMPDU情報の送信を行うことを示します。 ● **INFO**—ポートは、OAMPDU情報のみを送受信することを示します。 ● **ANY**—ポートは、どのタイプのEthernet OAMPDUも送受信することを示します。
Mux action	ローカル送信装置の動作モードです。 ● **FWD**—ポートはどのようなパケットも送信できることを示します。 ● **DISCARD**—ポートは、Ethernet OAMPDUの送信のみ行うことを示します。
Par action	ローカル受信装置の動作モードです。 ● **FWD**—ポートはどのようなパケットも受信できることを示します。 ● **DISCARD**—ポートは、Ethernet OAMPDUの受信のみ行うことを示します。 ● **LB**—ローカル受信装置はEthernet OAMループバック試験が有効であることを示します。この場合、Ethernet OAMPDU以外のすべてのパケットは、送信された経路に沿って送信元に返されます。
Flags	送信されたEthernet OAMPDUのローカルフラグフィールドに挿入されたローカルフラグを示します。
Link fault	Ethernet OAMリンクエラーがあるかどうかを示します。
Dying gasp	致命的なエラーがあるかどうかを示します。
Critical event	クリティカルエラーがあるかどうかを示します。
Local evaluating	ローカル装置からリモート装置への設定のネゴシエーションが完了したかどうかを示します。 ● **COMPLETE**—ネゴシエーションが完了しました。 ● **NOTCOMPLETE**—ネゴシエーションが完了していません。

フィールド	説明
Remote evaluating	リモート装置からローカル装置への設定のネゴシエーションが完了したかどうかを示します。 ● **COMPLETE**—ネゴシエーションが完了しました。 ● **NOTCOMPLETE**—ネゴシエーションが完了していません。 ● **RESERVED**—このフィールドは予約されており、ネゴシエーションは完了していません。 ● **UNSATISFIED**—リモート装置がローカル装置の設定に満足しておらず、ネゴシエーションが完了していません。
Packets statistics	送受信したEthernet OAMPDUの統計情報です。
OAMPDU	送受信したEthernet OAMPDUの総数です。
OAMInformation	送受信したEthernet OAMPDU情報の数です。
OAMEventNotification	送受信したOAMPDUイベント通知の数です。
OAMUniqueEventNotification	１回だけ送信あるいは受信した重複していないOAMPDUイベント通知の数です。
OAMDuplicateEventNotification	送信あるいは受信した重複したOAMPDUイベント通知の数です。

すべてのリモートポートの Ethernet OAM の情報を表示します。

<Switch> display oam remote

```
----------- [GigabitEthernet1/0/1] -----------
 OAM mode         : Active
 MAC address      : 3822-d6a2-a800
 MTU size         : 1500
 Mux action       : FWD
 Par action       : FWD
```

リモートポート GigabitEthernet 1/0/1 の Ethernet OAM の情報を表示します。

<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
```

表 1-2 コマンド出力

フィールド	説明
GigabitEthernet1/0/1	GigabitEthernet 1/0/1の情報です。
OAM mode	ローカルEthernet OAMモードです。 ● **Active**—ポートがアクティブEthernet OAMモードで動作することを示します。 ● **Passive**—ポートがパッシブEthernet OAMモードで動作することを示します。
MAC address	リモート装置のMACアドレスです。
MTU size	MTUサイズです。単位はバイトです。
Mux action	リモート送信装置の動作モードです。 ● **FWD**—ポートはどのようなパケットも受信できることを示します。 ● **DISCARD**—ポートは、Ethernet OAMPDUの受信のみ行うことを示します。
Par action	リモート受信装置の動作モードです。 ● **FWD**—ポートはどのようなパケットも受信できることを示します。 ● **DISCARD**—ポートは、Ethernet OAMPDUの受信のみ行うことを示します。 ● **LB**—ローカル受信装置はEthernet OAMループバック試験が有効であることを示します。この場合、Ethernet OAMPDU以外のすべてのパケットは、送信された経路に沿って送信元に返されます。
Configuration	リモートEthernet OAMエンティティの設定です。
Unidirectional	単方向通信がサポートされるかどうかを示します。
Remote loopback	Ethernet OAMリモートループバックがサポートされているかどうかを示します。
Link events	Ethernet OAMリンクエラーイベントがサポートされているかどうかを示します。

フィールド	説明
MIB retrieval	MIB変数検索がサポートされているかどうかを示します。
Flags	OAMパケットのピアのEthernet OAMPDUのフラグフィールドの値です。
Link fault	Ethernet OAMリンクエラーがあるかどうかを示します。
Dying gasp	致命的なエラーがあるかどうかを示します。
Critical event	クリティカルエラーがあるかどうかを示します。
Local evaluating	ローカル装置からリモート装置への設定のネゴシエーションが完了したかどうかを示します。 ● **COMPLETE**—ネゴシエーションが完了しました。 ● **NOTCOMPLETE**—ネゴシエーションが完了していません。 ● **RESERVED**—このフィールドは予約されており、ネゴシエーションは完了していません。 ● **UNSATISFIED**—リモート装置がローカル装置の設定に満足しておらず、ネゴシエーションが完了していません。
Remote evaluating	リモート装置からローカル装置への設定のネゴシエーションが完了したかどうかを示します。 ● **COMPLETE**—ネゴシエーションが完了しました。 ● **NOTCOMPLETE**—ネゴシエーションが完了していません。 ● **UNSATISFIED**—リモート装置がローカル装置の設定に満足しておらず、ネゴシエーションが完了していません。

関連コマンド

reset oam

1.1.2 display oam configuration

Syntax

display oam configuration [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: ポートのタイプと番号を指定します。

説明

display oam configuration コマンドは指定されたポートでのグローバルの Ethernet OAM の設定を表示します。Ethernet OAM リンクエラーの検出期間としきい値が含まれます。

パラメータを指定しない場合、デフォルトの設定で使用しないポートでのグローバルの Ethernet OAM の設定を表示します。

例

デフォルトの設定で使用しないポートでのグローバルの Ethernet OAM の設定を表示します。

<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
```

表 1-3 コマンド出力

フィールド	説明
Global	グローバルの情報です。
GigabitEthernet1/0/1	GigabitEthernet 1/0/1の情報です。
OAM timers	Ethernet OAM接続検出タイマです。
Hello timer	Ethernet OAMハンドシェークパケットの転送間隔です。
Keepalive timer	Ethernet OAM接続タイムアウトタイマです。
Link monitoring	リンクイベント検出数としきい値です。
Errored symbol period	エラーシンボルイベントです。
Errored frame	エラーフレームイベントです。
Errored frame period	エラーフレーム期間イベントです。
Errored frame seconds	エラーフレーム秒イベントです。
Window	リンクイベントで設定された検出数です。
Threshold	リンクイベントで設定されたトリガとなるしきい値です。

🕮 **メモ：**

Errored symbol period フィールド、Errored frame period フィールドは現在のソフトウェアバージョンでサポートしていません。

1.1.3 display oam critical-event

Syntax

display oam critical-event [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: ポートのタイプと番号を指定します。

説明

display oam critical-event コマンドはポートでのクリティカルな Ethernet OAM リンクイベントの統計情報を表示します。

パラメータを指定しない場合、装置のすべてのポートで発生したクリティカルな Ethernet OAM リンクイベントの統計情報を表示します。

例

すべてのポートで発生したクリティカルな Ethernet OAM リンクイベントの統計情報を表示します。

<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
```

表 1-4 コマンド出力

フィールド	説明
GigabitEthernet1/0/1	GigabitEthernet 1/0/1の情報です。
Local link status	ローカルリンクの状態です。UPあるいはDOWNがあります。
Event statistics	クリティカルなEthernet OAMリンクイベントの統計情報です。
Link fault	リンクエラーがあるかどうかを示します。
Dying Gasp	致命的なエラーがあるかどうかを示します。
Critical Event	クリティカルエラーがあるかどうかを示します。

1.1.4 display oam link-event

Syntax

display oam link-event { **local** | **remote** } [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

local: ローカルポートの Ethernet OAM リンクエラーイベントの統計情報を表示します。

remote: リモートポートの Ethernet OAM リンクエラーイベントの統計情報を表示します。

interface *interface-type interface-number*: ポートのタイプと番号を指定します。

説明

display oam link-event コマンドはローカルポートあるいはリモートポートで発生した Ethernet OAM リンクエラーイベントの統計情報を表示します。

Ethernet OAM リンクエラーイベントは、エラーシンボルイベント、エラーフレームイベント、エラーフレーム期間イベント、エラーフレーム秒イベントを含みます。

interface を指定しない場合、すべてのローカルポートおよびリモートポートの Ethernet OAM リンクエラーイベントの統計情報を表示します。

例

すべてのローカルポートの Ethernet OAM リンクエラーイベントの統計情報を表示します。

<Switch> display oam link-event local

```
----------- [GigabitEthernet1/0/1] -----------
 Link status: UP
 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
```

すべてのリモートポートの Ethernet OAM リンクエラーイベントの統計情報を表示します。

<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
```

表 1-5 コマンド出力

フィールド	説明
GigabitEthernet1/0/1	GigabitEthernet 1/0/1の情報です。
Link status	ローカルリンクの状態です。UPあるいはDOWNがあります。
OAM local/remote errored symbol event	リモートポートのエラーシンボルイベントの情報です。（エラーシンボルイベントが発生したときのみ有効です。） ● **Event time stamp**—エラーシンボルイベントが発生した時間です。 ● **Errored symbol window**—エラーシンボルの検出数です。 ● **Errored symbol threshold**—エラーシンボルイベントのトリガが発生したエラーのしきい値です。 ● **Errored symbol**—最新のエラーシンボルイベントが検出されたシンボル数です。 ● **Error running total**—エラーシンボルの総数です。 ● **Event running total**—発生したエラーシンボルイベントの総数です。
OAM local/remote errored frame event	ローカルポート、リモートポートのエラーフレームイベントの情報です。（エラーフレームイベントが発生したときのみ有効です。） ● **Event time stamp**—エラーフレームイベントが発生した時間です。 ● **Errored frame window**—エラーフレームの検出間隔です。 ● **Errored frame threshold**—エラーフレームイベントのトリガが発生したエラーのしきい値です。 ● **Errored frame**—最新のエラーフレームイベントが検出されたシンボル数です。 ● **Error running total**—エラーフレームの総数です。 ● **Event running total**—発生したエラーフレームイベントの総数です。

フィールド	説明
OAM local/remote errored frame period event	ローカルポート、リモートポートのエラーフレーム期間イベントの情報です。（エラーフレーム期間イベントが発生したときのみ有効です。） ● **Event time stamp**—エラーフレーム期間イベントが発生した時間です。 ● **Errored frame period window**—エラーフレーム期間の検出間隔です。 ● **Errored frame period threshold**—エラーフレーム期間イベントのトリガが発生したエラーのしきい値です。 ● **Errored frame period**—最新のエラーフレーム期間イベントが検出されたシンボル数です。 ● **Error running total**—エラーフレーム期間の総数です。 ● **Event running total**—発生したエラーフレーム期間イベントの総数です。
OAM local/remote errored frame seconds summary event	ローカルポート、リモートポートのエラーフレーム秒イベントの情報です。（エラーフレーム秒イベントが発生したときのみ有効です。） ● **Event time stamp**—エラーフレーム秒イベントが発生した時間です。 ● **Errored frame second window**—エラーフレーム秒の検出間隔です。 ● **Errored Frame seconds threshold**—エラーフレーム秒イベントのトリガが発生したエラーのしきい値です。 ● **Errored frame seconds**—最新のエラーフレーム秒イベントが検出されたシンボル数です。 ● **Error running total**—エラーフレーム秒の総数です。 ● **Event running total**—発生したエラーフレーム秒イベントの総数です。

🕮 **メモ：**

OAM local/remote errored symbol event フィールド、OAM local/remote errored frame period event フィールドは現在のソフトウェアバージョンでサポートしていません。

関連コマンド

reset oam

1.1.5 oam enable

Syntax

oam enable

undo oam enable

デフォルト

無効

View

Layer 2 Ethernet port view

定義済みユーザロール

network-admin

説明

oam enable コマンドは Ethernet OAM を有効にします。

undo oam enable コマンドは Ethernet OAM を無効にします。

例

GigabitEthernet 1/0/1 で Ethernet OAM を有効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] oam enable

1.1.6 oam errored-frame threshold

Syntax

oam errored-frame threshold *threshold-value*

undo oam errored-frame threshold

デフォルト

ポートはグローバルの設定を使用します。

View

Layer 2 Ethernet port view

定義済みユーザロール

network-admin

パラメータ

threshold-value: エラーフレームイベントのトリガが発生するしきい値を指定します。設定範囲は 0～4294967295 です。

説明

oam errored-frame threshold コマンドはポートでエラーフレームイベントのトリガが発生するしきい値を設定します。

undo oam errored-frame threshold コマンドはデフォルトに戻します。

port view の設定は指定されたポートで適用されます。port view での設定は、グローバルの設定よりも優先されます。

例

エラーフレームイベントのトリガが発生するしきい値を 100 に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] oam errored-frame threshold 100

関連コマンド

- **display oam configuration**
- **display oam link-event**
- **oam global errored-frame threshold**

1.1.7 oam errored-frame window

Syntax

oam errored-frame window *window-value*

undo oam errored-frame window

デフォルト

ポートはグローバルの設定を使用します。

View

Layer 2 Ethernet port view

定義済みユーザロール

network-admin

パラメータ

window-value: エラーフレームイベントの検出間隔を指定します。設定範囲は 10～600 です。単位は 1/10 秒（100 ミリ秒）です。たとえば、*window-value* が 10 である場合、1

秒(1000 ミリ秒)となります。10、20、30、・・・590、600 のように 10 の倍数で設定します。たとえば 15（1500 ミリ秒）を指定することはできません。

説明

oam errored-frame window コマンドはエラーフレームイベントの検出間隔を設定します。

undo oam errored-frame window コマンドはデフォルトに戻します。

port view の設定は指定されたポートで適用されます。port view での設定は、グローバルの設定よりも優先されます。

例

GigabitEthernet 1/0/1 でエラーフレームイベントの検出間隔を 20（2000 ミリ秒）に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] oam errored-frame window 20

関連コマンド

- **display oam configuration**
- **display oam link-event**
- **oam global errored-frame window**

1.1.8 oam errored-frame-seconds threshold

Syntax

oam errored-frame-seconds threshold *threshold-value*

undo oam errored-frame-seconds threshold

デフォルト

ポートはグローバルの設定を使用します。

View

Layer 2 Ethernet port view

定義済みユーザロール

network-admin

パラメータ

threshold-value: エラーフレーム秒イベントのトリガが発生するしきい値を指定します。設定範囲は 0～900 です。

説明

oam errored-frame-seconds threshold コマンドはポートでエラーフレーム秒イベントのトリガが発生するしきい値を設定します。

undo oam errored-frame-seconds threshold コマンドはデフォルトに戻します。

エラーフレーム秒イベントを動作させるために、エラーフレーム秒検出しきい値は、エラーフレーム秒イベントの検出期間（秒）より小さくする必要があります。そうでなければエラーフレーム秒イベントが動作しません。

port view の設定は指定されたポートで適用されます。port view での設定は、グローバルの設定よりも優先されます。

例

GigabitEthernet 1/0/1 でエラーフレーム秒イベントのトリガが発生するしきい値を 100 に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] oam errored-frame-seconds threshold 100

関連コマンド

- **display oam configuration**
- **display oam link-event**
- **oam errored-frame-seconds window**
- **oam global errored-frame-seconds threshold**

1.1.9 oam errored-frame-seconds window

Syntax

oam errored-frame-seconds window *window-value*

undo oam errored-frame-seconds window

デフォルト

ポートはグローバルの設定を使用します。

View

Layer 2 Ethernet port view

定義済みユーザロール

network-admin

パラメータ

window-value: エラーフレームイベントの検出間隔を指定します。設定範囲は 100～9000 です。単位は 1/10 秒（100 ミリ秒）です。たとえば、*window-value* が 100 である場合、10 秒(10000 ミリ秒)となります。100、200、300、・・・8990、9000 のように 10 の倍数で設定します。たとえば 105（10.5 秒（10500 ミリ秒））を指定することはできません。

説明

oam errored-frame-seconds window コマンドはエラーフレーム秒イベントの検出間隔を設定します。

undo oam errored-frame-seconds window コマンドはデフォルトに戻します。

エラーフレーム秒イベントを動作させるために、エラーフレーム秒検出しきい値は、エラーフレーム秒イベントの検出期間（秒）より小さくする必要があります。そうでなければエラーフレーム秒イベントが動作しません。

port view の設定は指定されたポートで適用されます。port view での設定は、グローバルの設定よりも優先されます。

例

エラーフレーム秒イベントの検出間隔を 100（10000 ミリ秒）に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] oam errored-frame-seconds window 100

関連コマンド

- **display oam configuration**
- **display oam link-event**
- **oam errored-frame-seconds threshold**
- **oam errored-frame-seconds period**

1.1.10 oam global errored-frame threshold

Syntax

oam global errored-frame threshold *threshold-value*

undo oam global errored-frame threshold

デフォルト

1

View

System view

定義済みユーザロール

network-admin

パラメータ

threshold-value: エラーフレームイベントのトリガが発生するしきい値を指定します。設定範囲は 0～4294967295 です。

説明

oam global errored-frame threshold コマンドはグローバルでエラーフレームイベントのトリガが発生するしきい値を設定します。

undo oam global errored-frame threshold コマンドはデフォルトに戻します。

system view の設定はすべてのポートで適用されます。port view での設定は、グローバルの設定よりも優先されます。

例

エラーフレームイベントのトリガが発生するしきい値を 100 に設定します。

<Switch> system-view

[Switch] oam global errored-frame threshold 100

関連コマンド

- **display oam configuration**
- **display oam link-event**
- **oam errored-frame threshold**

1.1.11 oam global errored-frame window

Syntax

oam global errored-frame window *window-value*

undo oam global errored-frame window

デフォルト

10（1000 ミリ秒）

View

System view

定義済みユーザロール

network-admin

パラメータ

window-value: エラーフレームイベントの検出間隔を指定します。設定範囲は 10～600 です。単位は 1/10 秒（100 ミリ秒）です。たとえば、*window-value* が 10 である場合、1 秒(1000 ミリ秒)となります。10、20、30、・・・590、600 のように 10 の倍数で設定します。たとえば 15（1500 ミリ秒）を指定することはできません。

説明

oam global errored-frame window コマンドはグローバルでエラーフレームイベントの検出間隔を設定します。

undo oam global errored-frame window コマンドはデフォルトに戻します。

system view の設定はすべてのポートで適用されます。port view での設定は、グローバルの設定よりも優先されます。

例

エラーフレームイベントの検出間隔を 20（2000 ミリ秒）に設定します。

<Switch> system-view

[Switch] oam global errored-frame window 20

関連コマンド

- **display oam configuration**
- **display oam link-event**
- **oam errored-frame window**

1.1.12 oam errored-frame-period threshold

Syntax

oam errored-frame-period threshold *threshold-value*

undo oam errored-frame-period threshold

デフォルト

ポートはグローバルの設定を使用します。

View

Layer 2 Ethernet port view, Layer 3 Ethernet port view

定義済みユーザロール

network-admin

パラメータ

threshold-value: エラーフレーム期間イベントのトリガが発生するしきい値を指定します。設定範囲は 0～4294967295 です。

説明

oam errored-frame-period threshold コマンドはポートでエラーフレーム期間イベントのトリガが発生するしきい値を設定します。

undo oam errored-frame-period threshold コマンドはデフォルトに戻します。

port view の設定は指定されたポートで適用されます。port view での設定は、グローバルの設定よりも優先されます。

例

GigabitEthernet 1/0/1 でエラーフレーム期間イベントのトリガが発生するしきい値を 100 に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] oam errored-frame-period threshold 100

関連コマンド

- **display oam configuration**
- **display oam link-event**
- **oam global errored-frame-period threshold**

1.1.13 oam errored-frame-period window

Syntax

oam errored-frame-period window *window-value*

undo oam errored-frame-period window

デフォルト

ポートはグローバルの設定を使用します。

View

Layer 2 Ethernet port view, Layer 3 Ethernet port view

定義済みユーザロール

network-admin

パラメータ

window-value: エラーフレーム期間イベントの検出数を指定します。設定範囲は 1～65535 です。検出数は *window-value* の 10000 倍の値です。たとえば、*window-value* が 200 である場合、2000000 となります。検出数の設定は 10000 の倍数で設定する必要があります。たとえば 15000 を検出するように設定することはできません。設定値が整数でない 1.5 となり、設定できません。

説明

oam errored-frame-period window コマンドはエラーフレーム期間イベントの検出数を設定します。

undo oam errored-frame-period window コマンドはデフォルトに戻します。

port view の設定は指定されたポートで適用されます。port view での設定は、グローバルの設定よりも優先されます。

例

エラーフレーム期間イベントの検出数を 20000000 に指定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] oam errored-frame-period window 2000

関連コマンド

- **display oam configuration**
- **display oam link-event**
- **oam global errored-frame-period window**

1.1.14 oam global errored-frame-period threshold

Syntax

oam global errored-frame-period threshold *threshold-value*

undo oam global errored-frame-period threshold

デフォルト

1

View

System view

定義済みユーザロール

network-admin

パラメータ

threshold-value: エラーフレーム期間イベントのトリガが発生するしきい値を指定します。設定範囲は 0～4294967295 です。

説明

oam global errored-frame-period threshold コマンドはグローバルでエラーフレーム期間イベントのトリガが発生するしきい値を設定します。

undo oam global errored-frame-period threshold コマンドはデフォルトに戻します。

system view の設定はすべてのポートで適用されます。port view での設定は、グローバルの設定よりも優先されます。

例

エラーフレーム期間イベントのトリガが発生するしきい値を 100 に設定します。

<Switch> system-view

[Switch] oam global errored-frame-period threshold 100

関連コマンド

- **display oam configuration**
- **display oam link-event**
- **oam errored-frame-period threshold**

1.1.15 oam global errored-frame-period window

Syntax

oam global errored-frame-period window *window-value*

undo oam global errored-frame-period window

デフォルト

10000000

View

System view

定義済みユーザロール

network-admin

パラメータ

window-value: エラーフレーム期間イベントの検出数を指定します。設定範囲は 1～65535 です。検出数は *window-value* の 10000 倍の値です

説明

oam global errored-frame-period window コマンドはグローバルでエラーフレーム期間イベントの検出数を設定します。

undo oam global errored-frame-period window コマンドはデフォルトに戻します。

system view の設定はすべてのポートで適用されます。port view での設定は、グローバルの設定よりも優先されます。

例

エラーフレーム期間イベントの検出数を 20000000 に指定します。

<Switch> system-view

[Switch] oam global errored-frame-period window 2000

関連コマンド

- **display oam configuration**
- **display oam link-event**
- **oam errored-frame-period window**

1.1.16 oam global errored-frame-seconds threshold

Syntax

oam global errored-frame-seconds threshold *threshold-value*

undo oam global errored-frame-seconds threshold

デフォルト

1

View

System view

定義済みユーザロール

network-admin

パラメータ

threshold-value: エラーフレーム秒イベントのトリガが発生するしきい値を指定します。設定範囲は 0～900 です。

説明

oam global errored-frame-seconds threshold コマンドはグローバルでエラーフレーム秒イベントのトリガが発生するしきい値を設定します。

undo oam global errored-frame-seconds threshold コマンドはデフォルトに戻します。

エラーフレーム秒イベントを動作させるために、エラーフレーム秒検出しきい値は、エラーフレーム秒イベントの検出期間（秒）より小さくする必要があります。そうでなければエラーフレーム秒イベントが動作しません。

system view の設定はすべてのポートで適用されます。port view での設定は、グローバルの設定よりも優先されます。

例

エラーフレーム秒イベントのトリガが発生するしきい値を 100 に設定します。

<Switch> system-view

[Switch] oam global errored-frame-seconds threshold 100

関連コマンド

- **display oam configuration**
- **display oam link-event**
- **oam errored-frame-seconds threshold**
- **oam global errored-frame-seconds window**

1.1.17 oam global errored-frame-seconds window

Syntax

oam global errored-frame-seconds window *window-value*

undo oam global errored-frame-seconds window

デフォルト

600（60000 ミリ秒）

View

System view

定義済みユーザロール

network-admin

パラメータ

window-value: エラーフレームイベントの検出間隔を指定します。設定範囲は 100～9000 です。単位は 1/10 秒（100 ミリ秒）です。たとえば、*window-value* が 100 である場合、10 秒(10000 ミリ秒)となります。100、200、300、・・・8990、9000 のように 10 の倍数で設定します。たとえば 105（10.5 秒（10500 ミリ秒））を指定することはできません。

説明

oam global errored-frame-seconds window コマンドはグローバルでエラーフレーム秒イベントの検出間隔を設定します。

undo oam global errored-frame-seconds window コマンドはデフォルトに戻します。

エラーフレーム秒イベントを動作させるために、エラーフレーム秒検出しきい値は、エラーフレーム秒イベントの検出期間（秒）より小さくする必要があります。そうでなければエラーフレーム秒イベントが動作しません。

system view の設定はすべてのポートで適用されます。port view での設定は、グローバルの設定よりも優先されます。

例

エラーフレーム秒イベントの検出間隔を 100（10000 ミリ秒）に設定します。

<Switch> system-view

[Switch] oam global errored-frame-seconds window 100

関連コマンド

- **display oam configuration**
- **display oam link-event**
- **oam errored-frame-seconds period**
- **oam global errored-frame-seconds threshold**

1.1.18 oam global timer hello

Syntax

oam global timer hello *interval*

undo oam global timer hello

デフォルト

1000 ミリ秒

View

System view

定義済みユーザロール

network-admin

パラメータ

interval: Ethernet OAM ハンドシェークパケットを転送する間隔を指定します。設定範囲は 500～5000 ミリ秒です。500、600、700、・・・4900、5000 のように 100 の倍数で設定します。

説明

oam global timer hello コマンドはグローバルの Ethernet OAM ハンドシェークパケットを転送する間隔を設定します。

undo oam global timer hello コマンドはデフォルトに戻します。

Ethernet OAM 接続のタイムアウトタイマが終了した後、ローカル OAM エンティティは、OAM 接続を切断し、ピアの OAM エンティティの接続を終了させます。Ethernet OAM 接続を安定的に維持するために、Ethernet OAM コネクションタイムアウト値は Ethernet OAM ハンドシェークパケットの送信間隔の少なくとも 5 倍以上にすることを推奨します。

system view の設定はすべてのポートで適用されます。port view での設定は、グローバルの設定よりも優先されます。

例

Ethernet OAM ハンドシェークパケットを転送する間隔を 600 ミリ秒に設定します。

<Switch> system-view

[Switch] oam global timer hello 600

関連コマンド

- **display oam configuration**
- **oam timer hello**

1.1.19 oam global timer keepalive

Syntax

oam global timer keepalive *interval*

undo oam global timer keepalive

デフォルト

5000 ミリ秒

View

System view

定義済みユーザロール

network-admin

パラメータ

interval: Ethernet OAM 接続のタイムアウトタイマを指定します。設定範囲は 1000～25000 ミリ秒です。1000、1100、1200、・・・24900、25000 のように 100 の倍数で設定します。

説明

oam global timer keepalive コマンドは Ethernet OAM 接続のタイムアウトタイマを設定します。

undo oam global timer keepalive コマンドはデフォルトに戻します。

Ethernet OAM 接続のタイムアウトタイマが終了した後、ローカル OAM エンティティは、OAM 接続を切断し、ピアの OAM エンティティの接続を終了させます。Ethernet OAM 接続を安定的に維持するために、Ethernet OAM コネクションタイムアウト値は Ethernet OAM ハンドシェークパケットの送信間隔の少なくとも 5 倍以上にすることを推奨します。

system view の設定はすべてのポートで適用されます。port view での設定は、グローバルの設定よりも優先されます。

例

Ethernet OAM 接続のタイムアウトタイマを 6000 ミリ秒に設定します。

<Switch> system-view

[Switch] oam global timer keepalive 6000

関連コマンド

- **display oam configuration**
- **oam timer keepalive**

1.1.20 oam mode

Syntax

oam mode { **active** | **passive** }

undo oam mode

デフォルト

アクティブ

View

Layer 2 Ethernet port view

定義済みユーザロール

network-admin

パラメータ

active: アクティブ Ethernet OAM モードを指定します。

passive: パッシブ Ethernet OAM モードを指定します。

説明

oam mode コマンドは Ethernet OAM モードを設定します。

undo oam mode コマンドはデフォルトに戻します。

Ethernet OAM が有効なポートで Ethernet OAM モードを変更する場合、最初にポートで Ethernet OAM を無効にする必要があります。

例

GigabitEthernet 1/0/1 で Ethernet OAM を無効にし、Ethernet OAM モードをパッシブで動作するように設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] undo oam enable

[Switch-GigabitEthernet1/0/1] oam mode passive

関連コマンド

oam enable

1.1.21 oam remote-failure action

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**

デフォルト

ポートはリモートエンドからの Ethernet OAM イベントのみログを行います。

View

Layer 2 Ethernet port view, Layer 3 Ethernet port view

定義済みユーザロール

network-admin

パラメータ

connection-expired: 接続タイムアウト障害を指定します。

critical-event: 重大な障害を指定します。

dying-gasp: 致命的な障害を指定します。

link-fault: リンク障害を指定します。

error-link-down: OAM 接続を終了し、ポートのリンク状態をダウンに設定します。

説明

oam remote-failure action コマンドは、リモートエンドから Ethernet OAM イベントを受信後にポートがとる行動を設定します。

undo oam remote-failure action コマンドは、 デフォルトに設定を戻します。

例

リモートエンドか致命的な障害を受信後に、OAM 接続を終わらせるよう GigabitEthernet 1/0/1 に設定し、ポートのリンクをダウンにします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] oam remote-failure dying-gasp action error-link-down

1.1.22 oam remote-loopback

Syntax

oam remote-loopback start

oam remote-loopback stop

デフォルト

無効

View

Layer 2 Ethernet port view

定義済みユーザロール

network-admin

説明

oam remote-loopback start コマンドは指定されたポートで Ethernet OAM リモートループバックを有効にします。

oam remote-loopback stop コマンドはポートの Ethernet OAM リモートループバックを無効にします。

Ethernet OAM リモートループバックは、Ethernet OAM 接続が確立され、Ethernet OAM エンティティがアクティブ Ethernet OAM モードであるときのみ実行可能です。

user view あるいは system view で指定されたポート、あるいは port view で指定された現在のポート上で Ethernet OAM リモートループバックを有効にすることができます。これらのポートで行われた設定は同一の効果が適用されます。

例

アクティブ Ethernet OAM モードを設定し、GigabitEthernet 1/0/1 で Ethernet OAM を有効にします。Layer 2 Ethernet port view で GigabitEthernet 1/0/1 の Ethernet OAM リモートループバックを有効にします。

<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

関連コマンド

- **oam enable**
- **oam mode**
- **oam remote-loopback interface**

1.1.23 oam remote-loopback interface

Syntax

oam remote-loopback start interface *interface-type interface-number*

oam remote-loopback stop interface *interface-type interface-number*

デフォルト

無効

View

User view, system view

定義済みユーザロール

network-admin

パラメータ

interface-type interface-number: ポートのタイプと番号を指定します。

説明

oam remote-loopback start interface コマンドはポートで Ethernet OAM リモートループバックを有効にします。

oam remote-loopback stop interface コマンドはポートで Ethernet OAM リモートループバックを無効にします。

Ethernet OAM リモートループバックは、Ethernet OAM 接続が確立され、Ethernet OAM エンティティがアクティブ Ethernet OAM モードであるときのみ実行可能です。

user view あるいは system view で指定されたポート、あるいは port view で指定された現在のポート上で Ethernet OAM リモートループバックを有効にすることができます。これらのポートで行われた設定は同一の効果が適用されます。

例

アクティブ Ethernet OAM モードを設定し、GigabitEthernet 1/0/1 で Ethernet OAM を有効にします。system view で GigabitEthernet 1/0/1 の Ethernet OAM リモートループバックを有効にします。

<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

関連コマンド

- **oam enable**
- **oam mode**
- **oam remote-loopback**

1.1.24 oam remote-loopback reject-request

Syntax

oam remote-loopback reject-request

undo oam remote-loopback reject-request

デフォルト

リモートポートからの Ethernet OAM リモートループバック要求を拒否しません。

View

Layer 2 Ethernet port view

定義済みユーザロール

network-admin

説明

oam remote-loopback reject-request コマンドはリモートポートからの Ethernet OAM リモートループバック要求を拒否するように設定します。

undo oam remote-loopback reject-request コマンドはデフォルトに戻します。

oam remote-loopback reject-request コマンドを実行したときポートがループバックである場合、設定は次回のループバックを開始したときに適用されます。

例

GigabitEthernet 1/0/1 でリモートポートからの Ethernet OAM リモートループバック要求を拒否するように設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] oam remote-loopback reject-request

1.1.25 oam timer hello

Syntax

oam timer hello *interval*

undo oam timer hello

デフォルト

ポートはグローバルの設定を使用します。

View

Layer 2 Ethernet port view

定義済みユーザロール

network-admin

パラメータ

interval: Ethernet OAM ハンドシェークパケットを転送する間隔を指定します。設定範囲は 500～5000 ミリ秒です。500、600、700、・・・4900、5000 のように 100 の倍数で設定します。

説明

oam timer hello コマンドは Ethernet OAM ハンドシェークパケットを転送する間隔を設定します。

undo oam timer hello コマンドはデフォルトに戻します。

Ethernet OAM 接続のタイムアウトタイマが終了した後、ローカル OAM エンティティは、OAM 接続を切断し、ピアの OAM エンティティの接続を終了させます。Ethernet OAM 接続を安定的に維持するために、Ethernet OAM コネクションタイムアウト値は Ethernet OAM ハンドシェークパケットの送信間隔の少なくとも 5 倍以上にすることを推奨します。

port view の設定は指定されたポートで適用されます。port view での設定は、グローバルの設定よりも優先されます。

例

Ethernet OAM ハンドシェークパケットを転送する間隔を 600 ミリ秒に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] oam timer hello 600

関連コマンド

- **display oam configuration**
- **oam global timer hello**

1.1.26 oam timer keepalive

Syntax

oam timer keepalive *interval*

undo oam timer keepalive

デフォルト

ポートはグローバルの設定を使用します。

View

Layer 2 Ethernet port view

定義済みユーザロール

network-admin

パラメータ

interval: Ethernet OAM 接続のタイムアウトタイマを指定します。設定範囲は 1000～25000 ミリ秒です。1000、1100、1200、・・・24900、25000 のように 100 の倍数で設定します。

説明

oam timer keepalive コマンドは Ethernet OAM 接続のタイムアウトタイマを設定します。

undo oam timer keepalive コマンドはデフォルトに戻します。

Ethernet OAM 接続のタイムアウトタイマが終了した後、ローカル OAM エンティティは、OAM 接続を切断し、ピアの OAM エンティティの接続を終了させます。Ethernet OAM 接続を安定的に維持するために、Ethernet OAM コネクションタイムアウト値は Ethernet OAM ハンドシェークパケットの送信間隔の少なくとも 5 倍以上にすることを推奨します。

port view の設定は指定されたポートで適用されます。port view での設定は、グローバルの設定よりも優先されます。

例

Ethernet OAM 接続のタイムアウトタイマを 6000 ミリ秒に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] oam timer keepalive 6000

関連コマンド

- **display oam configuration**
- **oam global timer keepalive**

1.1.27 reset oam

Syntax

reset oam [**interface** *interface-type interface-number*]

View

User view

定義済みユーザロール

network-admin

パラメータ

interface *interface-type interface-number*: ポートのタイプと番号を指定します。

説明

reset oam コマンドはポートの Ethernet OAM パケットの統計情報とリンクエラーイベントを削除します。

パラメータを指定しない場合、すべてのポートの Ethernet OAM パケットの統計情報とリンクエラーイベントを削除します。

例

すべてのポートの Ethernet OAM パケットの統計情報とリンクエラーイベントを削除します。

<Switch> reset oam

関連コマンド

- **display oam**

- **display oam link-event**

目次

このセクションのページは **10-x-x** です。

2 章 CFD 2-1
2.1 CFD 設定コマンド 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 2-4
2.1.5 cfd linktrace auto-detection 2-5
2.1.6 cfd loopback 2-6
2.1.7 cfd md 2-8
2.1.8 cfd mep 2-9
2.1.9 cfd meplist 2-11
2.1.10 cfd mip-rule 2-12
2.1.11 cfd service-instance 2-13
2.1.12 display cfd linktrace-reply 2-14
2.1.13 display cfd linktrace-reply auto-detection 2-16
2.1.14 display cfd md 2-18
2.1.15 display cfd mep 2-19
2.1.16 display cfd meplist 2-22
2.1.17 display cfd mp 2-23
2.1.18 display cfd remote-mep 2-25
2.1.19 display cfd service-instance 2-26
2.1.20 display cfd status 2-28

2章 CFD

2.1 CFD設定コマンド

2.1.1 cfd cc enable

Syntax

cfd cc service-instance *instance-id* **mep** *mep-id* **enable**

undo cfd cc service-instance *instance-id* **mep** *mep-id* **enable**

デフォルト

無効

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

service-instance *instance-id*: サービスインスタンス ID を指定します。設定範囲は 1～32767 です。

mep *mep-id*: MEP の ID を指定します。設定範囲は 1～8191 です。

説明

cfd cc enable コマンドは指定した MEP で CCM の送信を有効にします。

undo cfd cc enable コマンドは指定した MEP で CCM の送信を無効にします。

コマンドを使用するとき以下のガイドラインに従ってください。

- Ethernet interface view で設定されたコマンドは、Ethernet インタフェースでのみ適用されます。
- aggregate interface view で設定されたコマンドは、アグリゲートインタフェースとアグリゲーションメンバポートでのみ適用されます。
- メンバポートがアグリゲーションインタフェースから削除した場合、アグリゲーションメンバポートでのみ適用されます。

例

GigabitEthernet 1/0/1 においてサービスインスタンス 5 の MEP3 で CCM の送信を有効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] cfd cc service-instance 5 mep 3 enable

関連コマンド

cfd cc interval

2.1.2 cfd cc interval

Syntax

cfd cc interval *interval-value* **service-instance** *instance-id*

undo cfd cc interval [*interval-value*] **service-instance** *instance-id*

デフォルト

4

View

System view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: CCM メッセージの interval フィールドの値を指定します。interval フィールドの設定範囲は 1～7 です。装置は 1～2 の CCM メッセージの interval フィールドをサポートしていません。

service-instance *instance-id*: サービスインスタンス ID を指定します。設定範囲は 1～32767 です。

説明

cfd cc interval コマンドは CCM メッセージの interval フィールドの値を設定します。

undo cfd cc interval コマンドはデフォルトに戻します。

CCM メッセージの interval フィールドの値を設定するとき、表 2-1 に示す値を使用します。

表 2-1 CCM interval フィールドの変換

CCM interval フィールドの値	CCM の送信間隔	最大 CCM ライフタイム次官
1	10/3ミリ秒	35/3ミリ秒

CCM interval フィールドの値	CCM の送信間隔	最大 CCM ライフタイム次官
2	10ミリ秒	35ミリ秒
3	100ミリ秒	350ミリ秒
4	1秒	3.5秒
5	10秒	35秒
6	60秒	210秒
7	600秒	2100秒

例

サービスインスタンス 2 の CCM メッセージの interval フィールドの値を 7 に設定します。

<Switch> system-view

[Switch] cfd cc interval 7 service-instance 2

関連コマンド

cfd cc enable

2.1.3 cfd enable

Syntax

cfd enable

undo cfd enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

cfd enable コマンドは CFD を有効にします。

undo cfd enable コマンドは CFD を無効にします。

例

CFD を有効にします。

<Switch> system-view

[Switch] cfd enable

2.1.4 cfd linktrace

Syntax

cfd linktrace service-instance *instance-id* **mep** *mep-id* { **target-mac** *mac-address* | **target-mep** *target-mep-id* } [**ttl** *ttl-value*] [**hw-only**]

View

すべての view

定義済みユーザロール

network-admin

パラメータ

service-instance *instance-id*: サービスインスタンス ID を指定します。設定範囲は 1～32767 です。

mep *mep-id*: 送信元 MEP の ID を指定します。設定範囲は 1～8191 です。

target-mac *mac-address*: 宛先 MAC アドレスを指定します。形式は H-H-H です。

target-map *target-mep-id*: 宛先 MEP の ID を指定します。設定範囲は 1～8191 です。

ttl *ttl-value*: TTL(time to live)の値を指定します。設定範囲は 1～255 です。デフォルトは 64 です。

hw-only: LTM が送信する hw-only ビットを設定します。hw-only を指定した場合、MIP は未知の宛先 MAC アドレスの LTM メッセージをフラッディングしません。

説明

cfd linktrace コマンドは送信元 MEP と宛先 MP 間の経路を検索します。経路の検出は、2 つの MEP 間における LTM の送信と、受信 LTR の検出を通じて行われます。

例

サービスインスタンス 1 の送信元 MEP1101 と宛先 MEP2001 間の経路を定義します。

<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
```

表 2-2 コマンド出力

フィールド	説明
Linktrace to MEP 2001 with the sequence number 1101-43361	宛先MEP2001をシーケンス番号1101-43361に関連づけます。
MAC Address	LTRメッセージの送信元MACアドレスです。
TTL	LTMが装置を通過するときのTTLの値です。
Last Mac	LTMメッセージの最終ホップの装置のMACアドレスです。
Relay Action	転送する装置がMACアドレステーブルから宛先MACアドレスを検出したかどうかを示します。 CFDの標準バージョン（IEEE 802.1ag）が使用されたとき、以下のことを示します。 • **Hit**—現在の装置は宛先装置です。 • **FDB**—転送する装置は宛先MACアドレスを検出しました。 • **MPDB**—宛先MACアドレスが見つかりませんでした。あるいは、MEPまたはMIPデータベースに宛先MACアドレスが検出されました。

関連コマンド

- **cfd linktrace auto-detection**
- **display cfd linktrace-reply**

2.1.5 cfd linktrace auto-detection

Syntax

cfd linktrace auto-detection [**size** *size-value*]

undo cfd linktrace auto-detection

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

パラメータ

size *size-value*: 自動検出結果を保存するために使用するバッファサイズを指定します。設定範囲は 1～100 です。linktrace メッセージを送信するたびにバッファサイズが確保されます。最新の自動検出の結果を保存するバッファサイズのデフォルトは 5 です。

説明

cfd linktrace auto-detection コマンドは linktrace メッセージ（LT メッセージ）を自動で送信することを有効にします。

undo cfd linktrace auto-detection コマンドは linktrace メッセージを自動で送信することを無効にします。

LT メッセージを自動で送信することを有効にしたのち、ソース MEP が 3.5 回送信する間にターゲット MEP からの CCM フレームを受信しなれば、2 つの間のリンクは故障していると考えられ、LTM フレーム（LTM の宛先が宛先 MEP で、TTL は 255 です）が送信されます。MIP が応答した LTR にもとづいて、障害場所の特定ができます。

linktrace メッセージを自動で送信することを無効にすると、バッファ内の内容は削除されます。

例

LT メッセージを自動で送信することを有効にし、自動検出結果を保存するために使用するバッファサイズを 100 に指定します。

<Switch> system-view

[Switch] cfd linktrace auto-detection size 100

関連コマンド

- **cfd linktrace**
- **display cfd linktrace-reply auto-detection**

2.1.6 cfd loopback

Syntax

cfd loopback service-instance *instance-id* **mep** *mep-id* { **target-mac** *mac-address* | **target-mep** *target-mep-id* } [**number** *number*]

デフォルト

無効

View

すべての view

定義済みユーザロール

network-admin

パラメータ

service-instance *instance-id*: サービスインスタンス ID を指定します。設定範囲は 1～32767 です。

mep *mep-id*: 送信元 MEP の ID を指定します。設定範囲は 1～8191 です。

target-mac *mac-address*: MP の宛先 MAC アドレスを指定します。形式は H-H-H です。

target-map *target-mep-id*: 宛先 MEP の ID を指定します。設定範囲は 1～8191 です。

number *number*: LBM パケットを送信する数を指定します。設定範囲は 1～10 です。デフォルトは 5 です。

説明

cfd loopback コマンドは LBM が送信元 MEP から宛先 MP に送信し、LBR メッセージを受信できるように LB 機能を有効にします。

例

サービスインスタンス 1 の MEP1101 と MEP2001 間のリンク状態を確認するように LB を有効にします。（リンク状態が正常であると仮定します。）

<Switch> cfd loopback service-instance 1 mep 1101 target-mep 2001

```
Loopback to 0010-fc00-6512 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
```

サービスインスタンス 1 の MEP1101 と MEP2001 間のリンク状態を確認するように LB を有効にします。（リンク状態が異常であると仮定します。）

<Switch> cfd loopback service-instance 1 mep 1101 target-mep 2001

```
Loopback to 0010-fc00-6512 with the sequence number start from 1101-43404:
Sent: 5       Received: 0       Lost: 5
```

表 2-3 コマンド出力

フィールド	説明
Loopback to 0010-fc00-6512 with the sequence number start from 1101-43404	1101-43404で始まるシーケンス番号でLBMを送信します。
Reply from 0010-fc00-6512	MACアドレス0010-FC00-6512のMPからの応答です。

フィールド	説明
sequence number	LBRメッセージのシーケンス番号です。
Time=5ms	LBMメッセージが送信されてからLBRを受信するまでの間隔が5ミリ秒です。
Sent	LBMを送信した数です。
Received	LBRメッセージを受信した数です。
Lost	ロストLBRの数です。

2.1.7 cfd 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*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

md *md-name*: MD の名前を指定します。設定範囲は 1～43 です。英字、数字、以下の記号を含むことができます。アポストロフィー（'）、チルダ（~）、感嘆符（!）、アットマーク（@）、シャープ（#）、ダラーマーク（$）、パーセント（%）、キャロット（^）、アンパサンド（&）、アスタリスク（*）、括弧（{ }, ( ),[ ], < >）、ハイフン（-）、アンダーライン（_）、プラス（+）、イコール（=）、垂直バー（|）、コロン（:）、セミコロン（;）、逆クォート（`）、コンマ（,）、ドット（.）、スラッシュ（/）

index *index-value*: MD インデックスを指定します。設定範囲は 1～4294967295 です。指定しない場合、使用されていないインデックスのもっとも小さい番号が自動的に割り当てられます。システムが自動で割り当てるインデックスを使用することを推奨します。

level *level-value*: MD レベルを指定します。設定範囲は 0～7 です。

md-id: MEP が送信したパケットによって運ばれる MD 名を指定します。指定しない場合、MD 名は *md-name* となります。

dns *dns-name*: DNS 名の形式で MD 名を指定します。*dns-name* は DNS 名を示します。

mac *mac-address subnumber*: MAC アドレスと整数から構成される MD 名を指定します。*mac-address* は MD の MAC アドレスを示します。*subnumber* の設定範囲は 0～65535 です。

none: MEP によって送信されたパケットに MD 名が運ばれないように指定します。

説明

cfd md コマンドは MD を作成します。

undo cfd md コマンドは MD を削除します。

MD 名は IEEE802.1ag-2007 の表 21-19 に準拠する必要があります。

指定レベルで 1 つの MD を作成することができます。不正な MD 名あるいは既存の MD 名を指定した場合、MD を作成することができません。また MD インデックスが使用中である場合、MD を作成することができません。

MD を削除するとき、MD に関連する設定も削除されます。

例

MD レベルが 3 の MD 名 test_md1 を作成します。

<Switch> system-view

[Switch] cfd md test_md1 level 3

MD 名 test_md2 を作成し、MEP が送信したパケットによって運ばれる MD 名を MAC アドレス 1-1-1、整数 1 で設定します。

<Switch> system-view

[Switch] cfd md test_md2 level 5 md-id mac 1-1-1 1

2.1.8 cfd mep

Syntax

cfd mep *mep-id* **service-instance** *instance-id* { **inbound** | **outbound** }

undo cfd mep *mep-id* **service-instance** *instance-id*

デフォルト

設定なし

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

mep *mep-id*: MEP の ID を指定します。設定範囲は 1～8191 です。

service-instance *instance-id*: サービスインスタンス ID を指定します。設定範囲は 1～32767 です。

inbound: 内側向きの MEP を作成します。

outbound: 外側向きの MEP を作成します。

説明

cfd mep コマンドは MEP を作成します。

undo cfd mep コマンドは指定された MEP を削除します。

MEP を作成する際、指定したサービスインスタンスは、MEP が属している MD と MA を定義します。

MEP ID が関連するサービスインスタンスの MEP リストに含まれていない場合、MEP を作成することはできません。

コマンドを使用するとき以下のガイドラインに従ってください。

- Ethernet interface view で設定されたコマンドは、Ethernet インタフェースでのみ適用されます。
- aggregate interface view で設定されたコマンドは、アグリゲートインタフェースとアグリゲーションメンバポートでのみ適用されます。
- メンバポートがアグリゲーションインタフェースから削除した場合、アグリゲーションメンバポートでのみ適用されます。

例

サービスインスタンス 5 に MEP リストを作成し、GigabitEthernet 1/0/1 でサービスインスタンス 5 の内側向きの MEP3 を有効にします。

<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

関連コマンド

cfd meplist

2.1.9 cfd meplist

Syntax

cfd meplist *mep-list* **service-instance** *instance-id*

undo cfd meplist *mep-list* **service-instance** *instance-id*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

meplist *mep-list*: MEP ID のリストを指定します。形式は *mep-list* = { *mep-id* [**to** *mep-id*] }&<1-10>です。*mep-id* は MEP ID を示し、設定範囲は 1～8191 です。*&<1-10>* は最大 10 個の MEP ID の範囲を指定できることを示します。

service-instance *instance-id*: サービスインスタンス ID を指定します。設定範囲は 1～32767 です。

説明

cfd meplist コマンドは MEP リスト、およびローカル MEP と同一 MA でモニタされるリモート MEP の組み合わせを作成します。

undo cfd meplist コマンドは既存の MEP リストを削除します。

MEP リストを作成する前に、関連する MD、MA、サービスインスタンスを作成してください。

MEP リストを削除したのち、MEP リストをもとにしたすべてのローカルの MEP の設定が削除されます。

例

サービスインスタンス 5 の MEP9～MEP15 が含まれる MEP リストを作成します。

<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

関連コマンド

- **cfd md**

- **cfd service-instance**

2.1.10 cfd mip-rule

Syntax

cfd mip-rule { **default** | **explicit** } **service-instance** *instance-id*

undo cfd mip-rule [**default** | **explicit**] **service-instance** *instance-id*

デフォルト

MIP を作成するルールは設定されていません。システムは自動で MIP を作成しません。

View

System view

定義済みユーザロール

network-admin

パラメータ

default: デフォルトルールを指定します。インタフェースで低レベルの MIP が存在しない場合、現在のレベルで MIP が作成されます。インタフェースで MIP が設定されていない場合でも MIP が作成されます。

explicit: 明示ルールを指定します。インタフェースで低レベルの MIP が存在しない場合、現在のレベルで MIP がされます。インタフェースで低レベルの MEP が作成されたときのみ MIP を作成することができます。

service-instance *instance-id*: サービスインスタンス ID を指定します。設定範囲は 1～32767 です。

説明

cfd mip-rule コマンドは MIP を作成するルールを設定します。システムは設定されたルールに従い各ポートで MIP を自動的に作成します。

undo cfd mip-rule コマンドはデフォルトに戻します。

例

サービスインスタンス 5 の MIP 作成ルールをデフォルトに設定します。

<Switch> system-view

[Switch] cfd mip-rule default service-instance 5

2.1.11 cfd service-instance

Syntax

cfd service-instance *instance-id* **ma-id** { **icc-based** *icc-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*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

service-instance *instance-id*: サービスインスタンス ID を指定します。設定範囲は 1～32767 です。

ma-id: MA を作成します。

icc-based *icc-name*: ICC で定義した MA を指定します。設定範囲は 1～13 文字です。

integer *ma-num*: 整数で定義した MA を指定します。設定範囲は 0～65535 です。

string *ma-name*: 文字列で MA を指定します。設定範囲は 1～43 です。英字、数字、以下の記号を含むことができます。アポストロフィー（'）、チルダ（~）、感嘆符（!）、アットマーク（@）、シャープ（#）、ダラーマーク（$）、パーセント（%）、キャロット（^）、アンパサンド（&）、アスタリスク（*）、括弧（{ }, ( ),[ ], < >）、ハイフン（-）、アンダーライン（_）、プラス（+）、イコール（=）、垂直バー（|）、コロン（:）、セミコロン（;）、逆クォート（`）、コンマ（,）、ドット（.）、スラッシュ（/）

vlan-based [*vlan-id*]: VLAN ID で MA を指定します。設定範囲は 1～4094 です。*vlan-id* を指定しない場合、**vlan** *vlan-id* で指定された VLAN ID が使用されます。**vlan** *vlan-id* が指定されていない場合、**vlan-based** [*vlan-id*]の *vlan-id* を指定する必要があります。

ma-index *index-value*: MA インデックスを指定します。設定範囲は 1～4294967295 です。指定しない場合、使用されていないインデックスのもっとも小さい番号が自動的に割り当てられます。システムが自動で割り当てるインデックスを使用することを推奨します。

md *md-name*: MD の名前を指定します。設定範囲は 1～43 です。英字、数字、以下の記号を含むことができます。アポストロフィー（'）、チルダ（~）、感嘆符（!）、アットマーク（@）、シャープ（#）、ダラーマーク（$）、パーセント（%）、キャロット（^）、アンパサンド（&）、アスタリスク（*）、括弧（{ }, ( ),[ ], < >）、ハイフン（-）、アンダーライン（_）、プラス（+）、イコール（=）、垂直バー（|）、コロン（:）、セミコロン（;）、逆クォート（`）、コンマ（,）、ドット（.）、スラッシュ（/）

vlan *vlan-id*: MA が提供する VLAN を指定します。設定範囲は 1～4094 です。

説明

cfd service-instance コマンドは MD 名でサービスインスタンスを作成します。

undo cfd service-instance コマンドはサービスインスタンスを削除します。

サービスインスタンスは MD 内にある MA を示すため、数字で示されます。MD と MA はサービスインスタンスの MP で処理されたメッセージのレベルの属性と VLAN の属性を定義します。MA インデックスは MD の中の MA を一意に識別します。MA インデックスは異なる MD で使用することができます。

MD 名は IEEE802.1ag-2007 の表 21-19 に準拠する必要があります。

このコマンドは **vlan-based** [*vlan-id*]あるいは **vlan** *vlan-id* を使用して VLAN 属性を運ぶ MA を作成します。**vlan-based** [*vlan-id*]あるいは **vlan** *vlan-id* を指定しない場合、MA は VLAN 属性を運びません。

MD 名でサービスインスタンスを作成する前に関連する MD と MA を作成する必要があります。

サービスインスタンスを削除するとき、サービスインスタンスに関連する設定を削除する必要があります。

サービスインスタンスを削除すると、サービスインスタンスとサービスインスタンスに対応する MA との関係を解消します。MA 自身は削除されません。

例

レベル 3 の MD 名が test_md の MD を作成し、VLAN100 で MA を識別するサービスインスタンス 5 を作成します。

<Switch> system-view

[Switch] cfd md test_md level 3

[Switch] cfd service-instance 5 ma-id vlan-based md test_md vlan 100

関連コマンド

cfd md

2.1.12 display cfd linktrace-reply

Syntax

display cfd linktrace-reply [**service-instance** *instance-id* [**mep** *mep-id*]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

service-instance *instance-id*: サービスインスタンス ID を指定します。設定範囲は 1～32767 です。指定しない場合、すべてのサービスインスタンスのすべての MEP で保存された LTR の情報を表示します。

mep *mep-id*: MEP の ID を指定します。設定範囲は 1～8191 です。指定しない場合、すべての MEP で保存された LTR の情報を表示します。

説明

display cfd linktrace-reply コマンドは MEP で保存された LTR の情報を表示します。

このコマンドは **cfd linktrace** コマンドを実行して受信した LTR の情報のみを表示します。

例

各サービスインスタンスのすべての MEP で保存された LTR の情報を表示します。

<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
```

表 2-4 コマンド出力

フィールド	説明
Service instance	LTMを送信するMEPが所属するサービスインスタンスです。
MEP ID	LTMを送信するMEPのIDです。
MAC address	LTRメッセージの送信元MACアドレスです。
TTL	LTMが装置を通過するときのTTLの値です。
Last MAC	LTMメッセージの最終ホップの装置のMACアドレスです。

フィールド	説明
Relay action	転送する装置がMACアドレステーブルから宛先MACアドレスを検出したかどうかを示します。 CFDの標準バージョン（IEEE 802.1ag）が使用されたとき、以下のことを示します。 ● **Hit**—現在の装置は宛先装置です。 ● **FDB**—転送する装置は宛先MACアドレスを検出しました。 ● **MPDB**—宛先MACアドレスが見つかりませんでした。あるいは、MEPまたはMIPデータベースに宛先MACアドレスが検出されました。

関連コマンド

cfd linktrace

2.1.13 display cfd linktrace-reply auto-detection

Syntax

display cfd linktrace-reply auto-detection [**size** *size-value*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

size *size-value*: 自動検出結果を保存するために使用するバッファサイズを指定します。設定範囲は 1～100 です。指定しない場合、バッファのすべての情報が表示されます。

説明

display cfd linktrace-reply コマンドは自動的に送信された LTM への応答として、受信した LTR メッセージの内容を表示します。

このコマンドは **cfd linktrace auto-detection** コマンドを実行して受信した LTR の情報のみを表示します。

例

自動的に送信された LTM への応答として、受信した LTR メッセージの内容を表示します。

<Switch> display cfd linktrace-reply auto-detection

```
Service instance: 1      MEP ID: 1003   Time: 2014/05/22 10:43:57
Target MEP ID: 2005      TTL: 255
MAC address            TTL    Last MAC        Relay action
0000-fc00-6505          254    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: 2014/05/22 10:44:06
Target MEP ID: 2025      TTL: 255
MAC address            TTL    Last MAC        Relay action
0000-fc00-6508          61     000f-e269-a852   Hit
```

表 2-5 コマンド出力

フィールド	説明
Service instance	LTMを送信するMEPが所属するサービスインスタンスです。
MEP ID	LTMを送信するMEPのIDです。
Time	LTMを自動で送信した時間です。
Target MEP ID	宛先MEPのIDです。
TTL	LTMを自動で送信したときの初期TTLの値です。
MAC address	LTRメッセージの送信元MACアドレスです。
TTL	LTMが装置を通過するときのTTLの値です。
Last MAC	LTMメッセージの最終ホップの装置のMACアドレスです。
Relay action	転送する装置がMACアドレステーブルから宛先MACアドレスを検出したかどうかを示します。 CFDの標準バージョン（IEEE 802.1ag）が使用されたとき、以下のことを示します。 ● **Hit**—現在の装置は宛先装置です。 ● **FDB**—転送する装置は宛先MACアドレスを検出しました。 ● **MPDB**—宛先MACアドレスが見つかりませんでした。あるいは、MEPまたはMIPデータベースに宛先MACアドレスが検出されました。

関連コマンド

cfd linktrace auto-detection

2.1.14 display cfd md

Syntax

display cfd md

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display cfd md コマンドは MD の設定情報を表示します。

例

MD の設定情報を表示します。

<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        0001-0001-0001-1
3      4         md_3                                  NONE       Without ID
```

表 2-6 コマンド出力

フィールド	説明
Maintenance domains configured	設定されたMDの数です。
Level	MDのレベルです。
Index	MDのインデックスです。
Maintenance domain	MD名です。
MD format	MD名の形式です。 ● **CHARSTRING**—文字列の形式です。 ● **DNS**—DNS名です。 ● **MAC**—MACアドレスと整数です。 ● **NONE**—MD名が運ばれません。

フィールド	説明
MD ID	MD IDの値です。 ● MDの形式が**CHARSTRING**である場合、文字列です。 ● MDの形式が**DNS**である場合、DNS名です。 ● MDの形式が**MAC**である場合、MACアドレス-整数です。 ● MDの形式が**NONE**である場合、IDはありません。

2.1.15 display cfd mep

Syntax

display cfd mep *mep-id* **service-instance** *instance-id*

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

mep *mep-id*: MEP の ID を指定します。設定範囲は 1～8191 です。

service-instance *instance-id*: サービスインスタンス ID を指定します。設定範囲は 1～32767 です。

説明

display cfd mep コマンドは MEP の属性と動作情報を表示します。

例

サービスインスタンス 1 の MEP50 の属性と動作情報を表示します。

<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: Enable
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: 2014/03/06 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: 2014/03/06 13:01:34

Some other MEPs are transmitting the RDI bit.
```

表 2-7 コマンド出力

フィールド	説明
Interface	MDが属しているインタフェースです。
Maintenance domain	MEPが属しているMDです。（もしMD名がない場合、**Without ID** と表示されます。）
Maintenance domain index	MEPがある場所のMDのインデックスです。
Maintenance association	MEPが属しているMAです。
Maintenance association index	MEPがある場所のMAのインデックスです。
Level	MDのレベルです。

フィールド	説明
VLAN	MAが属しているVLANです。
Direction	MEPの方向です。
Current state	MEPの状態です。Activeあるいは Inactiveがあります。
CCM send	MEPがCCMを送信しているかどうかを示します。
FNG state	FNG (Fault Notification Generator)の状態です。 ● **FNG_RESET**—障害がクリアされました。 ● **FNG_DEFECT**—障害が検出されました。 ● **FNG_REPORT_DEFECT**—障害を通知します。 ● **FNG_DEFECT_REPORTED**—障害が通知されました。 ● **FNG_DEFECT_CLEARING**—障害がクリアされています。 このフィールドがサポートされていない場合、ハイフン(-)が表示されます。
CCM	CCMに関連する情報です。
Current state	送信したCCMの状態です。 ● **CCI_IDLE**—初期状態です。 ● **CCI_WAITING**—送信状態です。 このフィールドがサポートされていない場合、ハイフン(-)が表示されます。
Interval	CCMを送信する間隔です。 **Not Supported**はMEPがCCM送信をサポートしていないことを示します。
SendCCM	MEPによって送信されたCCMの数です。 このフィールドがサポートされていない場合、ハイフン(-)が表示されます。
Loopback	ループバックに関連する情報です。
NextSeqNumber	次に送信されるLBMのシーケンス番号です。
SendLBR	送信されたLBRの数です。MEPが内向きである場合、LBRの数はカウントされません。
ReceiveInOrderLBR	正常な順番で受信したLBRメッセージの数です。
ReceiveOutOrderLBR	受信した不正なLBRメッセージの数です。
Linktrace	linktraceに関連した情報です。
NextSeqNumber	次に送信されるLTMのシーケンス番号です。

フィールド	説明
SendLTR	送信されたLTRの数です。MEPが内向きである場合、LBRの数はカウントされません。
ReceiveLTM	受信されたLTMの数です。
No CCM received from some remote MEPs.	あるリモートMEPからCCMを受信するのに失敗しました。（この情報はあるCCMがロストしたときのみ表示されます）
One or more streams of error CCMs is received. The last received CCM:	1つ以上のCCMが受信されたとき最後のエラーCCMの内容を表示します。（この情報はエラーCCMを受信したのみ表示されます）
Maintenance domain	最後のエラーCCMメッセージのMDです。 このフィールドがサポートされていない場合、ハイフン(-)が表示されます。
Maintenance association	最後のエラーCCMメッセージのMAです。 このフィールドがサポートされていない場合、ハイフン(-)が表示されます。
MEP	最後のエラーCCMメッセージのMEPのIDです。 このフィールドがサポートされていない場合、ハイフン(-)が表示されます。
Sequence Number	最後のエラーCCMメッセージのシーケンス番号です。 このフィールドがサポートされていない場合、ハイフン(-)が表示されます。
Received Time	最後のエラーCCMメッセージを受信した時間です。 このフィールドがサポートされていない場合、ハイフン(-)が表示されます。
One or more streams of cross-connect CCMs is received. The last received CCM:	クロスコネクトのCCMを受信し、最後のクロスコネクトのCCMの内容を表示します。（クロスコネクトCCMを受信した場合のみ、この情報が表示されます。）
Some other MEPs are transmitting the RDI bit.	他のMEPから受信したRDIフラグビットのCCMです。（この情報は、このタイプのCCMを受信した場合にのみ表示されます）

2.1.16 display cfd meplist

Syntax

display cfd meplist [**service-instance** *instance-id*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

service-instance *instance-id*: サービスインスタンス ID を指定します。設定範囲は 1～32767 です。指定しない場合、すべてのサービスインスタンスの MEP リストを表示します。

説明

display cfd meplist コマンドはサービスインスタンスの MEP リストを表示します。

例

サービスインスタンス 5 の MEP リストを表示します。

<Switch> display cfd meplist service-instance 5

```
Service instance: 5
MEP list: 1 to 20, 30, 50.
```

2.1.17 display cfd mp

Syntax

display cfd mp [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: ポートタイプとポート番号で指定された MP の情報を表示します。指定しない場合、すべてのポートの MP の情報を表示します。

説明

display cfd mp コマンドは MP の情報を表示します。

表示される情報は、ポート名でソートされます。ポートで、VLAN を提供する MP を表示し、そして VLAN を提供しない MP を表示します。VLAN を提供する MP は VLAN ID の昇順で表示されます。同一 VLAN で、MIP と MEP（高いレベルから低いレベル）の昇順で表示します。VLAN を提供しない MEP は高いレベルから低いレベルでソートされます。

例

すべてのポートの MP の情報を表示します。

<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
```

表 2-8 コマンド出力

フィールド	説明
Interface GigabitEthernet1/0/1 VLAN 100	GigabitEthernet 1/0/1のVLANのMPの情報です。
MIP	MPのMIPです。
Level	MPが属しているMDのレベルです。
Service instance	MPが属しているサービスインスタンスです。
Maintenance domain	MPが属しているMDです。
Maintenance domain index	MPが属しているMDのインデックスです。
Maintenance association	MPが属しているMAです。
Maintenance association index	MPが属しているMAのインデックスです。
Direction	MEPの方向です。内側向き、外側向きがあります。

2.1.18 display cfd remote-mep

Syntax

display cfd remote-mep service-instance *instance-id* **mep** *mep-id*

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

service-instance *instance-id*: サービスインスタンス ID を指定します。設定範囲は 1～32767 です。

mep *mep-id*: MEP の ID を指定します。設定範囲は 1～8191 です。

説明

display cfd remote-mep コマンドはリモート MEP の情報を表示します。

例

サービスインスタンス 4 の MEP10 のリモート MEP の情報を表示します。

<Switch> display cfd remote-mep service-instance 4 mep 10

```
MEP ID   MAC address     State       Time                MAC status
20       f474-8800-6565  OK          2014/03/06 02:36:38   UP
30       f474-8827-6502  OK          2014/03/06 02:36:38   DOWN
40       f474-8800-6510  FAILED      2014/03/06 02:36:39   DOWN
50       f474-8852-baa0  OK          2014/03/06 02:36:44   DOWN
60       0010-fc00-6502  OK          2014/03/06 02:36:42   DOWN
```

表 2-9 コマンド出力

フィールド	説明
MEP ID	リモートMEPのIDです。
MAC address	リモートMEP装置のMACアドレスです。 このフィールドがサポートされていない場合、ハイフン(-)が表示されます。
State	リモートMEPの動作状態です。OK、FAILEDがあります。

フィールド	説明
Time	最後にMEPがFAILEDあるいはOKの状態になったときの時間です。 このフィールドがサポートされていない場合、ハイフン(-)が表示されます。
MAC status	リモートMEPから最後に受信したCCMのインタフェースの状態です。 ● **UP**—インタフェースがパケットを通過する準備ができています。 ● **DOWN**—インタフェースがパケットを通過することができません。 ● **TESTING**—インタフェースがあるテストモード中です。 ● **UNKNOWN**—インタフェースの状態が不明です。 ● **DORMANT**—インタフェースがパケットを通過する状態ではありません。そのかわり、ある外部イベントの待ち状態にあります。 ● **NOT-PRESENT**—インタフェースのある構成が欠けています。 ● **LLD**—下位レイヤのインタフェースの状態であるため、ダウンしています。 このフィールドがサポートされていない場合、ハイフン(-)が表示されます。

2.1.19 display cfd service-instance

Syntax

display cfd service-instance [*instance-id*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

instance-id: サービスインスタンス ID を指定します。設定範囲は 1～32767 です。指定しない場合、すべてのサービスインスタンスの設定情報を表示します。

説明

display cfd service-instance コマンドはサービスインスタンスの設定情報を表示します。

例

すべてのサービスインスタンスの設定情報を表示します。

<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
```

表 2-10 コマンド出力

フィールド	説明
Service instances are configured.	設定されたサービスインスタンスの数です。
Service instance	サービスインスタンスのIDです。
Maintenance domain	サービスインスタンスのMDです。 （もしMD名がない場合、**Without ID**と表示されます。）
Maintenance domain index	サービスインスタンスが属しているMDのインデックスです。
Maintenance association:	サービスインスタンスのMAです。
Maintenance association index	サービスインスタンスが属しているMAのインデックスです。
Level	MDレベルです。
VLAN	MAが属しているVLANです。

フィールド	説明
MIP rule	サービスインスタンスで設定されたMIPの作成ルールです。
CCM interval	CCMを送信する間隔です。
Direction	サービスインスタンスで設定されたMEPの方向です。
MEP ID	サービスインスタンスで設定されたMEPのIDです。
Interface	サービスインスタンスで設定されたMEPのインタフェースです。

2.1.20 display cfd status

Syntax

display cfd status

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display cfd status コマンドは CFD の状態を表示します。

例

CFD の状態を表示します。

<Switch> display cfd status

```
CFD is enabled.
```

目次

このセクションのページは **10-x-x** です。

3 章 DLDP 3-1
3.1 DLDP 設定コマンド 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 3-6
3.1.5 dldp delaydown-timer 3-7
3.1.6 dldp enable 3-8
3.1.7 dldp global enable 3-8
3.1.8 dldp interval 3-9
3.1.9 dldp port unidirectional-shutdown 3-10
3.1.10 dldp unidirectional-shutdown 3-11
3.1.11 reset dldp statistics 3-12

3章 DLDP

3.1 DLDP設定コマンド

3.1.1 display dldp

Syntax

display dldp [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: ポートのタイプと番号を指定します。指定しない場合、グローバルとポート指定の DLDP の設定を表示します。

説明

display dldp コマンドは DLDP の情報を表示します。

例

グローバルとポート指定の DLDP の設定を表示します。

<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)
```

GigabitEthernet 1/0/1 の DLDP の設定を表示します。

<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
```

表 3-1 コマンド出力

フィールド	説明
DLDP global status	グローバルのDLDPの状態です。Enabled、Disabledがあります。
DLDP advertisement interval	接続先との関係を維持するためにAdvertisementパケットを送信する間隔です。単位は秒です。
DLDP authentication-mode	DLDP認証モードです。None、Simple、MD5があります。
DLDP authentication-password	DLDP認証のパスワードです。 ● ******—パスワードが設定されています。 ● **Not configured**—認証モードが設定されていますが、パスワードは設定されていません。
DLDP unidirectional-shutdown mode	片方向リンクが検出されたのち、ポートがシャットダウンモードになりました。auto、manual、hybridがあります。
DLDP port unidirectional-shutdown mode	片方向リンクが検出されたのち、インタフェースのポートがシャットダウンモードになりました。Auto、Manualまたはhybridがあります。インタフェースにポートシャットダウンモードが設定されていない場合、このフィールドには**None**と表示されます。
DLDP delaydown-timer value	DelayDownタイマの設定です。単位は秒です。
Number of enabled ports	DLDPが有効なポート数です。
Interface	DLDPが有効なポートのインデックスです。

フィールド	説明
DLDP port state	ポートのDLDPの状態です。 ● Bidirectional ● Inactive ● Initial ● Unidirectional
Number of the port's neighbors	ネイバの現在の番号です。
Maximum number ever detected	ポートで一度検出されたネイバの最大数です。 このフィールドは、ネイバの現在の数が、一度検出されたネイバの最大数と異なるときのみ表示します。
Neighbor MAC address	ネイバのMACアドレスです。
Neighbor port index	ネイバポートのインデックスです。
Neighbor state	ネイバ状態です。Confirmed、Unconfirmedがあります。
Neighbor aged time	ネイバのエージング時間です。

3.1.2 display dldp statistics

Syntax

display dldp statistics [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: ポートのタイプと番号を指定します。指定しない場合、すべてのインタフェースの DLDP パケットの統計情報を表示します。

説明

display dldp statisticsコマンドは DLDP パケットの統計情報を表示します。

例

すべてのインタフェースの DLDP パケットの統計情報を表示します。

<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
```

表 3-2 コマンド出力

フィールド	説明
Interface	ポートのインデックスです。
Packets sent	DLDPパケットを送信した総数です。
Packets received	DLDPパケットを受信した総数です。
Invalid packets received	不正パケットを受信した数です。
Loop packets received	ループバックパケットを受信した数です。
Authentication failed packets received	認証されなかったパケットを受信した数です。
Valid packets received	有効なパケットを受信した数です。

関連コマンド

reset dldp statistics

3.1.3 dldp authentication-mode

Syntax

dldp authentication-mode { **md5** | **none** | **simple** }

undo dldp authentication-mode

デフォルト

none

View

System view

定義済みユーザロール

network-admin

パラメータ

md5: MD5 認証モードを指定します。

none: 認証を行わないように指定します。

simple: プレーンテキストの認証モードを指定します。

説明

dldp authentication-mode コマンドは DLDP の認証を設定します。

undo dldp authentication-mode コマンドはデフォルトに戻します。

DLDP を正常に動作させるため、リンクの両端で DLDP の認証モードとパスワードを同一にしてください。

認証モードを設定した後、認証のパスワードを設定しない場合、認証モードは none モードになります。

例

DLDP の認証モードをプレーンテキストで設定し、パスワードを abc に設定します。（Device A と Device B が DLDP リンクで接続されていると仮定します）

- Device A の設定

<DeviceA> system-view

[DeviceA] dldp authentication-mode simple

[DeviceA] dldp authentication-password simple abc

- Device B の設定

<DeviceB> system-view

[DeviceB] dldp authentication-mode simple

[DeviceB] dldp authentication-password simple abc

関連コマンド

- **display dldp**
- **dldp authentication-password**

3.1.4 dldp authentication-password

Syntax

dldp authentication-password { **cipher** | **simple** } *string*

undo dldp authentication-password

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

cipher: 暗号パスワードを設定します。

simple: プレーンテキストパスワードを設定します。セキュリティのため、プレーンテキストで設定されたパスワードを含むすべての DLDP 認証のパスワードは暗号テキストで保存されます。

string: パスワードを指定します。プレーンテキストの設定範囲は 1～16 文字です。大文字、小文字を区別します。暗号パスワードテキストの設定範囲は 1～53 文字です。大文字、小文字を区別します。

説明

dldp authentication-password コマンドは DLDP 認証のパスワードを設定します。

undo dldp authentication-password コマンドはデフォルトに戻します。

DLDP を正常に動作させるため、リンクの両端で DLDP の認証モードとパスワードを同一にしてください。

認証モードを設定した後、認証のパスワードを設定しない場合、認証モードは none モードになります。

例

DLDP の認証モードをプレーンテキストで設定し、パスワードを abc に設定します。（Device A と Device B が DLDP リンクで接続されていると仮定します）

- Device A の設定

<DeviceA> system-view

[DeviceA] dldp authentication-mode simple

[DeviceA] dldp authentication-password simple abc

- Device B の設定

<DeviceB> system-view

[DeviceB] dldp authentication-mode simple

[DeviceB] dldp authentication-password simple abc

関連コマンド

- **display dldp**
- **dldp authentication-mode**

3.1.5 dldp delaydown-timer

Syntax

dldp delaydown-timer *time*

undo dldp delaydown-timer

デフォルト

1 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

time: DelayDown タイマを指定します。設定範囲は 1～5 秒です。

説明

dldp delaydown-timer コマンドは DelayDown タイマを設定します。

undo dldp delaydown-timer コマンドはデフォルトに戻します。

このコマンドを使用して設定された DelayDown タイマはすべての DLDP が有効なポートに適用されます。

例

DelayDown タイマを 2 秒に設定します。

<Switch> system-view

[Switch] dldp delaydown-timer 2

関連コマンド

display dldp

3.1.6 dldp enable

Syntax

dldp enable

undo dldp enable

デフォルト

無効

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

説明

dldp enable コマンドはポートで DLDP を有効にします。

undo dldp enable コマンドはポートで DLDP を無効にします。

グローバルとポートで DLDP を有効にしたのち、DLDP が適用されます。

例

グローバルで DLDP を有効にし、GigabitEthernet 1/0/1 で DLDP を有効にします。

<Switch> system-view

[Switch] dldp global enable

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] dldp enable

関連コマンド

- **display dldp**
- **dldp global enable**

3.1.7 dldp global enable

Syntax

dldp global enable

undo dldp global enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

dldp global enable コマンドはグローバルで DLDP を有効にします。

undo dldp global enable コマンドはグローバルで DLDP を無効にします。

グローバルとポートで DLDP を有効にしたのち、DLDP が適用されます。

例

グローバルで DLDP を有効にします。

<Switch> system-view

[Switch] dldp global enable

関連コマンド

- **display dldp**
- **dldp enable**

3.1.8 dldp interval

Syntax

dldp interval *interval*

undo dldp interval

デフォルト

5 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

interval: Advertisement パケットを送信する間隔を指定します。設定範囲は 1～100 秒です。

説明

dldp interval コマンドは Advertisement パケットを送信する間隔を設定します。

undo dldp interval コマンドはデフォルトに戻します。

このコマンドはすべての DLDP が有効なポートに適用されます。

DLDP を正常に動作させるため、リンクの両端で Advertisement パケットを送信する間隔を同一にしてください。

例

Advertisement パケットを送信する間隔を 20 秒に設定します。

<Switch> system-view

[Switch] dldp interval 20

関連コマンド

display dldp

3.1.9 dldp port unidirectional-shutdown

Syntax

dldp port unidirectional-shutdown { **auto | hybrid** | **manual** }

undo dldp port unidirectional-shutdown

デフォルト

グローバル

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

auto: ポートシャットダウンモードを自動モードとして指定します。このモードでは DLDP が片方向リンクを検出したとき、DLDP は片方向リンクのポートをシャットダウンします。リンクが双方向になると、DLDP はシャットダウンされたポートを起動します。

hybrid: ポートシャットダウンモードをハイブリッドモードとして指定します。このモードでは、DLDP が片方向リンクを検出すると、片方向ポートをシャットダウンし、リンク検出を停止します。リンクステータスを確認するには、**undo shutdown** コマンドを使用してポートを起動します。リンクが双方向になると、ポートは双方向になります。

manual: ポートシャットダウンモードを手動モードとして指定します。このモードでは DLDP が片方向リンクを検出したとき、DLDP は関連したポートをシャットダウンしません。手動でシャットダウンする必要があります。リンクステータスを確認するには、**undo shutdown** コマンドを使用してポートを起動します。リンクが双方向になると、ポートは双方向になります。

説明

dldp port unidirectional-shutdown コマンドはインタフェースのポートシャットダウンモードを設定します。

undo dldp port unidirectional-shutdown コマンドはデフォルトに戻します。

DLDP で片方向リンクが検出された場合は、インタフェースおよびケーブルの障害をトラブルシューティングする必要があります。

インタフェースのポートシャットダウンモードの設定は、現在のインタフェースにのみ有効で、グローバルポートシャットダウンモードの設定よりも優先されます。

例

GigabitEthernet 1/0/1 のポートシャットダウンモードを **manual** に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] dldp port unidirectional-shutdown manual

関連コマンド

- **display dldp**
- **dldp unidirectional-shutdown**

3.1.10 dldp unidirectional-shutdown

Syntax

dldp unidirectional-shutdown { **auto** | **hybrid** | **manual** }

undo dldp unidirectional-shutdown

デフォルト

auto

View

System view

定義済みユーザロール

network-admin

パラメータ

auto: ポートシャットダウンモードを自動モードとして指定します。このモードでは DLDP が片方向リンクを検出したとき、DLDP は片方向リンクのポートをシャットダウンします。リンクが双方向に回復したとき、DLDP はシャットダウンのポートを up に変更します。

hybrid: ポートシャットダウンモードをハイブリッドモードとして指定します。このモードでは、DLDP が片方向リンクを検出すると、片方向ポートをシャットダウンし、リンク検出を停止します。リンクステータスを確認するには、**undo shutdown** コマンドを使用してポートを起動します。リンクが双方向になると、ポートは双方向になります。

manual: ポートシャットダウンモードを手動モードとして指定します。このモードでは DLDP が片方向リンクを検出したとき、DLDP は関連したポートをシャットダウンしません。手動でシャットダウンする必要があります。リンクが双方向に回復したとき、手動でポートを up にする必要があります。

説明

dldp unidirectional-shutdown コマンドはポートシャットダウンモードを設定します。

undo dldp unidirectional-shutdown コマンドはデフォルトに戻します。

例

ポートシャットダウンモードを手動モードに設定します。

<Switch> system-view

[Switch] dldp unidirectional-shutdown manual

関連コマンド

- **display dldp**
- **dldp port unidirectional-shutdown**

3.1.11 reset dldp statistics

Syntax

reset dldp statistics [**interface** *interface-type interface-number*]

View

User view

定義済みユーザロール

network-admin

パラメータ

interface *interface-type interface-number*: ポートのタイプと番号を指定します。指定しない場合、すべてのインタフェースの DLDP パケットの統計情報を削除します。

説明

reset dldp statistics コマンドは DLDP パケットの統計情報を削除します。

例

すべてのインタフェースの DLDP パケットの統計情報を削除します。

<Switch> reset dldp statistics

関連コマンド

display dldp statistics

目次

このセクションのページは **10-x-x** です。

4 章 RRPP 4-1
4.1 RRPP 設定コマンド 4-1
4.1.1 control-vlan 4-1
4.1.2 display rrpp brief 4-2
4.1.3 display rrpp ring-group 4-5
4.1.4 display rrpp statistics 4-6
4.1.5 display rrpp verbose 4-10
4.1.6 domain ring 4-15
4.1.7 protected-vlan 4-16
4.1.8 reset rrpp statistics 4-17
4.1.9 ring 4-18
4.1.10 ring enable 4-20
4.1.11 rrpp domain 4-21
4.1.12 rrpp enable 4-22
4.1.13 rrpp ring-group 4-23
4.1.14 snmp-agent trap enable rrpp 4-24
4.1.15 timer 4-25

4章 RRPP

4.1 RRPP設定コマンド

4.1.1 control-vlan

Syntax

control-vlan *vlan-id*

undo control-vlan

デフォルト

設定なし

View

RRPP domain view

定義済みユーザロール

network-admin

パラメータ

vlan-id: プライマリコントロール VLAN の ID を指定します。設定範囲は 2～4093 です。

説明

control-vlan コマンドはRRPP ドメインのプライマリコントロールVLAN を設定します。

undo control-vlan コマンドは RRPP ドメインからプライマリコントロール VLAN を削除します。

RRPP ドメインのコントロール VLAN を設定するとき、プライマリコントロール VLAN のみを設定する必要があります。システムは自動でセカンダリコントロール VLAN を設定します。セカンダリコントロール VLAN ID としてプライマリコントロール VLAN ID に 1 を加算した VLAN を自動的に割り当てます。コントロール VLAN の設定を正常に行うため、2 つのコントロール VLAN の ID が連続し、ID が未割り当てであることを確認してください。

RRPPDU の転送を正常に行うため、以下のガイドラインに従ってください。

- コントロール VLAN として RRPP リングにアクセスするデフォルト VLAN を設定しないでください。
- コントロール VLAN で QinQ あるいは VLAN マッピングを有効にしないでください。

RRPP ドメインの RRPP リングを設定した後、ドメインのプライマリコントロール VLAN を削除あるいは変更することはできません。プライマリコントロール VLAN を削除あるいは変更する場合、**undo control-vlan** コマンドを使用します。

例

RRPP ドメイン 1 のプライマリコントロール VLAN として VLAN 100 を設定します。（VLAN100、VLAN101 が割り当てられていないと仮定します。）

<Switch> system-view

[Switch] rrpp domain 1

[Switch-rrpp-domain1] control-vlan 100

4.1.2 display rrpp brief

Syntax

display rrpp brief

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display rrpp brief コマンドは RRPP の概要情報を表示します。

例

RRPP の概要情報を表示します。

<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
```

表 4-1 コマンド出力

フィールド	説明
Flags for node mode	RRPPノードモードです。 • **M**—マスタモードです。 • **T**—トランジットモードです。 • **E**—エッジモードです。 • **A**—アシスタントエッジモードです。
RRPP protocol status	RRPPの状態です。 • **Enabled**—グローバルで有効です。 • **Disabled**—グローバルで無効です。
Domain ID	RRPPのドメインIDです。
Control VLAN	RRPPドメインのプライマリ、セカンダリコントロールVLANです。
Protected VLAN	RRPPドメインによって保護されたVLANに対応するMSTIです。VLANインスタンスマッピングを表示する場合、**display stp region-configuration**コマンドを使用します。（コマンドマニュアルのセクション3 *アクセス”STP”*を参照してください。）
Hello timer	Helloタイマの値です。単位は秒です。
Fail timer	Failタイマの値です。単位は秒です。
Fast detection status	Fast detectionの状態です。EnabledあるいはDisabledがあります。このフィールドは現在のソフトウェアバージョンでサポートしていません。

フィールド	説明
Fast-Hello timer	Fast-Helloタイマの値です。単位はミリ秒です。 このフィールドは現在のソフトウェアバージョンでサポートしていません。
Fast-Fail timer	Fast-Failタイマの値です。単位はミリ秒です。 このフィールドは現在のソフトウェアバージョンでサポートしていません。
Fast-Edge-Hello timer	Fast-Edge-Helloタイマの値です。単位はミリ秒です。 このフィールドは現在のソフトウェアバージョンでサポートしていません。
Fast-Edge-Fail timer	Fast-Edge-Failタイマの値です。単位はミリ秒です。 このフィールドは現在のソフトウェアバージョンでサポートしていません。
Ring ID	RRPPリングのIDです。
Ring level	RRPPリングのレベルです。 • **0**—プライマリリングです。 • **1**—サブリングです。
Primary/Common port	ノードモードがマスタノードあるいはトランジットノードであるとき、このフィールドはプライマリポートを表示します。 ノードのモードがエッジノードあるいはアシスタンドエッジノードであるとき、このフィールドは共通ポートを表示します。 以下の状況の発生するときハイフン（-）を表示します。 • ポートがリングに設定されていません。 • ポートがリンクアグリゲーショングループのメンバです。
Secondary/Edge port	ノードモードがマスタノードあるいはトランジットノードであるとき、このフィールドはセカンダリポートを表示します。 ノードのモードがエッジノードあるいはアシスタンドエッジノードであるとき、このフィールドはエッジポートを表示します。 以下の状況の発生するときハイフン（-）を表示します。 • ポートがリングに設定されていません。 • ポートがリンクアグリゲーショングループのメンバです。
Enable status	RRPPリングの状態です。 • **Yes**—有効です。 • **No**—無効です。

4.1.3 display rrpp ring-group

Syntax

display rrpp ring-group [*ring-group-id*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ring-group-id: RRPP リンググループの ID を指定します。設定範囲は 1～64 です。指定しない場合、すべてのリンググループの設定を表示します。

説明

display rrpp ring-group コマンドは RRPP リンググループの設定を表示します。

エッジノードの RRPP リンググループでは、Edge-Hello パケットを送信するサブリングも表示します。

例

すべての RRPP リンググループの設定を表示します。

<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
```

表 4-2 コマンド出力

フィールド	説明
Ring group 1	RRPPリンググループ1です。
Domain 1 ring 1 to 3, 5	RRPPドメイン1のリング1、2、3、5を含むリンググループのサブリングです。

フィールド	説明
Domain 1 ring 1 is the sending ring	RRPPドメイン1のリンググループの送信リングが1です。

4.1.4 display rrpp statistics

Syntax

display rrpp statistics domain *domain-id* [**ring** *ring-id*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

domain *domain-id*: RRPP ドメインの ID を指定します。設定範囲は 1～128 です。

ring *ring-id*: RRPP リングの ID を指定します。設定範囲は 1～128 です。指定しない場合、指定した RRPP ドメインのすべてのリングの RRPPDU の統計情報を表示します。

説明

display rrpp statistics コマンドは RRPPDU の統計情報を表示します。

ポートが 2 つ以上のリングに属している場合、RRPPDU の統計情報は、リングごとに取得され、表示します。

リングが非アクティブからアクティブ状態に遷移すると、リングのパケットのカウントを初期化します。

例

RRPP ドメイン 2 のすべてのリングの RRPPDU の統計情報を表示します。

<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
```

表 4-3 コマンド出力

フィールド	説明
Ring ID	RRPPのリングIDです。

フィールド	説明
Ring level	RRPPのリングレベルです。 • **0**—プライマリリングです。 • **1**—サブリングです。
Node mode	ノードモードです。 • マスタノードです。 • トランジットノードです。 • エッジノードです。 • アシスタンドエッジノードです。
Active status	RRPPのリング状態です。 • **Yes**—アクティブです。 • **No**—非アクティブです。
Primary port	プライマリポートのフィールドは、ノードのモードがマスタノードあるいはトランジットノードであることを示します。 以下の状況の発生するときハイフン（-）を表示します。 • ポートがリングに設定されていません。 • ポートがリンクアグリゲーショングループのメンバです。
Secondary port	セカンダリポートのフィールドは、ノードのモードがマスタノードあるいはトランジットノードであることを示します。 以下の状況の発生するときハイフン（-）を表示します。 • ポートがリングに設定されていません。 • ポートがリンクアグリゲーショングループのメンバです。
Common port	共通ポートのフィールドは、ノードのモードがエッジノードあるいはアシスタントエッジノードであることを示します。 以下の状況の発生するときハイフン（-）を表示します。 • ポートがリングに設定されていません。 • ポートがリンクアグリゲーショングループのメンバです。

フィールド	説明
Edge port	エッジポートのフィールドは、ノードのモードがエッジノードあるいはアシスタントエッジノードであることを示します。 以下の状況の発生するときハイフン（-）を表示します。 ● ポートがリングに設定されていません。 ● ポートがリンクアグリゲーショングループのメンバです。
Fast-Hello packets	ポートのFast-Helloパケットの統計情報です。 ● **Sent**—ポートで送信したFast-Helloパケットの数です。 ● **Received**—ポートで受信したFast-Helloパケットの数です。 このフィールドは現在のソフトウェアバージョンでサポートしていません。
Fast-Edge-Hello packets	ポートのFast-Edge-Helloパケットの統計情報です。 ● **Sent**—ポートで送信したFast-Edge-Helloパケットの数です。 ● **Received**—ポートで受信したFast-Edge-Helloパケットの数です。 このフィールドは現在のソフトウェアバージョンでサポートしていません。
Packet direct	ポートのパケット転送方向です。 ● **Out**—パケットの送信方向です。 ● **In**—パケットの受信方向です。
Hello	ポートで送受信されたHelloパケットの統計情報です。
Link down	ポートで送受信されたLink-Downパケットの統計情報です。
Common flush FDB	ポートで送受信されたCommon-Flush-FDBパケットの統計情報です。
Complete flush FDB	ポートで送受信されたComplete-Flush-FDBパケットの統計情報です。
Edge hello	ポートで送受信されたEdge-Helloパケットの統計情報です。
Major fault	ポートで送受信されたMajor-Faultパケットの統計情報です。
Total	ポートで送受信された以下のパケットの総数です。 RRPPのHelloパケット、Link-Downパケット、Common-Flush-FDBパケット、Complete-Flush-FDBパケット、Edge-Helloパケット、Major-Faultパケット

関連コマンド

reset rrpp statistics

4.1.5 display rrpp verbose

Syntax

display rrpp verbose domain *domain-id* [**ring** *ring-id*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

domain *domain-id*: RRPP ドメインの ID を指定します。設定範囲は 1～128 です。

ring *ring-id*: RRPP リングの ID を指定します。設定範囲は 1～128 です。指定しない場合、指定した RRPP ドメインのすべてのリングの詳細情報を表示します。

説明

display rrpp verbose コマンドは RRPP の詳細情報を表示します。

例

RRPP ドメイン 2 のすべてのリングの詳細情報を表示します。

<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: -
```

表 4-4 コマンド出力

フィールド	説明
Domain ID	RRPPドメインIDです。
Control VLAN	RRPPドメインのコントロールVLANです。 ● **Primary**—プライマリコントロールVLANです。 ● **Secondary**—セカンダリコントロールVLANです。
Protected VLAN	RRPPドメインによって保護されたVLANに対応するMSTIです。 VLANインスタンスマッピングを表示する場合、**display stp region-configuration**コマンドを使用します。（コマンドマニュアルのセクション3 *アクセス" STP"* を参照してください。
Hello timer	Helloタイマの値です。単位は秒です。
Fail timer	Failタイマの値です。単位は秒です。
Fast detection status	Fast detectionメカニズムの状態です。EnabledあるいはDisabledがあります。 このフィールドは現在のソフトウェアバージョンでサポートしていません。
Fast-Hello timer	Fast-Helloタイマの値です。単位はミリ秒です。 このフィールドは現在のソフトウェアバージョンでサポートしていません。
Fast-Fail timer	Fast-Failタイマの値です。単位はミリ秒です。 このフィールドは現在のソフトウェアバージョンでサポートしていません。
Fast-Edge-Hello timer	Fast-Edge-Helloタイマの値です。単位はミリ秒です。 このフィールドは現在のソフトウェアバージョンでサポートしていません。
Fast-Edge-Fail timer	Fast-Edge-Failタイマの値です。単位はミリ秒です。 このフィールドは現在のソフトウェアバージョンでサポートしていません。

フィールド	説明
Ring ID	RRPPリングIDです。
Ring level	RRPP リングレベルです。 • **0**—プライマリリングです。 • **1**—サブリングです。
Node mode	ノードモードです。 • マスタノードです。 • トランジットノードです。 • エッジノードです。 • アシスタントエッジノードです。

フィールド	説明
Ring state	RRPPリング状態です。 ● マスターノードでの可能な状態： o Completed—リングが正常です。 o Failed—リングが閉じていません。 o Unknown—RRPPドメインが無効です。 ● トランジットノードまたはエッジノードでの可能な状態： o LinkUp—ノード上の全てのポートがアップしています。 o LinkDown—ノード上の少なくとも1つのポートがダウンしています。 o PreForward—ノード上のポートがブロックされています。 o Unknown—RRPPドメインが無効です。 ● アシスタントエッジノードでの可能な状態： o LinkUp—ノード上の全てのポートがアップしています。 o LinkDown—ノード上の少なくとも1つのポートがダウンしています。 o PreForward—ノード上のポートがブロックされています。 o LinkUpNotify—LinkUp状態でEdge-Helloパケットを受信しません。 o LinkDnNotify—LinkDown状態でEdge-Helloパケットを受信しません。 o PreForwardNotify—直接接続されたエッジノードのポートがアップする、またはPreForward状態でアシスタントエッジノードがEdge-Helloパケットを受信しません。 Unknown—RRPPドメインが無効です。
Enable status	RRPPリングの状態です。 ● **Yes**—有効です。 ● **No**—無効です。

フィールド	説明
Active status	RRPPリングの状態です。 ● **Yes**—アクティブです。 ● **No**—非アクティブです。 RRPPとRRPPリングが有効である場合、RRPPリングのみアクティブにすることができます。このフィールドはRRPPが有効かどうかを識別します。
Primary port	プライマリポートのフィールドは、ノードのモードがマスタノードあるいはトランジットノードであることを示します。 以下の状況の発生するときハイフン（-）を表示します。 ● ポートがリングに設定されていません。 ● ポートがリンクアグリゲーショングループのメンバです。
Secondary port	セカンダリポートのフィールドは、ノードのモードがマスタノードあるいはトランジットノードであることを示します。 以下の状況の発生するときハイフン（-）を表示します。 ● ポートがリングに設定されていません。 ● ポートがリンクアグリゲーショングループのメンバです。
Common port	共通ポートのフィールドは、ノードのモードがエッジノードあるいはアシスタントエッジノードであることを示します。 以下の状況の発生するときハイフン（-）を表示します。 ● ポートがリングに設定されていません。 ● ポートがリンクアグリゲーショングループのメンバです。
Edge port	エッジポートのフィールドは、ノードのモードがエッジノードあるいはアシスタントエッジノードであることを示します。 以下の状況の発生するときハイフン（-）を表示します。 ● ポートがリングに設定されていません。 ● ポートがリンクアグリゲーショングループのメンバです。

フィールド	説明
Port status	ポートの状態です。Down、up、blockedがあります。 以下の状況の発生するときハイフン（-）を表示します。 ● リングが非アクティブです。 ● ポートがリングに設定されていません。 ● ポートがリンクアグリゲーショングループのメンバです。

4.1.6 domain ring

Syntax

domain *domain-id* **ring** *ring-id-list*

undo domain *domain-id* [**ring** *ring-id-list*]

デフォルト

設定なし

View

RRPP ring group view

定義済みユーザロール

network-admin

パラメータ

domain-id: RRPP ドメインの ID を指定します。設定範囲は 1～128 です。

ring *ring-id-list*: RRPP サブリングの ID を指定します。半角スペースで区切り 10 まで指定するか、RRPP サブリングの ID の範囲を指定します。設定範囲は 1～128 です。指定しない場合、指定したドメインのリンググループからすべてのサブリングを削除します。

説明

domain ring コマンドは RRPP リンググループのサブリングを設定します。

undo domain ring コマンドは RRPP リンググループからサブリングを削除します。

エッジノード、アシスタントエッジノードの RRPP リンググループを設定するとき、以下のガイドラインに従ってください。

- リンググループにアクティブリングを割り当てるとき、最初にアシスタントエッジノードのグループを割り当て、次にエッジノードのグループを割り当ててください。
- リンググループからアクティブリングを削除する場合、最初にエッジノードを削除し、次にアシスタントエッジノードを削除してください。

- すべてのリンググループを削除する場合、最初にエッジノードを削除し、次にアシスタントエッジノードを削除してください。
- リンググループのリングをアクティブ状態にする場合、最初にエッジノードをアクティブ状態にし、次にアシスタントエッジノードをアクティブ状態にしてください。
- リンググループのリングを非アクティブ状態にする場合、最初にアシスタントエッジノードを非アクティブ状態にし、次にエッジノードを非アクティブ状態にしてください。

ガイドラインに従わない場合、アシスタントエッジノードは Edge-Hello パケットの受信に失敗する可能性があり、誤ってプライマリリングが故障したと認識します。

例

RRPP リンググループ 1 を作成し、ドメイン 1、ドメイン 2 にサブリング 1、2、3、5 を追加します。

<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

関連コマンド

- **display rrpp ring-group**
- **rrpp ring-group**

4.1.7 protected-vlan

Syntax

protected-vlan reference-instance *instance-id-list*

undo protected-vlan [**reference-instance** *instance-id-list*]

デフォルト

設定なし

View

RRPP domain view

定義済みユーザロール

network-admin

パラメータ

reference-instance *instance-id-list*: MSTI（Multiple Spanning Tree Instances）の ID を指定します。MSTI の ID を 10 まで指定するか、範囲で指定します。MSTI を範囲で指定す

る形式は *instance-id-list* = { *instance-id* [**to** *instance-id*] }&<1-10>です。*instance-id* の設定範囲は 0～4094 です。VLAN インスタンスのマッピングを表示する場合、**display stp region-configuration** コマンドを使用します。パラメータを指定しない場合、RRPP ドメインによって参照されるすべての MSTI を削除します。

説明

protected-vlan コマンドは RRPP ドメインのプロテクト VLAN を設定します。

undo protected-vlan コマンドは RRPP ドメインからプロテクト VLAN を削除します。

装置のスパニングツリーの動作モードが PVST モード の場合、MSTI の ID の値は 0 だけです。

プロテクト VLAN のリングを設定する前後に、RRPP ドメインで設定したプロテクト VLAN を削除、あるいは修正することができます。しかしドメインで設定されたすべてのプロテクト VLAN の設定を削除することはできません。

VLAN インスタンスのマッピングを変更するとき、RRPP ドメインのプロテクト VLAN も変更します。

例

MSTI 1 に VLAN 1～VLAN 30 をマッピングし、MST リージョンの設定をアクティブ状態にします。RRPP ドメイン 1 のコントロール VLAN として VLAN 100 を設定します。RRPP ドメイン 1 のプライマリコントロール VLAN として MSTI 1 にマッピングされた VLAN を設定します。

```
<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
```

関連コマンド

- **display stp region-configuration** （コマンドマニュアルのセクション 3 *アクセス*“*STP*”）
- **rrpp domain**

4.1.8 reset rrpp statistics

Syntax

reset rrpp statistics domain *domain-id* [**ring** *ring-id*]

View

User view

定義済みユーザロール

network-admin

パラメータ

domain *domain-id*: RRPP ドメインの ID を指定します。設定範囲は 1～128 です。

ring *ring-id*: RRPP リングの ID を指定します。設定範囲は 1～128 です。指定しない場合、指定した RRPP ドメインのすべての RRPP リングの RRPPDU の統計情報を削除します。

説明

reset rrpp statistics コマンドは RRPPDU の統計情報を削除します。

例

RRPP ドメイン 1 のリング 10 の RRPPDU の統計情報を削除します。

<Switch> reset rrpp statistics domain 1 ring 10

関連コマンド

display rrpp statistics

4.1.9 ring

メモ:

RRPP リングのトランジットノードに加えてマスタノード、エッジノード、アシスタントエッジノードもサポートしています。

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*

デフォルト

装置は RRPP リングのノードではありません。

View

RRPP domain view

定義済みユーザロール

network-admin

パラメータ

ring-id: RRPP リングの ID を指定します。設定範囲は 1～128 です。

master: 装置を RRPP リングのマスタノードとして指定します。

transit: 装置を RRPP リングのトランジットノードとして指定します。

primary-port: プライマリポートを指定します。

interface-type interface-number: ポートのタイプと番号を指定します。

secondary-port: セカンダリポートを指定します。

level *level-value*: RRPP リングレベルを指定します。0 はプライマリリングで、1 はサブリングです。

assistant-edge: 装置を RRPP リングのアシスタントエッジノードとして指定します。

edge: 装置を RRPP リングのエッジノードとして指定します。

edge-port: ノードのエッジポートを指定します。

説明

ring コマンドは装置のノードモード、指定した RRPP ポートの役割、RRPP リングのレベルを設定します。

undo ring コマンドは RRPP リングを削除します。

ドメインの RRPP リングの ID は固有にする必要があります。

RRPP リングがアクティブ状態であるとき､RRPP ポートを設定することはできません。

エッジノード、アシスタントエッジノードを設定するとき、最初にプライマリリングを設定し、次にサブリングを設定してください。

設定した後、RRPP リングのノードモード、RRPP ポートの役割、リングレベルは変更することができません。設定を変更する場合、最初に現在の設定を削除してください。

エッジノードあるいはアシスタントエッジノードのプライマリリングの設定を削除する前に、すべてのサブリングの設定を削除してください。しかしアクティブ状態の RRPP リングは削除することができません。

装置で RRPP が有効であるとき、削除する前に、RRPP リングを無効にしてください。装置で RRPP が無効であるとき、**ring enable** コマンドの設定を使用して RRPP リングを直接削除することができます。

例

装置を RRPP ドメイン 1 のプライマリリング 10 のトランジットノードとして指定します。プライマリポートとして GigabitEthernet 1/0/1 を指定し、セカンダリポートとして GigabitEthernet 1/0/2 を指定します。装置を RRPP ドメイン 1 のサブリング 20 のエッジノードとして指定します｡エッジポートとして GigabitEthernet 1/0/3 を指定します。

<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

関連コマンド

ring enable

4.1.10 ring enable

Syntax

ring *ring-id* **enable**

undo ring *ring-id* **enable**

デフォルト

無効

View

RRPP domain view

定義済みユーザロール

network-admin

パラメータ

ring-id: RRPP リングの ID を指定します。設定範囲は 1～128 です。

説明

ring enable コマンドは RRPP リングを有効にします。

undo ring enable コマンドは RRPP リングを無効にします。

RRPP リングをアクティブにする場合、RRPP、RRPP リングを有効にする必要があります。

装置でサブリングを有効にする前に、プライマリリングを有効にする必要があります。装置でプライマリリングを無効にする前に、すべてのサブリングを無効にする必要があります。そうでない場合、システムはエラーメッセージを表示します。

例

RRPP ドメイン 1 の RRPP リング 10 を有効にします。

<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

関連コマンド

rrpp enable

4.1.11 rrpp domain

Syntax

rrpp domain *domain-id*

undo rrpp domain *domain-id*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

domain-id: RRPP ドメインの ID を指定します。設定範囲は 1～128 です。

説明

rrpp domain コマンドは RRPP ドメインを作成し、RRPP domain view に移行します。

undo rrpp domain コマンドは RRPP ドメインを削除します。

RRPP ドメインを削除するとき、コントロール VLAN とプロテクト VLAN の設定が同時に削除されます。

RRPP ドメインを正常に削除するため、RRPP リングがないことを確認してください。

例

RRPP ドメイン 1 を作成し、RRPP domain 1 view に移行します。

<Switch> system-view

[Switch] rrpp domain 1

[Switch-rrpp-domain1]

関連コマンド

- **control-vlan**
- **protected-vlan**

4.1.12 rrpp enable

Syntax

rrpp enable

undo rrpp enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

rrpp enable コマンドは RRPP を有効にします。

undo rrpp enable コマンドは RRPP を無効にします。

RRPP ドメインをアクティブ状態にするため、RRPP と RRPP ドメインの RRPP リングを有効にします。

例

RRPP を有効にします。

<Switch> system-view

[Switch] rrpp enable

関連コマンド

ring enable

4.1.13 rrpp ring-group

Syntax

rrpp ring-group *ring-group-id*

undo rrpp ring-group *ring-group-id*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

ring-group-id: RRPP リンググループの ID を指定します。設定範囲は 1～64 です。

説明

rrpp ring-group コマンドは RRPP リンググループを作成し、RRPP ring group view に移行します。RRPP リンググループがすでに存在する場合、その view に移行します。

undo rrpp ring-group コマンドは RRPP リンググループを削除します。

リンググループを削除するとき、最初にエッジノードのリンググループを削除し、次にアシスタントエッジノードのリンググループを削除してください。そうでない場合、アシスタントエッジノードが Edge-Hello パケットの受信に失敗する可能性があり、誤ってプライマリリングが故障したと認識します。

リンググループが削除されたのち、リンググループのすべてのサブリングはいずれのリンググループに属していないことになります。

例

RRPP リンググループ 1 を作成し、RRPP ring group view に移行します。

<Switch> system-view

[Switch] rrpp ring-group 1

[Switch-ring-group1]

関連コマンド

- **display rrpp ring-group**
- **domain ring**

4.1.14 snmp-agent trap enable 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**] *

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

パラメータ

major-fault: アシスタントエッジノートとエッジノート間のSRPT間が切断されたとき、SNMP notification を送信します。

multi-master: RRPP リングに複数のマスタノードが設定されているとき、SNMP notification を送信します。

ring-fail: RRPP リングの状態が Health から Disconnect に遷移したとき、SNMP notification を送信します。

ring-recover: RRPP リングの状態が Disconnect から Health に遷移したとき、SNMP notification を送信します。

説明

snmp-agent trap enable rrpp コマンドは RRPP の SNMP notification（inform あるいはトラップ）の送信を有効にします。

undo snmp-agent trap enable rrpp コマンドは RRPP の SNMP notification（inform あるいはトラップ）の送信を無効にします。

NMS に重大な RRPP イベントを通知するため、RRPP の SNMP notification を有効にします。SNMP notification を送信するため、必要なパラメータを設定してください。SNMP notification の設定の詳細は、オペレーションマニュアルのセクション 11 *システム管理* “*SNMP*”を参照してください。

snmp-agent trap enable rrpp コマンドでパラメータを指定しない場合、装置でサポートする RRPP に関するすべての SNMP notification を有効にします。**undo snmp-agent trap enable rrpp** コマンドでパラメータを指定しない場合、装置でサポートする RRPP に関するすべての SNMP notification を無効にします。

例

RRPP リングの状態が Disconnect から Health に遷移したとき、SNMP notification を送信します。

<Switch> system-view

[Switch] snmp-agent trap enable rrpp ring-recover

4.1.15 timer

Syntax

timer hello-timer *hello-value* **fail-timer** *fail-value*

undo timer

デフォルト

Hello タイマは 1 秒、Fail タイマは 3 秒です。

View

RRPP domain view

定義済みユーザロール

network-admin

パラメータ

hello-timer *hello-value*: Hello タイマを指定します。設定範囲は 1～10 秒です。

fail-timer *fail-value*: Fail タイマを指定します。設定範囲は 3～30 秒です。

説明

timer コマンドは Hello タイマと Fail タイマを設定します。

undo timer コマンドはデフォルトに戻します。

Fail タイマは Hello タイマの 3 倍以上にする必要があります。

例

RRPP ドメイン 1 の Hello タイマを 2 秒、Fail タイマを 7 秒に設定します。

<Switch> system-view

[Switch] rrpp domain 1

[Switch-rrpp-domain1] timer hello-timer 2 fail-timer 7

目次

このセクションのページは **10-x-x** です。

5 章 Smart Link 5-1
5.1 Smart Link 設定コマンド 5-1
5.1.1 display smart-link flush 5-1
5.1.2 display smart-link group 5-2
5.1.3 flush enable 5-3
5.1.4 port 5-4
5.1.5 port smart-link group 5-6
5.1.6 port smart-link group track 5-7
5.1.7 preemption delay 5-9
5.1.8 preemption mode 5-10
5.1.9 protected-vlan 5-10
5.1.10 reset smart-link statistics 5-12
5.1.11 smart-link flush enable 5-12
5.1.12 smart-link group 5-13

5章 Smart Link

5.1 Smart Link設定コマンド

5.1.1 display smart-link flush

Syntax

display smart-link flush

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display smart-link flush コマンドは受信した flush メッセージの情報を表示します。

例

受信した flush メッセージの情報を表示します。

<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
```

表 5-1 コマンド出力

フィールド	説明
Received flush packets	受信したflushメッセージの情報の総数です。
Receiving interface of the last flush packet	最後にflushメッセージを受信したポートです。
Receiving time of the last flush packet	最後にflushメッセージを受信した時間です。
Device ID of the last flush packet	最後にflushメッセージを受信した装置のIDです。
Control VLAN of the last flush packet	最後にflushメッセージを受信した制御VLANのIDです。

関連コマンド

reset smart-link statistics

5.1.2 display smart-link group

Syntax

display smart-link group { *group-id* | **all** }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

group-id: Smart Link グループの ID を指定します。設定範囲は 1～48 です。

all: すべての Smart Link グループの情報を表示します。

説明

display smart-link group コマンドは指定した Smart Link グループあるいはすべての Smart Link グループの情報を表示します。

例

Smart Link グループ 1 の情報を表示します。

<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
```

表 5-2 コマンド出力

フィールド	説明
Preemption mode	Preemptionモードです。 ● **None**—Preemptionが無効です。 ● **Role**—PreemptionモードがRoleです。 ● **Speed**—PreemptionモードがSpeedです。このモードはサポートしていません。
Preemption delay	Preemption delay時間です。単位は秒です。
Control-VLAN	制御VLAN IDです。
Protected VLAN	Smart Linkグループのプロテクト VLANです。参照するMSTI（Multiple Spanning Tree Instances）が表示されます。参照するMSTIにマッピングされるVLANを表示する場合、**display stp region-configuration**コマンドを使用します。
Member	Smart Linkグループのメンバポートです。
Role	ポートの役割です。primary、secondaryがあります。
State	ポート状態です。active、down、standbyがあります。
Flush-count	転送されたflushメッセージの数です。
Last-flush-time	最後にflushメッセージが転送した時間です。（flushメッセージが転送されていない場合、**NA**と表示されます。）

5.1.3 flush enable

Syntax

flush enable [**control-vlan** *vlan-id*]

undo flush enable

デフォルト

Smart Link グループの flush アップデートは有効です。flush メッセージの送信は VLAN 1 を使用します。

View

Smart link group view

定義済みユーザロール

network-admin

パラメータ

control-vlan *vlan-id*: flush メッセージを送信する制御 VLAN を指定します。設定範囲は 1 ～4094 です。

説明

flush enable コマンドは flush アップデートを有効にします。

undo flush enable コマンドは flush アップデートを無効にします。

Smart link グループで設定された制御 VLAN は、他の Smart Link グループに設定された制御 VLAN と異なるようにしてください。

- 設定された制御 VLAN が作成されていることを確認してください。制御 VLAN に Smart Link メンバポートを割り当ててください。
- Smart Link グループの制御 VLAN はプロテクト VLAN にしてください。制御 VLAN を削除しないでください。制御 VLAN を削除すると flush メッセージを正常に送信することができません。

例

Smart Link グループ 1 の flush アップデートを無効にします。

<Switch> system-view

[Switch] smart-link group 1

[Switch-smlk-group1] undo flush enable

関連コマンド

smart-link flush enable

5.1.4 port

Syntax

port *interface-type interface-number* { **primary** | **secondary** }

undo port *interface-type interface-number*

デフォルト

設定なし

View

Smart link group view

定義済みユーザロール

network-admin

パラメータ

interface-type interface-number: ポートのタイプと番号を指定します。ポートはレイヤ 2 Ethernet インタフェースあるいはアグリゲートインタフェースが設定できます。

primary: ポートを primary ポートとして指定します。

secondary: ポートを secondary ポートとして指定します。

説明

port コマンドは指定されたポートを現在の Smart Link グループの primary あるいは secondary ポートとして割り当てます。

undo port コマンドは Smart Link グループから指定されたポートを削除します。

Smart Link グループのメンバポートを設定する前に、Smart Link グループのプロテクト VLAN を設定してください。

Smart Link グループに追加するポートではスパニングツリー機能を無効にしてください。Smart Link グループメンバポートでスパニングツリー機能を有効にすることができません。

ポートにアグリゲーショングループメンバと Smart Link グループメンバの両方を設定した場合、アグリゲーショングループの設定が適用されます。ポートは **display smart-link group** コマンドで表示されません。Smart Link グループの設定はアグリゲーショングループからポートを削除した後、適用されます。

interface view で **port smart-link group** コマンドを使用して Smart Link グループにポートを割り当てることができます。

例

GigabitEthernet 1/0/1 を Smart Link グループ 1 の secondary ポートとして設定します。

<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

関連コマンド

port smart-link group

5.1.5 port smart-link group

Syntax

port smart-link group *group-id* { **primary** | **secondary** }

undo port smart-link group *group-id*

デフォルト

設定なし

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

group-id: Smart Link グループの ID を指定します。設定範囲は 1～48 です。

primary: ポートを primary ポートとして指定します。

secondary: ポートを secondary ポートとして指定します。

説明

port smart-link group コマンドは現在のポートを指定された Smart Link グループのメンバポートとして設定します。

undo port smart-link group コマンドは指定された Smart Link グループからポートを削除します。

Smart Link グループのメンバポートを設定する前に、Smart Link グループのプロテクト VLAN を設定してください。

Smart Link グループに追加するポートではスパニングツリー機能を無効にしてください。Smart Link グループメンバポートでスパニングツリー機能を有効にすることができません。

ポートにアグリゲーショングループメンバと Smart Link グループメンバの両方を設定した場合、アグリゲーショングループの設定が適用されます。ポートは **display smart-link group** コマンドで表示されません。Smart Link グループの設定はアグリゲーショングループからポートを削除した後、適用されます。

smart link group view で **port** コマンドを使用して Smart Link グループにポートを割り当てることができます。

例

GigabitEthernet 1/0/1 を Smart Link グループ 1 の primary ポートとして設定します。

<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

アグリゲートインタフェース 1 を Smart Link グループ 1 の primary ポートとして設定します。

<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

関連コマンド

port

5.1.6 port smart-link group track

Syntax

port smart-link group *group-id* **track** *track-entry-number*

undo port smart-link group *group-id* **track** *track-entry-number*

デフォルト

設定なし

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

group-id: Smart Link グループの ID を指定します。設定範囲は 1～48 です。

track-entry-number: CFD の CC 機能に関連づけられる track エントリの ID を指定します。

説明

port smart-link group track コマンドは Smart Link グループメンバポートと track エントリ間のコラボレーションを設定します。

undo port smart-link group track コマンドはコラボレーションを削除します。

Smart Link は、トラックエントリを介してリンク検出プロトコルと連携します。リンク検出を実装するために CFD の CC 機能のみをサポートします。CFD の CC 機能をトラックエントリに関連付けるには、**track cfd** コマンドを使用します。

ポートで Smart Link と track 間のコラボレーションを設定する前に、指定した Smart Link グループにポートが追加されていることを確認してください。

例

リンクの状態を検出するため、GigabitEthernet 1/0/1 の Smart Link グループ 1 の primary ポートと、track エントリ 1 を通した CFD の CC 機能のコラボレーションを設定します。

<Switch> system-view

[Switch] track 1 cfd cc service-instance 100 mep 2

[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

リンクの状態を検出するため、ブリッジアグリゲーション 1 の Smart Link グループ 1 の primary ポートと、track エントリ 1 を通した CFD の CC 機能のコラボレーションを設定します。

<Switch> system-view

[Switch] track 1 cfd cc service-instance 100 mep 2

[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

関連コマンド

track cfd

5.1.7 preemption delay

Syntax

preemption delay *delay*

undo preemption delay

デフォルト

1 秒

View

Smart link group view

定義済みユーザロール

network-admin

パラメータ

delay: preemption delay を指定します。設定範囲は 0～300 秒です。

説明

preemption delay コマンドは preemption delay を設定します。

undo preemption delay コマンドはデフォルトに戻します。

preemption のモードを role に設定し、preemption delay を設定した後、上流の装置の切り替えが発生すると、コラボレーションを引き継ぐ前に、primary ポートは指定した preemption delay の間、引き継ぎを待ちます。

preemption delay は preemption モードが設定されたのち適用されます。

例

preemption を有効にし、モードを role に設定します。preemption delay を 10 秒に設定します。

<Switch> system-view

[Switch] smart-link group 1

[Switch-smlk-group1] preemption mode role

[Switch-smlk-group1] preemption delay 10

関連コマンド

preemption mode

5.1.8 preemption mode

Syntax

preemption mode role

undo preemption mode

デフォルト

無効

View

Smart link group view

定義済みユーザロール

network-admin

パラメータ

role: preemption モードを role に指定します。このモードは primary ポートからアクティブ状態の secondary ポートに早急に切り替わる（プリエンプトする）ことを有効にします。

説明

preemption mode コマンドは preemption を有効にし、モードを role に設定します。

undo preemption mode コマンドは preemption を無効にします。

例

preemption を有効にし、モードを role に設定します。

<Switch> system-view

[Switch] smart-link group 1

[Switch-smlk-group1] preemption mode role

5.1.9 protected-vlan

Syntax

protected-vlan reference-instance *instance-id-list*

undo protected-vlan [**reference-instance** *instance-id-list*]

デフォルト

設定なし

View

Smart link group view

定義済みユーザロール

network-admin

パラメータ

reference-instance *instance-id-list*: 参照される MSTI を指定します。形式は *instance-id-list* = { *instance-id* [**to** *instance-id*] }&<1-10>です。*instance-id* は MSTI ID です。設定範囲は 0～4094 です。MSTI ID が 0 の場合、CIST（common internal spanning tree）です。&<*1-10*>は 10 個の MSTI ID あるいは MSTI ID の範囲を指定することができることを示します。インスタンスと VLAN マッピングを表示する場合、**display stp region-configuration** コマンドを使用します。

説明

protected-vlan コマンドは Smart Link グループのプロテクト VLAN を設定します。

undo protected-vlan コマンドは Smart Link グループのプロテクト VLAN を削除します。

Smart Link グループのメンバポートが所属するすべてのプロテクト VLAN を設定する必要があります。

VLAN-MSTI マッピングが変更された場合、プロテクト VLAN が変更されます。

プロテクト VLAN の設定を削除する場合、以下の制限とガイドラインに従ってください。

- **undo protected-vlan** コマンドで **reference-instance** *instance-id-list* パラメータが指定されている場合、指定された MSTI にマッピングされた VLAN の設定を削除します。指定されていない場合、すべてのプロテクト VLAN を削除します。
- Smart Link グループにメンバポートがある場合、プロテクト VLAN の設定を削除することはできません。Smart link グループにメンバポートが割り当てられていない場合、Smart link グループからプロテクト VLAN を削除することができます。

例

MSTI 1 に VLAN 1～VLAN 30 をマッピングし、MST リージョン設定を有効にします。Smart link グループ 1 のプロテクト VLAN として MSTI 1 をマッピングします。

```
<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
```

関連コマンド

- **display stp region-configuration** （コマンドマニュアルのセクション 3 *アクセス “STP”*）
- **smart-link group**

5.1.10 reset smart-link statistics

Syntax

reset smart-link statistics

View

User view

定義済みユーザロール

network-admin

説明

reset smart-link statistics コマンドは flush メッセージの統計情報を削除します。

例

flush メッセージの統計情報を削除します。

<Switch> reset smart-link statistics

関連コマンド

display smart-link flush

5.1.11 smart-link flush enable

Syntax

smart-link flush enable [**control-vlan** *vlan-id-list*]

undo smart-link flush enable [**control-vlan** *vlan-id-list*]

デフォルト

無効

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

control-vlan *vlan-id-list*: flush メッセージを受信するために使用する制御 VLAN を指定します。デフォルトは 1 です。*vlan-id-list* の形式は *vlan-id-list* = { *vlan-id* [**to** *vlan-id*] }&<1-10>です。*vlan-id* は制御 VLAN の ID です。設定範囲は 1～4094 です。&<1-10>は VLAN ID あるいは VLAN ID リストを 10 個まで設定できることを示します。

説明

smart-link flush enable コマンドは flush メッセージの受信機能を有効にします。

undo smart-link flush enable コマンドは flush メッセージの受信機能を無効にします。

例

flush メッセージを制御 VLAN で受信することを GigabitEthernet 1/0/1 で有効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] smart-link flush enable

flush メッセージを制御 VLAN 1 で受信することをアグリゲートインタフェース 1 で有効にします。

<Switch> system-view

[Switch] interface bridge-aggregation 1

[Switch-Bridge-Aggregation1] smart-link flush enable

関連コマンド

flush enable

5.1.12 smart-link group

Syntax

smart-link group *group-id*

undo smart-link group *group-id*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

group-id: Smart Link グループの ID を指定します。設定範囲は 1～48 です。

説明

smart-link group コマンドは Smart Link グループを作成し、smart link group view に移行します。

undo smart-link group コマンドは Smart Link グループを削除します。

メンバポートの Smart Link グループを削除することはできません。

例

Smart Link グループ 1 を作成し、smart link group view に移行します。

<Switch> system-view

[Switch] smart-link group 1

[Switch-smlk-group1]

目次

このセクションのページは **10-x-x** です。

6 章 Monitor Link 6-1
6.1 Monitor Link 設定コマンド 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 6-4

6章 Monitor Link

6.1 Monitor Link設定コマンド

6.1.1 display monitor-link group

Syntax

display monitor-link group { *group-id* | **all** }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

group-id: Monitor Link グループの ID を指定します。設定範囲は 1～16 です。

all: すべての Monitor Link グループを指定します。

説明

display monitor-link group コマンドは Monitor Link グループの情報を表示します。

このコマンドはリンクアグリゲーショングループに所属しているポートの情報を表示しません。

例

すべての Monitor Link グループの情報を表示します。

<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
```

表 6-1 コマンド出力

フィールド	説明
Monitor link protocol status	Monitor Linkが有効かどうかを示します。 ● **Enabled**－有効です。 ● **Disabled**－無効です。
Group status	Monitor Linkグループの状態です。 ● **DOWN**－downしています。 ● **UP**－upしています。 ● **N/A**－Monitor Linkグループがグローバルで無効です。Monitor Linkグループが動作していません。
Downlink up-delay	Monitor Linkグループのダウンリンクインタフェースを切り替えるdelayです。単位は秒です。
Last-up-time	Monitor Linkグループが最後にupした時間です。
Last-down-time	Monitor Linkグループが最後にdownした時間です。
Up-port-threshold	Monitor Linkグループの状態を切り替えるアップリンクインタフェースのしきい値です。
Member	Monitor Linkグループのメンバインタフェースです。
Role	インタフェースの役割です。アップリンクインタフェース、ダウンリンクインタフェースがあります。
Status	メンバリンクの状態です。up、downがあります。

6.1.2 monitor-link group

Syntax

monitor-link group *group-id*

undo monitor-link group *group-id*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

group-id: Monitor Link グループの ID を指定します。設定範囲は 1～16 です。

説明

monitor-link group コマンドは Monitor Link グループを作成し、monitor link group view に移行します。Monitor Link グループが既に存在する場合、その view に移行します。

undo monitor-link group コマンドは Monitor Link を削除します。

例

Monitor Link グループ 1 を作成し、monitor link group view に移行します。

<Switch> system-view

[Switch] monitor-link group 1

[Switch-mtlk-group1]

6.1.3 port

Syntax

port *interface-type interface-number* { **downlink** | **uplink** }

undo port *interface-type interface-number*

デフォルト

設定なし

View

Monitor link group view

定義済みユーザロール

network-admin

パラメータ

interface-type: インタフェースのタイプを指定します。

interface-number: インタフェースの番号を指定します。

downlink: ダウンリンクインタフェースを指定します。

uplink: アップリンクインタフェースを指定します。

説明

port コマンドは Monitor Link グループにインタフェースを割り当てます。

undo port コマンドは Monitor Link グループからインタフェースを削除します。

インタフェースは 1 つの Monitor link グループのみ割り当てることができます。

interface view で **port monitor-link group** コマンドを使用して Monitor link グループにインタフェースを割り当てることができます。

Monitor Link の動作の中断を防ぐため、アグリゲートインタフェースとアグリゲーショングループのメンバポートを同じ Monitor Link グループに割り当てないでください。

例

Monitor Link グループ 1 のアップリンクインタフェースとして GigabitEthernet 1/0/1 を設定し、ダウンリンクインタフェースとして GigabitEthernet 1/0/2 を設定します。

<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

関連コマンド

port monitor-link group

6.1.4 port monitor-link group

Syntax

port monitor-link group *group-id* { **downlink** | **uplink** }

undo port monitor-link group *group-id*

デフォルト

設定なし

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

group-id: Monitor Link グループの ID を指定します。設定範囲は 1～16 です。

downlink: ダウンリンクインタフェースを指定します。

uplink: アップリンクインタフェースを指定します。

説明

port monitor-link group コマンドはメンバインタフェースとして Monitor Link グループに現在のインタフェースを割り当てます。

undo port monitor-link group コマンドは Monitor Link グループから現在のインタフェースを削除します。

インタフェースは 1 つの Monitor link グループのみ割り当てることができます。

monitor link group view で **port** コマンドを使用して Monitor link グループにインタフェースを割り当てることができます。

Monitor Link の動作の中断を防ぐため、アグリゲートインタフェースとアグリゲーショングループのメンバポートを同じ Monitor Link グループに割り当てないでください。

例

Monitor Link グループ 1 のアップリンクインタフェースとして GigabitEthernet 1/0/1 を設定し、ダウンリンクインタフェースとして GigabitEthernet 1/0/2 を設定します。

<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

関連コマンド

port

目次

このセクションのページは **10-x-x** です。

7 章 VRRP 7-1
7.1 IPv4 VRRP 設定コマンド 7-1
7.1.1 display vrrp 7-1
7.1.2 display vrrp statistics 7-5
7.1.3 reset vrrp statistics 7-7
7.1.4 snmp-agent trap enable vrrp 7-8
7.1.5 vrrp check-ttl enable 7-9
7.1.6 vrrp dscp 7-10
7.1.7 vrrp version 7-10
7.1.8 vrrp vrid 7-11
7.1.9 vrrp vrid authentication-mode 7-13
7.1.10 vrrp vrid preempt-mode 7-14
7.1.11 vrrp vrid priority 7-16
7.1.12 vrrp vrid timer advertise 7-17
7.1.13 vrrp vrid track 7-18
7.2 IPv6 VRRP 設定コマンド 7-20
7.2.1 display vrrp ipv6 7-20
7.2.2 display vrrp ipv6 statistics 7-24
7.2.3 reset vrrp ipv6 statistics 7-26
7.2.4 vrrp ipv6 dscp 7-27
7.2.5 vrrp ipv6 vrid 7-28
7.2.6 vrrp ipv6 vrid preempt-mode 7-29
7.2.7 vrrp ipv6 vrid priority 7-31
7.2.8 vrrp ipv6 vrid timer advertise 7-32
7.2.9 vrrp ipv6 vrid track 7-33

7章 VRRP

7.1 IPv4 VRRP設定コマンド

VRRP は、LAG グループのメンバポートでは未サポートです。

7.1.1 display vrrp

Syntax

display vrrp [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]] [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: インタフェースのタイプと番号を指定します。

vrid *virtual-router-id*: IPv4 VRRP グループの仮想ルータ ID を指定します。*virtual-router-id* 引数の値の範囲は 1～255 です。

verbose: IPv4 VRRP グループの詳細情報を表示します。指定しない場合、IPv4 VRRP グループの概要情報を表示します。

説明

display vrrp コマンドは IPv4 VRRP グループの状態を表示します。

インタフェースあるいは VRRP グループが指定されない場合、すべての IPv4 VRRP グループの状態を表示します。

インタフェースのみが指定されている場合、指定したインタフェースのすべての IPv4 VRRP グループの状態を表示します。

インタフェースと IPv4 VRRP グループの両方が指定されている場合、指定されたインタフェースの指定された IPv4 VRRP グループの状態を表示します。

例

VRRP が standard モードで動作するとき、装置のすべての IPv4 VRRP グループの概要情報を表示します。

<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
```

表 7-1 コマンド出力（standard モード）

操作	説明
Running Mode	VRRP動作モードです。（standardモード）
Total number of virtual routers	VRRPグループの総数です。
Interface	VRRPグループが設定されたインタフェースです。
VRID	仮想ルータIDです。（VRRPグループ番号）
State	VRRPグループのルータの状態です。 ● **Master**－マスタ状態です。 ● **Backup**－バックアップ状態です。 ● **Initialize**－初期化状態です。 ● **Inactive**－非アクティブ状態です。
Running Pri	ルータの現在の優先度です。 Trackエントリがルータの VRRPグループに関連づけられている場合、Trackエントリの状態が変更したとき、ルータの優先度が変更します。
Adver Timer	VRRPアドバタイズメントの送信間隔です。単位はセンチ秒です。
Auth Type	認証タイプです。 ● **None**—認証を行いません。 ● **Simple**—Simple認証です。 ● **MD5**—MD5認証です。
Virtual IP	VRRPグループの仮想IPアドレスです。

VRRP が standard モードで動作するとき、装置のすべての IPv4 VRRP グループの詳細情報を表示します。

<Switch> display vrrp verbose

```
IPv4 Virtual Router Information:
 Running Mode     : Standard
 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
VRRP Track Information:
  Track Object  : 1                   State : Positive   Pri Reduced : 50
Interface Vlan-interface2
  VRID          : 11                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   : 0000-5e00-010b
  Master IP     : 1.1.1.12
```

表 7-2 コマンド出力（standard モード）

操作	説明
Running Mode	VRRP動作モードです。（standardモード）
Total number of virtual routers	VRRPグループの総数です。
Interface	VRRPグループが設定されたインタフェースです。
VRID	仮想ルータIDです。（VRRPグループ番号）
Adver Timer	VRRPアドバタイズメントの送信間隔です。単位はセンチ秒です。
Admin Status	管理状態です。**up**あるいは**down**があります。
State	VRRPグループのルータの状態です。 ● **Master**－マスタ状態です。 ● **Backup**－バックアップ状態です。 ● **Initialize**－初期化状態です。 ● **Inactive**－非アクティブ状態です。
Config Pri	ルータの優先度です。**vrrp vrid priority**コマンドで設定します。

操作	説明
Running Pri	ルータの現在の優先度です。 TrackエントリがルータのVRRPグループに関連づけられている場合、Trackエントリの状態が変更するときルータの優先度が変更します。
Preempt Mode	Preemptive モードです。 ● **Yes**ー有効です。 ● **No**ー無効です。
Delay Time	Preemption delayタイマです。単位はセンチ秒です。
Become Master	バックアップルータがマスタに切り替わるまでの待ち時間です。単位はミリ秒です。
Auth Type	認証タイプです。 ● **None**—認証を行いません。 ● **Simple**—Simple認証です。 ● **MD5**—MD5認証です。
Key	認証キーです。認証が必要ない場合、表示されません。
Virtual IP	VRRPグループの仮想IPアドレスです。
Virtual MAC	VRRPグループの仮想IPアドレスの仮想MACアドレスです。ルータがマスタであるとき表示されます。
Master IP	マスタが存在するインタフェースのプライマリIPアドレスです。
VRRP Track Information	Trackエントリの情報です。**vrrp vrid track**コマンドが設定された後、表示されます。
Track Object	VRRPグループに関連づけられたTrackエントリです。
State	Trackエントリの状態です。 ● Negative ● Positive ● NotReady
Pri Reduced	関連したTrackエントリの状態がNegativeになるときに、減少する優先度の値です。
Switchover	切り替わりモードです。関連したTrackエントリがNegativeになるとき、バックアップルータがすぐさまマスタになります。

7.1.2 display vrrp statistics

Syntax

display vrrp statistics [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: インタフェースのタイプと番号を指定します。

vrid *virtual-router-id*: IPv4 VRRP グループの仮想ルータ ID を指定します。*virtual-router-id* 引数の値の範囲は 1～255 です。

説明

display vrrp statistics コマンドは IPv4 VRRP グループの統計情報を表示します。

インタフェースあるいは VRRP グループが指定されない場合、すべての IPv4 VRRP グループの統計情報を表示します。

インタフェースのみが指定されている場合、指定したインタフェースのすべての IPv4 VRRP グループの統計情報を表示します。

インタフェースと IPv4 VRRP グループの両方が指定されている場合、指定されたインタフェースの指定された IPv4 VRRP グループの統計情報を表示します。

IPv4 VRRP グループの統計情報を削除する場合、**reset vrrp statistics** コマンドを使用します。

例

VRRP が standard モードで動作するとき、装置のすべての IPv4 VRRP グループの統計情報を表示します。

<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
```

表 7-3 関連コマンド (standard モード)

操作	説明
Interface	VRRPグループが設定されたインタフェースです。
VRID	VRRPグループの数です。
CheckSum Errors	チェックサムエラーのパケット数です。
Version Errors	バージョンエラーのパケット数です。
Invalid Pkts Rcvd	不正なパケットタイプのパケットを受信した数です。
Unexpected Pkts Rcvd	予期しないパケットを受信した数です。
Advertisement Interval Errors	アドバタイズメント間隔のエラーによるパケット数です。
IP TTL Errors	TTLエラーのパケット数です。
Auth Failures	認証に失敗したパケット数です。
Invalid Auth Type	不正な認証タイプのため認証に失敗したパケット数です。
Auth Type Mismatch	認証タイプが不一致のため認証に失敗したパケット数です。
Packet Length Errors	VRRPパケット長エラーのパケット数です。
Address List Errors	仮想IPアドレス制限エラーのパケット数です。
Become Master	ルータがマスタとして選定された回数です。
Priority Zero Pkts Rcvd	ルータの優先度が0のアドバタイズメントを受信した数です。
Adver Rcvd	アドバタイズメントを受信した数です。
Priority Zero Pkts Sent	ルータの優先度が0のアドバタイズメントを送信した数です。

操作	説明
Adver Sent	アドバタイズメントを送信した数です。
Global statistics	すべてのVRRPグループのグローバルの統計情報です。
CheckSum Errors	チェックサムエラーのパケットの総数です。
Version Errors	バージョンエラーのパケットの総数です。
VRID Errors	VRIDエラーのパケットの総数です。

関連コマンド

reset vrrp statistics

7.1.3 reset vrrp statistics

Syntax

reset vrrp statistics [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]]

View

User view

定義済みユーザロール

network-admin

パラメータ

interface *interface-type interface-number*: インタフェースのタイプと番号を指定します。

vrid *virtual-router-id*: IPv4 VRRP グループの仮想ルータ ID を指定します。*virtual-router-id* 引数の値の範囲は 1～255 です。

説明

reset vrrp statistics コマンドは IPv4 VRRP グループの統計情報を削除します。

インタフェースあるいは VRRP グループが指定されない場合、すべての IPv4 VRRP グループの統計情報を削除します。

インタフェースのみが指定されている場合、指定したインタフェースのすべての IPv4 VRRP グループの統計情報を削除します。

インタフェースと IPv4 VRRP グループの両方が指定されている場合、指定されたインタフェースの指定された IPv4 VRRP グループの統計情報を削除します。

例

すべてのインタフェースのすべての IPv4 VRRP グループの統計情報を削除します。

<Switch> reset vrrp statistics

関連コマンド

display vrrp statistics

7.1.4 snmp-agent trap enable vrrp

Syntax

snmp-agent trap enable vrrp [**auth-failure** | **new-master**]

undo snmp-agent trap enable vrrp [**auth-failure** | **new-master**]

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

パラメータ

auth-failure: VRRP グループの装置がローカルの設定に一致しない認証タイプ、あるいはキーの VRRP アドバタイズメントを受信するとき、RFC2787 で定義されている notification を作成します。

new-master: VRRP グループの装置が初期化あるいはバックアップからマスタに変更するとき、RFC2787 で定義されている notification を作成します。

説明

snmp-agent trap enable vrrp コマンドは VRRP の SNMP notification を有効にします。

undo snmp-agent trap enable vrrp コマンドは VRRP の SNMP notification を無効にします。

SNMP notification 機能が有効なとき、装置は宛先ホストに notification を送信することができます。notification のタイプ（inform あるいはトラップ）と宛先ホストを指定する場合、**snmp-agent target-host** コマンドを使用します。

例

VRRP グループの装置がローカルの設定に一致しない認証タイプ、あるいはキーの VRRP アドバタイズメントを受信するとき、RFC2787 で定義されている notification を作成します。

<Switch> system-view

[Switch] snmp-agent trap enable vrrp auth-failure

7.1.5 vrrp check-ttl enable

Syntax

vrrp check-ttl enable

undo vrrp check-ttl enable

デフォルト

有効

View

Interface view

定義済みユーザロール

network-admin

説明

vrrp check-ttl enable コマンドは IPv4 VRRP パケットの TTL チェックを有効にします。

undo vrrp check-ttl enable コマンドは IPv4 VRRP パケットの TTL チェックを無効にします。

IPv4 VRRP グループのマスタは、マスタが存在していることを宣言するため定期的に VRRP アドバタイズメントを送信します。VRRP アドバタイズメントはローカルサブネットにマルチキャストします。ルータによって転送することができません。そのため、TTL の値が変更されません。マスタが VRRP アドバタイズメントを送信するとき、TTL の値を 255 に設定します。TTL チェックを有効にした場合、バックアップルータは他のサブネットからの攻撃を防ぐため、TTL の値が 255 以外の VRRP アドバタイズメントを廃棄します。

他社製品では、VRRP の仕様が QX シリーズと異なる可能性があります。QX シリーズが他社製品と相互に通信しているとき、VRRP パケットの TTL チェックを有効にすると、予期しないパケットの廃棄が行われる可能性があります。この場合、VRRP パケットの TTL チェックを無効にするため、**undo vrrp check-ttl enable** コマンドを使用します。

例

IPv4 VRRP パケットの TTL チェックを無効にします。

<Switch> system-view

[Switch] interface vlan-interface 2

[Switch-Vlan-interface2] undo vrrp check-ttl enable

7.1.6 vrrp dscp

Syntax

vrrp dscp *dscp-value*

undo vrrp dscp

デフォルト

48

View

System view

定義済みユーザロール

network-admin

パラメータ

dscp-value: VRRP の DSCP を指定します。設定範囲は 0～63 です。

説明

vrrp dscp コマンドは VRRP パケットの DSCP を設定します。

undo vrrp dscp コマンドはデフォルトに戻します。

VRRP パケットの DSCP の値はパケットのプライオリティを指定します。パケットを送信するプライオリティに影響します。DSCP の値が大きくなると、プライオリティが高くなります。

例

VRRP パケットの DSCP を 30 に設定します。

<Switch> system-view

[Switch] vrrp dscp 30

7.1.7 vrrp version

Syntax

vrrp version *version-number*

undo vrrp version

デフォルト

VRRPv3 is used.

View

Interface view

定義済みユーザロール

network-admin

パラメータ

version-number: VRRP バージョンを指定します。設定範囲は 2～3 です。2 は VRRPv2（RFC3768 で定義）で、3 は VRRPv3（RFC5798 で定義）を示します。

説明

vrrp version コマンドはインタフェースの IPv4 VRRP のバージョンを指定します。

undo vrrp version コマンドはデフォルトに戻します。

IPv4 VRRP グループのすべてのルータで VRRP のバージョンを同一にする必要があります。

例

VLAN インタフェース 10 で VRRPv2 を指定します。

<Switch> system-view

[Switch] interface vlan-interface 10

[Switch-Vlan-interface10] vrrp version 2

7.1.8 vrrp vrid

Syntax

vrrp vrid *virtual-router-id* **virtual-ip** *virtual-address*

undo vrrp vrid *virtual-router-id* [**virtual-ip** [*virtual-address*]]

デフォルト

設定なし

View

Interface view

定義済みユーザロール

network-admin

パラメータ

virtual-router-id: IPv4 VRRP グループの仮想ルータ ID を指定します。設定範囲は 1～255 です。

virtual-ip *virtual-address*: 仮想 IP アドレスを指定します。すべて 0（0.0.0.0）、ブロードキャストアドレス(255.255.255.255)、ループバックアドレス、クラス A、B、C 以外の IP アドレス、無効な IP アドレス（たとえば 0.0.0.1）にすることはできません。パラメータを指定しない場合、**undo vrrp vrid** コマンドは既存の IPv4 VRRP グループからすべての仮想 IP アドレスを削除します。

説明

vrrp vrid コマンドは IPv4 VRRP グループを作成し、IPv4 VRRP グループに仮想 IP アドレスを割り当てます。あるいは既存の IPv4 VRRP グループに仮想 IP アドレスを割り当てます。

undo vrrp vrid コマンドは既存の IPv4 VRRP グループのすべての設定を削除します。あるいは既存の IPv4 VRRP グループから仮想 IP アドレスを削除します。

IPv4 VRRP グループに最大 16 の仮想 IP アドレスを割り当てることができます。

IPv4 VRRP グループが作成されているが、仮想 IPv4 アドレスが割り当てられていない場合、VRRP グループは非アクティブ状態で動作しません。

IPv4 VRRP グループの仮想 IP アドレスと VRRP グループの下流インタフェースの IP アドレスは同一サブネットにする必要があります。異なるサブネットである場合、サブネットのホストは外部ネットワークへアクセスすることができません。

VRRP がロードバランスモードで正しく動作するためには、IPv4 VRRP グループの仮想 IP アドレスが VRRP グループのインタフェースの IP アドレスでないことを確認してください。

例

IPv4 VRRP グループ 1 を作成し、仮想 IP アドレス 10.10.10.10 を VRRP グループに割り当てます。次に、仮想 IP アドレス 10.10.10.11 を割り当てます。

```
<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
```

関連コマンド

display vrrp

7.1.9 vrrp vrid authentication-mode

Syntax

vrrp vrid *virtual-router-id* **authentication-mode** { **md5** | **simple** } { **cipher** | **plain** } *string*

undo vrrp vrid *virtual-router-id* **authentication-mode**

デフォルト

VRRP グループが VRRP パケットを送受信するとき、認証は無効です。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

virtual-router-id: IPv4 VRRP グループの仮想ルータ ID を指定します。*virtual-router-id* 引数の値の設定範囲は 1～255 です。

md5: MD5 認証モードを指定します。

simple: Simple 認証モードを指定します。

cipher: 暗号テキスト認証キーを設定します。

plain: プレーンテキスト認証キーを設定します。

セキュリティ上の理由から、プレーンテキスト形式で指定されたキーは暗号化形式で保存されます。

string:キーを指定します。プレーンテキスト形式は、1~8 文字の大文字と小文字を区別する文字列です。 暗号化形式は、1~41 文字の大文字と小文字を区別する文字列です。

説明

vrrp vrid authentication-mode コマンドは認証モードを設定し、VRRP パケットの送受信を行うため、IPv4 VRRP グループの認証キーを設定します。

undo vrrp vrid authentication-mode コマンドはデフォルトに戻します。

認可されていないユーザからの攻撃を防御するため、VRRP マスタールータは、お互いを認証するため、VRRP パケットに認証キーを追加します。VRRP は以下の認証方式を提供します。

simple—Simple テキスト認証です。

送信装置は VRRP パケットに認証キーを追加し、受信装置は受信した認証キーとローカル認証キーを比較します。もし 2 つの認証キーが同一である場合、受信した VRRP パケットは正式なパケットとなります。もし同一でない場合、受信したパケットは不正なパケットとして廃棄されます。

md5—MD5 認証です。

送信装置は、認証キーと MD5 アルゴリズムを使用して送信されるパケットを暗号化し、結果を VRRP パケットの認証ヘッダに保存します。パケットを受信した装置は、認証キーでパケットを復号化し、パケットが正式かどうかをチェックします。同一である場合、受信した VRRP パケットは正式なパケットとなります。もし同一でない場合、受信したパケットは不正なパケットとして廃棄されます。

MD5 認証は Simple 認証よりもセキュリティの強度は高くなりますが、多くのリソースを消費します。

セキュリティのため、プレーンテキストで設定されたキーを含むすべてのキーは暗号テキストで保存されます。

⚠ **重要:**

- インタフェースで VRRP グループに異なる認証モードと認証キーを設定することができます。しかし、同じ VRRP グループのメンバは同じ認証モードと同じ認証キーを使用する必要があります。
- VRRPv3 を使用する場合、このコマンドは効果がありません。

例

VLAN インタフェース 2 の VRRP グループ 1 の認証モードを simple、認証キーを Sysname に設定します。

<Switch> system-view

[Switch] interface vlan-interface 2

[Switch-Vlan-interface2] vrrp vrid 1 authentication-mode simple plain Sysname

関連コマンド

display vrrp

vrrp version

7.1.10 vrrp vrid preempt-mode

Syntax

vrrp vrid *virtual-router-id* **preempt-mode** [**delay** *delay-value*]

undo vrrp vrid *virtual-router-id* **preempt-mode** [**delay**]

デフォルト

装置は preemption モードで動作します。preemption delay は 0 センチ秒です。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

virtual-router-id: IPv4 VRRP グループの仮想ルータ ID を指定します。設定範囲は 1～255 です。

delay *delay-value*: preemption delay タイマを指定します。設定範囲は 0～180000 センチ秒です。デフォルトは 0 センチ秒です。

説明

vrrp vrid preempt-mode コマンドは IPv4 VRRP グループにある装置の preemption モードを有効にし、preemption delay を設定します。

undo vrrp vrid preempt-mode コマンドは IPv4 VRRP グループにある装置の preemption モードを無効にします。

undo vrrp vrid preempt-mode delay コマンドは preemption delay をデフォルトに戻します。

Non-preemptive モードである場合、IPv4 VRRP グループの装置がマスタになるとき、たとえバックアップルータがマスタ装置より高い優先度を割り当てられたとしても、正常に動作している限り、装置はマスタとして動作します。Non-preemptive モードはマスタ装置とバックアップ装置が頻繁に切り替わることを避けることができます。

Preemptive モードである場合、優先度が稼働中のマスタ装置よりも高いことを検出したバックアップ装置は、VRRP アドバタイズメントを送信して、VRRP グループで新しいマスタ装置の選出を開始し、マスタになります。Preemptive モードは VRRP グループのもっとも高い優先度の装置が常にマスタとして動作します。

VRRP グループのメンバ間で状態が頻繁に変更することを防ぎ、バックアップ装置が情報（ルーティング情報など）を収集するための十分な時間を提供するため、バックアップがローカルの優先度より低い優先度のアドバタイズメントを受信したのち、バックアップ装置はすぐにマスタ装置になりません。マスタに切り替わる前に一定の時間待ちます。

例

VLAN インタフェース 2 の preemptive mode を有効にし、preemptive delay タイマを 500 センチ秒に設定します。

<Switch> system-view

[Switch] interface vlan-interface 2

[Switch-Vlan-interface2] vrrp vrid 1 preempt-mode delay 500

関連コマンド

display vrrp

7.1.11 vrrp vrid priority

Syntax

vrrp vrid *virtual-router-id* **priority** *priority-value*

undo vrrp vrid *virtual-router-id* **priority**

デフォルト

100

View

Interface view

定義済みユーザロール

network-admin

パラメータ

virtual-router-id: IPv4 VRRP グループの仮想ルータ ID を指定します。設定範囲は 1～255 です。

priority-value: 優先度を指定します。設定範囲は 1～254 です。値が大きいほど優先度が高くなります。

説明

vrrp vrid priority コマンドは IPv4 VRRP グループの装置の優先度を設定します。

undo vrrp vrid priority コマンドはデフォルトに戻します。

VRRP は、優先度によって VRRP グループの各装置の役割（マスタあるいはバックアップ）を決定します。高い優先度を持つ装置がマスタになります。

VRRP の優先度の範囲は 1～254 です。値が大きいほど優先度が高くなります。0 の優先度は特別用途向けに割り当てられています。255 の優先度は IP アドレスのオーナです。VRRP グループの IP アドレスのオーナとして動作する装置は常に優先度が 255 です。正常に動作する限りマスタとして動作します。

例

VLAN インタフェース 2 の VRRP グループ 1 の装置の優先度を 150 に設定します。

<Switch> system-view

[Switch] interface vlan-interface 2

[Switch-Vlan-interface2] vrrp vrid 1 priority 150

関連コマンド

display vrrp

vrrp vrid track

7.1.12 vrrp vrid timer advertise

Syntax

vrrp vrid *virtual-router-id* **timer advertise** *adver-interval*

undo vrrp vrid *virtual-router-id* **timer advertise**

デフォルト

100 センチ秒

View

Interface view

定義済みユーザロール

network-admin

パラメータ

virtual-router-id: IPv4 VRRP グループの仮想ルータ ID を指定します。設定範囲は 1～255 です。

adver-interval: 指定された IPv4 VRRP グループのマスタが VRRP アドバタイズメントを送信する間隔を指定します。設定範囲は 10～4095 センチ秒です。VRRPv2 では *adver-interval* は 100 の倍数のみ設定することができます。たとえば、設定範囲を 10～100、101～200、4001～4095 にする場合、実際の値はそれぞれ、100、200、4100 です。VRRPv3 では *adver-interval* は 100 の倍数という制限はなく、設定した値が適用されます。

説明

vrrp vrid timer advertise コマンドは IPv4 VRRP グループのマスタが VRRP アドバタイズメントを送信する間隔を指定します。

undo vrrp vrid timer advertise コマンドはデフォルトに戻します。

IPv4 VRRP グループのマスタは、自身が存在することを知らせるため、定期的に VRRP アドバタイズメントを送信します。**vrrp vrid timer advertise** コマンドを使用して VRRP アドバタイズメントを送信する間隔を設定することができます。

システムが安定して動作しつづけるため、VRRP アドバタイズメントの間隔は 100 センチ秒よりも大きい値に設定することを推奨します。

VRRPv2 では、IPv4 VRRP グループのすべてのルータは、VRRP アドバタイズメントを送信する間隔を同一にする必要があります。

VRRPv3 では、IPv4 VRRP グループのルータは、VRRP アドバタイズメントを送信する間隔を異なる間隔に設定することができます。VRRP グループのマスタは指定した間隔で VRRP アドバタイズメントを送信し、アドバタイズメントによって送信間隔の属性が運ばれます。バックアップルータがアドバタイズメントを受信した後、アドバタイズメントの間隔を記録します。(記録された間隔の 3 倍 ＋ Skew_Time) の時間が経過したとき、バックアップがマスタから新しい VRRP アドバタイズメントを受信しない場合、バックアップはマスタが故障したと認識し、新しいマスタを切り替えます。

大規模なネットワークのトラフィックによってバックアップルータが指定した時間内にマスタから VRRP アドバタイズメントを受信できず、予期しないマスタの切り替えが引き起こる可能性があります。この問題を解決するため、このコマンドを使用して送信間隔を大きい値に設定することができます。

例

IPv4 VRRP グループ 1 のマスタで VRRP アドバタイズメントを送信する間隔を 500 センチ秒に設定します。

<Switch> system-view

[Switch] interface vlan-interface 2

[Switch-Vlan-interface2] vrrp vrid 1 timer advertise 500

関連コマンド

display vrrp

7.1.13 vrrp vrid track

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**]]

デフォルト

VRRP グループは Track エントリに関連づけられていません。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

virtual-router-id: IPv4 VRRP グループ番号を指定します。設定範囲は 1～255 です。

track-entry-number: Track エントリを指定します。設定範囲は 1～1024 です。

priority reduced *priority-reduced*: 指定した Track エントリを Negative に変更するとき VRRP グループのルータの優先度を指定した値に減少させます。設定範囲は 1～255 です。デフォルトは 10 です。

switchover: 指定した Track エントリを Negative に変更した後、バックアップがすぐさまマスタに切り替わることを有効にします。

説明

vrrp vrid track コマンドは、トラックエントリで検出された変更（アップリンク状態の変更など）に対応して、VRRP グループ内のトラックエントリを Track エントリに関連づけ、マスタの切り替えを制御します。

undo vrrp vrid track コマンドは VRRP グループと Track エントリの関連づけを削除します。Track エントリが指定されていない場合、VRRP グループとすべての Track エントリ間の関連づけを削除します。

関連づけられた Track エントリが Negative 状態に変更するとき、設定に依存して以下の状態の 1 つが発生します。

- VRRP グループのルータの優先度が指定した値に減少します。
- バックアップルータである場合、すぐさまマスタとして引き継ぎます。

このコマンドを実行する前に、インタフェースで VRRP グループを作成し、仮想 IP アドレスを割り当ててください。

priority reduced が指定されているが、*priority-reduced* が指定されていない場合、Track エントリが Negative 状態に変更するとき VRRP グループのルータの優先度は 10 減少します。

Track エントリが Negative から Positive、あるいは NotReady に変更するとき、ルータは自動で優先度をもとに戻します。故障したルータが再度マスタになります。

重要:

- **vrrp vrid track priority reduced** コマンドあるいは **vrrp vrid track switchover** コマンドは IP アドレスのオーナに影響を与えることはできません。IP アドレスオーナにコマンドを設定している場合、設定は非 IP アドレスオーナに変更した後に有効になります。
- トラックエントリは VRRP グループへ関連づけする前後のどちらでも、**track** コマンドを使用してトラックエントリを作成することができます。Track エントリの設定の詳細は、オペレーションマニュアルのセクション 10 *高可用性*”*Track*”を参照してください。

例

VLAN インタフェース 2 の VRRP グループ 1 を Track エントリ 1 に関連づけ、Track エントリ 1 の状態が Negative に変更するとき、VRRP グループのルータの優先度を 50 減少させます。

<Switch> system-view

[Switch] interface vlan-interface 2

[Switch-Vlan-interface2] vrrp vrid 1 track 1 priority reduced 50

関連コマンド

display vrrp

7.2 IPv6 VRRP設定コマンド

7.2.1 display vrrp ipv6

Syntax

display vrrp ipv6 [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]] [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: インタフェースのタイプと番号を指定します。

vrid *virtual-router-id*: IPv6 VRRP グループの仮想ルータ ID を指定します。*virtual-router-id* 引数の値の範囲は 1～255 です。

verbose: IPv5 VRRP グループの詳細情報を表示します。指定しない場合、IPv4 VRRP グループの概要情報を表示します。

説明

display vrrp ipv6 コマンドは IPv6 VRRP グループの状態を表示します。

インタフェースあるいは IPv6 VRRP グループが指定されない場合、すべての IPv6 VRRP グループの状態を表示します。

インタフェースのみが指定されている場合、指定したインタフェースのすべての IPv6 VRRP グループの状態を表示します。

インタフェース、IPv6 VRRP グループの両方が指定されている場合、指定されたインタフェースの指定された IPv6 VRRP グループの状態を表示します。

例

VRRP が standard モードで動作するとき、装置のすべての IPv6 VRRP グループの概要情報を表示します。

<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
```

表 7-4 コマンド出力（standard モード）

操作	説明
Running Mode	VRRP動作モードです。（standardモード）
Total number of virtual routers	VRRPグループの総数です。
Interface	VRRPグループが設定されたインタフェースです。
VRID	仮想ルータIDです。（VRRPグループ番号）

操作	説明
State	VRRPグループのルータの状態です。 ● **Master**－マスタ状態です。 ● **Backup**－バックアップ状態です。 ● **Initialize**－初期化状態です。 ● **Inactive**－非アクティブ状態です。
Running Pri	ルータの現在の優先度です。 Trackエントリがルータの VRRPグループに関連づけられている場合、Trackエントリの状態が変更したとき、ルータの優先度が変更します。
Adver Timer	VRRPアドバタイズメントの送信間隔です。単位はセンチ秒です。
Auth Type	認証タイプです。noneのみが有効です。noneは認証が行われていないことを示します。
Virtual IP	VRRPグループの仮想IPアドレスです。

VRRP が standard モードで動作するとき、装置のすべての IPv6 VRRP グループの詳細情報を表示します。

<Switch> display vrrp ipv6 verbose

```
IPv6 Virtual Router Information:
 Running Mode      : Standard
 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
   VRRP Track Information:
     Track Object  : 1                  State : Positive   Pri Reduced : 50
   Interface Vlan-interface2
     VRID          : 11                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    : 0000-5e00-020b
Master IP      : FE80::12
```

表 7-5 コマンド出力（standard モード）

操作	説明
Running Mode	VRRP動作モードです。（standardモード）
Total number of virtual routers	VRRPグループの総数です。
Interface	VRRPグループが設定されたインタフェースです。
VRID	仮想ルータIDです。（VRRPグループ番号）
Adver Timer	VRRPアドバタイズメントの送信間隔です。単位はセンチ秒です。
Admin Status	管理状態です。upあるいはdownがあります。
State	VRRPグループのルータの状態です。 ● **Master**－マスタ状態です。 ● **Backup**－バックアップ状態です。 ● **Initialize**－初期化状態です。 ● **Inactive**－非アクティブ状態です。
Config Pri	ルータの優先度です。**vrrp ipv6 vrid priority**コマンドで設定します。
Running Pri	ルータの現在の優先度です。 Trackエントリがルータの VRRPグループに関連づけられている場合、Trackエントリの状態が変更するときルータの優先度が変更します。
Preempt Mode	Preemptive モードです。 ● **Yes**－有効です。 ● **No**－無効です。
Delay Time	Preemption delayタイマです。単位はセンチ秒です。
Become Master	バックアップルータがマスタに切り替わるまでの待ち時間です。単位はミリ秒です。
Auth Type	認証タイプです。noneのみが有効です。noneは認証が行われていないことを示します。
Virtual IP	VRRPグループの仮想IPアドレスです。
Virtual MAC	VRRPグループの仮想IPアドレスの仮想MACアドレスです。ルータがマスタであるとき表示されます。

操作	説明
Master IP	マスタが存在するインタフェースのリンクローカルアドレスです。
VRRP Track Information	Trackエントリの情報です。**vrrp ipv6 vrid track**コマンドが設定された後、表示されます。
Track Object	VRRPグループに関連づけられたTrackエントリです。
State	Trackエントリの状態です。 ● Negative ● Positive ● NotReady
Pri Reduced	関連したTrackエントリの状態がNegativeになるときに、減少する優先度の値です。
Switchover	切り替わりモードです。関連したTrackエントリがNegativeになるとき、バックアップルータがすぐさまマスタになります。

7.2.2 display vrrp ipv6 statistics

Syntax

display vrrp ipv6 statistics [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: インタフェースのタイプと番号を指定します。

vrid *virtual-router-id*: IPv6 VRRP グループの仮想ルータ ID を指定します。*virtual-router-id* 引数の値の範囲は 1～255 です。

説明

display vrrp ipv6 statistics コマンドは IPv6 VRRP グループの統計情報を表示します。

インタフェースあるいは VRRP グループが指定されない場合、すべての IPv6 VRRP グループの統計情報を表示します。

インタフェースのみが指定されている場合、指定したインタフェースのすべての IPv6 VRRP グループの統計情報を表示します。

インタフェースと IPv6 VRRP グループの両方が指定されている場合、指定されたインタフェースの指定された IPv6 VRRP グループの統計情報を表示します。

IPv6 VRRP グループの統計情報を削除する場合、**reset vrrp ipv6 statistics** コマンドを使用します。

例

VRRP が standard モードで動作するとき、装置のすべての IPv6 VRRP グループの統計情報を表示します。

<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

Global statistics
CheckSum Errors       : 0
Version Errors        : 0
VRID Errors           : 0
```

表 7-6 コマンド出力

操作	説明
Interface	IPv6 VRRP グループが設定されたインタフェースです。
VRID	IPv6 VRRP グループの数です。
CheckSum Errors	チェックサムエラーのパケット数です。
Version Errors	バージョンエラーのパケット数です。
Invalid Pkts Rcvd	不正なパケットタイプのパケットを受信した数です。
Unexpected Pkts Rcvd	予期しないパケットを受信した数です。
Advertisement Interval Errors	アドバタイズメント間隔のエラーによるパケット数です。
Hop Limit Errors	ホップリミットエラーのパケット数です。

操作	説明
Auth Failures	認証に失敗したパケット数です。
Invalid Auth Type	不正な認証タイプのため認証に失敗したパケット数です。
Auth Type Mismatch	認証タイプが不一致のため認証に失敗したパケット数です。
Packet Length Errors	VRRPパケット長エラーのパケット数です。
Address List Errors	仮想IPアドレス制限エラーのパケット数です。
Become Master	ルータがマスタとして選定された回数です。
Priority Zero Pkts Rcvd	ルータの優先度が0のアドバタイズメントを受信した数です。
Adver Rcvd	アドバタイズメントを受信した数です。
Priority Zero Pkts Sent	ルータの優先度が0のアドバタイズメントを送信した数です。
Adver Sent	アドバタイズメントを送信した数です。
Global statistics	すべてのIPv6 VRRPグループのグローバルの統計情報です。
CheckSum Errors	チェックサムエラーのパケットの総数です。
Version Errors	バージョンエラーのパケットの総数です。
VRID Errors	VRIDエラーのパケットの総数です。

関連コマンド

reset vrrp ipv6 statistics

7.2.3 reset vrrp ipv6 statistics

Syntax

reset vrrp ipv6 statistics [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]]

View

User view

定義済みユーザロール

network-admin

パラメータ

interface *interface-type interface-number*: インタフェースのタイプと番号を指定します。

vrid *virtual-router-id*: IPv6 VRRP グループの仮想ルータ ID を指定します。設定範囲は 1～255 です。

説明

reset vrrp ipv6 statistics コマンドは IPv6 VRRP グループの統計情報を削除します。

インタフェースあるいは IPv6 VRRP グループが指定されない場合、すべての IPv6 VRRP グループの統計情報を削除します。

インタフェースのみが指定されている場合、指定したインタフェースのすべての IPv6 VRRP グループの統計情報を削除します。

インタフェースと IPv6 VRRP グループの両方が指定されている場合、指定されたインタフェースの指定された IPv6 VRRP グループの統計情報を削除します。

例

すべてのインタフェースのすべての IPv6 VRRP グループの統計情報を削除します。

<Switch> reset vrrp ipv6 statistics

関連コマンド

display vrrp ipv6 statistics

7.2.4 vrrp ipv6 dscp

Syntax

vrrp ipv6 dscp *dscp-value*

undo vrrp ipv6 dscp

デフォルト

56

View

System view

定義済みユーザロール

network-admin

パラメータ

dscp-value: IPv6 VRRP の DSCP を指定します。設定範囲は 0～63 です。

説明

vrrp ipv6 dscp コマンドは IPv6 VRRP パケットの DSCP を設定します。

undo vrrp ipv6 dscp コマンドはデフォルトに戻します。

VRRP パケットの DSCP の値はパケットのプライオリティを指定します。パケットを送信するプライオリティに影響します。DSCP の値が大きくなると、プライオリティが高くなります。

例

IPv6 VRRP パケットの DSCP を 30 に設定します。

<Switch> system-view

[Switch] vrrp ipv6 dscp 30

7.2.5 vrrp ipv6 vrid

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**]]]

デフォルト

設定なし

View

Interface view

定義済みユーザロール

network-admin

パラメータ

virtual-router-id: IPv6 VRRP グループの仮想ルータ ID を指定します。設定範囲は 1～255 です。

virtual-ip *virtual-address*: 仮想 IPv6 アドレスを指定します。パラメータを指定しない場合、**undo vrrp ipv6 vrid** コマンドは既存の IPv6 VRRP グループからすべての仮想 IPv6 アドレスを削除します。

link-local: 仮想 IPv6 アドレスとしてリンクローカルアドレスを指定します。

説明

vrrp ipv6 vrid コマンドは IPv6 VRRP グループを作成し、IPv6 VRRP グループに仮想 IPv6 アドレスを割り当てます。あるいは既存の IPv6 VRRP グループに仮想 IPv6 アドレスを割り当てます。

undo vrrp ipv6 vrid コマンドは既存の IPv6 VRRP グループのすべての設定を削除します。あるいは既存の IPv6 VRRP グループから仮想 IPv6 アドレスを削除します。

vrrp ipv6 vrid コマンドは IPv6 VRRP グループを作成し、IPv6 VRRP グループに仮想 IPv6 アドレスを割り当てます。あるいは既存の IPv6 VRRP グループに仮想 IPv6 アドレスを割り当てます。

undo vrrp ipv6 vrid コマンドは既存の IPv6 VRRP グループのすべての設定を削除します。あるいは既存の IPv6 VRRP グループから仮想 IPv6 アドレスを削除します。

IPv6 VRRP グループに最大 16 の仮想 IPv6 アドレスを割り当てることができます。

IPv6 VRRP グループに割り当てる最初の仮想 IPv6 アドレスはリンクローカルアドレスにする必要があります。仮想 IPv6 アドレスを削除する場合、最後にリンクローカルアドレスを削除する必要があります。

IPv6 VRRP グループは仮想 IPv6 アドレスとして 1 つのリンクローカルアドレスのみ持つことができます。

IPv6 VRRP グループが作成されているが、仮想 IPv6 アドレスが割り当てられていない場合、IPv6 VRRP グループは非アクティブ状態で動作しません。

IPv6 VRRP グループの仮想 IPv6 アドレスと IPv6 VRRP グループの下流インタフェースの IPv6 アドレスは同一サブネットにする必要があります。異なるサブネットである場合、サブネットのホストは外部ネットワークへアクセスすることができません。

例

IPv6 VRRP グループ 1 を作成し、IPv6 VRRP グループに仮想 IPv6 アドレス fe80::10 を割り当てます。IPv6 VRRP グループに仮想 IPv6 アドレス 1::10 を割り当てます。

```
<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
```

関連コマンド

display vrrp ipv6

7.2.6 vrrp ipv6 vrid preempt-mode

Syntax

vrrp ipv6 vrid *virtual-router-id* **preempt-mode** [**delay** *delay-value*]

undo vrrp ipv6 vrid *virtual-router-id* **preempt-mode** [**delay**]

デフォルト

装置は preemption モードで動作します。preemption delay は 0 センチ秒です。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

virtual-router-id: IPv6 VRRP グループの仮想ルータ ID を指定します。設定範囲は 1～255 です。

delay *delay-value*: preemption delay タイマを指定します。設定範囲は 0～180000 センチ秒です。デフォルトは 0 センチ秒です。

説明

vrrp ipv6 vrid preempt-mode コマンドは IPv6 VRRP グループにある装置の preemption モードを有効にし、preemption delay を設定します。

undo vrrp ipv6 vrid preempt-mode コマンドは IPv6 VRRP グループにある装置の preemption モードを無効にします。

undo vrrp ipv6 vrid preempt-mode delay コマンドは preemption delay をデフォルトに戻します。

Non-preemptive モードである場合、IPv6 VRRP グループの装置がマスタになるとき、たとえバックアップルータがマスタ装置より高い優先度を割り当てられたとしても、正常に動作している限り、装置はマスタとして動作します。Non-preemptive モードはマスタ装置とバックアップ装置が頻繁に切り替わることを避けることができます。

Preemptive モードである場合、優先度が稼働中のマスタ装置よりも高いことを検出したバックアップ装置は、VRRP アドバタイズメントを送信して、IPv6 VRRP グループで新しいマスタ装置の選出を開始し、マスタになります。Preemptive モードは IPv6 VRRP グループのもっとも高い優先度の装置が常にマスタとして動作します。

IPv6 VRRP グループのメンバ間で状態が頻繁に変更することを防ぎ、バックアップ装置が情報（ルーティング情報など）を収集するための十分な時間を提供するため、バックアップがローカルの優先度より低い優先度のアドバタイズメントを受信したのち、バックアップ装置はすぐにマスタ装置になりません。マスタに切り替わる前に一定の時間待ちます。

例

VRRP グループ 1 の preemptive mode を有効にし、preemptive delay タイマを 500 センチ秒に設定します。

<Switch> system-view

[Switch] interface vlan-interface 2

[Switch-Vlan-interface2] vrrp ipv6 vrid 10 preempt-mode delay 500

関連コマンド

display vrrp ipv6

7.2.7 vrrp ipv6 vrid priority

Syntax

vrrp ipv6 vrid *virtual-router-id* **priority** *priority-value*

undo vrrp ipv6 vrid *virtual-router-id* **priority**

デフォルト

100

View

Interface view

定義済みユーザロール

network-admin

パラメータ

virtual-router-id: IPv6 VRRP グループの仮想ルータ ID を指定します。設定範囲は 1～255 です。

priority-value: 優先度を指定します。設定範囲は 1～254 です。値が大きいほど優先度が高くなります。

説明

vrrp ipv6 vrid priority コマンドは IPv6 VRRP グループの装置の優先度を設定します。

undo vrrp ipv6 vrid priority コマンドはデフォルトに戻します。

VRRP は、優先度によって IPv6 VRRP グループの各装置の役割（マスタあるいはバックアップ）を決定します。高い優先度を持つ装置がマスタになります。

VRRP の優先度の範囲は 0～255 です。値が大きいほど優先度が高くなります。1～255 の優先度は設定可能です。0 の優先度は特別用途向けに割り当てられています。255 の優先度は IP アドレスのオーナです。IPv6 VRRP グループの IP アドレスのオーナとして動作する装置は常に優先度が 255 です。正常に動作する限りマスタとして動作します。

例

VLANインタフェース 2の IPv6 VRRP グループ 1の装置の優先度を 150に設定します。

<Switch> system-view

[Switch] interface vlan-interface 2

[Switch-Vlan-interface2] vrrp ipv6 vrid 1 priority 150

関連コマンド

display vrrp ipv6

7.2.8 vrrp ipv6 vrid timer advertise

Syntax

vrrp ipv6 vrid *virtual-router-id* **timer advertise** *adver-interval*

undo vrrp ipv6 vrid *virtual-router-id* **timer advertise**

デフォルト

100 センチ秒

View

Interface view

定義済みユーザロール

network-admin

パラメータ

virtual-router-id: IPv6 VRRP グループの仮想ルータ ID を指定します。設定範囲は 1～255 です。

adver-interval: 指定された IPv6 VRRP グループのマスタが VRRP アドバタイズメントを送信する間隔を指定します。設定範囲は 100～4095 センチ秒です。

説明

vrrp ipv6 vrid timer advertise コマンドは IPv6 VRRP グループのマスタが VRRP アドバタイズメントを送信する間隔を指定します。

undo vrrp ipv6 vrid timer advertise コマンドはデフォルトに戻します。

IPv6 VRRP グループのマスタは、自身が存在することを宣言するため、定期的に VRRP アドバタイズメントを送信します。**vrrp ipv6 vrid timer advertise** コマンドを使用して VRRP アドバタイズメントを送信する間隔を設定することができます。

システムが安定して動作しつづけるため、VRRP アドバタイズメントの間隔は 100 センチ秒よりも大きい値に設定することを推奨します。

IPv6 VRRP グループのマスタは指定した間隔で VRRP アドバタイズメントを送信し、アドバタイズメントによって送信間隔の属性が運ばれます。バックアップルータがアドバタイズメントを受信した後、アドバタイズメントの間隔を記録します。（記録された間隔の 3 倍＋Skew_Time）の時間が経過したとき、バックアップがマスタから新しい VRRP アドバタイズメントを受信しない場合、バックアップはマスタが故障したと認識し、新しいマスタを切り替えます。

大規模なネットワークのトラフィックによってバックアップルータが指定した時間内にマスタから VRRP アドバタイズメントを受信できず、予期しないマスタの切り替えを引き起こす可能性があります。この問題を解決するため、このコマンドを使用して送信間隔を大きい値に設定することができます。

例

IPv6 VRRP グループ 1 のマスタで VRRP アドバタイズメントを送信する間隔を 500 センチ秒に設定します。

<Switch> system-view

[Switch] interface vlan-interface 2

[Switch-Vlan-interface2] vrrp ipv6 vrid 1 timer advertise 500

関連コマンド

display vrrp ipv6

7.2.9 vrrp ipv6 vrid track

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**]]

デフォルト

IPv6 VRRP グループは Track エントリに関連づけられていません。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

virtual-router-id: IPv6 VRRP グループ番号を指定します。設定範囲は 1～255 です。

track-entry-number: Track エントリを指定します。設定範囲は 1～1024 です。

priority reduced *priority-reduced*: 指定した Track エントリを Negative に変更するとき VRRP グループのルータの優先度を指定した値に減少させます。設定範囲は 1～255 です。デフォルトは 10 です。

switchover: 指定した Track エントリを Negative に変更した後、バックアップがすぐさまマスタに切り替わることを有効にします。

説明

vrrp ipv6 vrid track コマンドは、トラックエントリで検出された変更（アップリンク状態の変更など）に対応して、IPv6 VRRP グループ内のトラックエントリを Track エントリに関連づけ、マスタの切り替えを制御します。

undo vrrp ipv6 vrid track コマンドは IPv6 VRRP グループと Track エントリの関連づけを削除します。Track エントリが指定されていない場合、VRRP グループとすべての Track エントリ間の関連づけを削除します。

関連づけられた Track エントリが Negative 状態に変更するとき、設定に依存して以下の状態の 1 つが発生します。

VRRP グループのルータの優先度が指定した値に減少します。
バックアップルータである場合、すぐさまマスタとして引き継ぎます。

このコマンドを実行する前に、インタフェースで IPv6 VRRP グループを作成し、仮想 IPv6 アドレスを割り当ててください。

priority reduced が指定されているが、*priority-reduced* が指定されていない場合、Track エントリが Negative 状態に変更するとき IPv6 VRRP グループのルータの優先度は 10 減少します。

Track エントリが Negative から Positive、あるいは NotReady に変更するとき、ルータは自動で優先度をもとに戻します。故障したルータが再度マスタになります。

⚠ **重要:**

- **vrrp ipv6 vrid track priority reduced** コマンドあるいは **vrrp ipv6 vrid track switchover** コマンドは IP アドレスのオーナに影響を与えることはできません。IP アドレスオーナにコマンドを設定している場合、設定は非 IP アドレスオーナに変更した後に有効になります。
- トラックエントリは IPv6 VRRP グループへ関連づけする前後のどちらでも、**track** コマンドを使用してトラックエントリを作成することができます。Track エントリの設定の詳細は、オペレーションマニュアルのセクション 10 *高可用性*”*Track*”を参照してください。

例

VLAN インタフェース 2 の IPv6 VRRP グループ 1 を Track エントリ 1 に関連づけ、Track エントリ 1 の状態が Negative に変更するとき、VRRP グループのルータの優先度を 50 減少させます。

<Switch> system-view

[Switch] interface Vlan-interface2

[Switch-Vlan-interface2] vrrp vrid 1 track 1 priority reduced 50

関連コマンド

display vrrp ipv6

目次

このセクションのページは **10-x-x** です。

8 章 BFD 8-1
8.1 BFD 設定コマンド 8-1
8.1.1 bfd authentication-mode 8-1
8.1.2 bfd demand enable 8-2
8.1.3 bfd detect-multiplier 8-3
8.1.4 bfd echo enable 8-4
8.1.5 bfd echo-source-ip 8-5
8.1.6 bfd echo-source-ipv6 8-5
8.1.7 bfd min-echo-receive-interval 8-6
8.1.8 bfd min-receive-interval 8-7
8.1.9 bfd min-transmit-interval 8-8
8.1.10 bfd multi-hop authentication-mode 8-9
8.1.11 bfd multi-hop destination-port 8-10
8.1.12 bfd multi-hop detect-multiplier 8-11
8.1.13 bfd multi-hop min-receive-interval 8-12
8.1.14 bfd multi-hop min-transmit-interval 8-13
8.1.15 bfd session init-mode 8-14
8.1.16 display bfd session 8-15
8.1.17 reset bfd session statistics 8-18
8.1.18 snmp-agent trap enable bfd 8-18

8章 BFD

8.1 BFD設定コマンド

8.1.1 bfd authentication-mode

Syntax

bfd authentication-mode { **md5** | **sha1** | **simple** } *key-id* { **cipher** | **plain** } *string*

undo bfd authentication-mode

デフォルト

設定なし

View

Interface view

BFD template view

定義済みユーザロール

network-admin

パラメータ

md5: MD5 アルゴリズムを指定します。

sha1: SHA1 アルゴリズムを指定します。

simple: simple 認証モードを指定します。

key-id: 認証 key ID を設定します。設定範囲は 1～255 です。

cipher: 暗号文パスワードを設定します。

plain: プレーンテキストパスワードを設定します。セキュリティのために、プレーンテキストで設定されたパスワードを含むすべての認証パスワードは暗号文で保存します。

string: パスワードを指定します。暗号文パスワードの設定範囲は 1～16 文字です。プレーンテキストパスワードの設定範囲は 33～53 文字です。大文字、小文字を区別します。

説明

bfd authentication-mode コマンドは、シングル hop BFD コントロールパケットの BFD 認証モードを設定します。

undo bfd authentication-mode コマンドは、デフォルトに戻します。

BFD セッションセキュリティを強化するためにこのコマンドを使用してください。

このコマンドは BFD バージョン 0 ではサポートしていません。設定は適用されません。

例

VLAN-interface 11 にシングル hop BFD コントロールパケットの simple 認証モードを設定します。key ID は 1 で、パスワードは 123456 です。

<Switch> system-view

[Switch] interface vlan-interface 11

[Switch-Vlan-interface11] bfd authentication-mode simple 1 plain 123456

8.1.2 bfd demand enable

Syntax

bfd demand enable

undo bfd demand enable

デフォルト

Asynchronous モード

View

Interface view

定義済みユーザロール

network-admin

説明

bfd demand enable コマンドは、Demand BFD セッションモードを有効にします。

undo bfd demand enable コマンドは、デフォルトに戻します。

Demand モードでは、装置は BFD コントロールパケットを周期的に送信します。ピアの片端がデフォルト設定の Asynchronous モードで動作する場合、BFD コントロールパケットの送信を停止します。片端が Demand モードで動作する場合、両端装置で BFD コントロールパケットの送信を停止します。別のシステムへの接続性が明示する必要がある際は、システムはネゴシエートした送信間隔で Poll（P）ビットがセットされた BFD コントロールパケットを数回送信します。検出時間内に応答がない場合、セッションがダウンしたとみなします。接続していると認識した場合、次のコマンドが送信されるまで BFD コントロールパケットを送信しません。

Asynchronous モードでは、装置は BFD コントロールパケットを周期的に送信します。指定した時間内に BFD コントロールパケットを受信しない場合、装置はセッションがダウンしたとみなします。

このコマンドは BFD バージョン 0 ではサポートしていません。設定は適用されません。

例

VLAN-interface 11 で Demand BFD セッションモードを有効にします。

<Switch> system-view

[Switch] interface vlan-interface 11

[Switch-Vlan-interface11] bfd demand enable

8.1.3 bfd detect-multiplier

Syntax

bfd detect-multiplier *value*

undo bfd detect-multiplier

デフォルト

5

View

Interface view

BFD template view

定義済みユーザロール

network-admin

パラメータ

value: シングル Hop 検出時間の乗数を指定します。設定範囲は 3～50 です。

説明

bfd detect-multiplier コマンドはシングル Hop 検出時間の乗数を設定します。

undo bfd detect-multiplier コマンドはデフォルトに戻します。

検出時間の乗数は、廃棄される同時 BFD パケット（コントロールパケットとエコーパケットを含みます）の最大数を決定します。

表 8-1 検出間隔の計算方法

モード	検出間隔
エコーパケットモード	送信側の検出時間の乗数 × 送信側の実際のパケット送信間隔
BFDセッションのasynchronousモードのコントロールパケットモード	受信側の検出時間の乗数 × 受信側の実際のパケット送信間隔

モード	検出間隔
BFDセッションのdemandモードのコントロールパケットモード	送信側の検出時間の乗数 × 送信側の実際のパケット送信間隔

例

VLAN インタフェース 11 のシングル Hop 検出時間の乗数を 6 に設定します。

<Switch> system-view

[Switch] interface vlan-interface 11

[Switch-Vlan-interface11] bfd detect-multiplier 6

8.1.4 bfd echo enable

Syntax

bfd echo enable

undo bfd echo enable

デフォルト

無効

View

Interface view

定義済みユーザロール

network-admin

説明

bfd echo enable to コマンドは、エコーパケットモードを有効にします。

undo bfd echo enable コマンドは、設定をデフォルトに戻します。

コントロールパケットが送信されてセッションがアップしている BFD セッションにエコーパケットモードを有効にした場合、BFD は以下を行います。

- リンク接続を検出するために周期的にエコーパケットを送信します。
- 同時にコントロールパケットの受信レートを下げます。

このコマンドは BFD バージョン 0 ではサポートしていません。設定は適用されません。

例

VLAN インタフェース 11 でエコーパケットモードを有効にします。

<Switch> system-view

[Switch] interface vlan-interface 11

[Switch-Vlan-interface11] bfd echo enable

8.1.5 bfd echo-source-ip

Syntax

bfd echo-source-ip *ip-address*

undo bfd echo-source-ip

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

ip-address: BFD エコーパケットの送信元 IP アドレスを指定します。

説明

bfd echo-source-ip コマンドは BFD エコーパケットの送信元 IP アドレスを設定します。

undo bfd echo-source-ip コマンドは BFD エコーパケットの送信元 IP アドレスを削除します。

送信元 IP アドレスは、ローカルインタフェースの IP アドレスと同一ネットワークセグメントに属することができません。そうでなければ、大量の ICMP リダイレクトパケットがピアから送信され、リンクの衝突が発生する可能性があります。

例

BFD エコーパケットの送信元 IP アドレスを 8.8.8.8 に設定します。

<Switch> system-view

[Switch] bfd echo-source-ip 8.8.8.8

8.1.6 bfd echo-source-ipv6

Syntax

bfd echo-source-ipv6 *ipv6-address*

undo bfd echo-source-ipv6

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

ipv6-address: BFD エコーパケットの送信元 IPv6 アドレスを指定します。

説明

bfd echo-source-ipv6 コマンドは、BFD エコーパケットの送信元 IPv6 アドレスを設定します。

undo bfd echo-source-ipv6 コマンドは、BFD エコーパケットの設定済み送信元 IPv6 アドレスを削除します。

エコーパケットの送信元 IPv6 アドレスは、グローバルユニキャストアドレスだけです。

送信元 IPv6 アドレスは、ローカルインタフェースの IP アドレスと同じネットワークセグメントには存在できません。そうでないと、多数の ICMP リダイレクトパケットがピアから送信され、リンクの輻輳が発生する可能性があります。

例

BFD エコーパケットの送信元 IPv6 アドレスを 80::2 に設定します。

<Switch> system-view

[Switch] bfd echo-source-ipv6 80::2

8.1.7 bfd min-echo-receive-interval

Syntax

bfd min-echo-receive-interval *interval*

undo bfd min-echo-receive-interval

デフォルト

400 ミリ秒

View

Interface view

定義済みユーザロール

network-admin

パラメータ

interval: BFD エコーパケットの最小受信間隔を指定します。単位はミリ秒です。設定範囲は 100～1000 ミリ秒、あるいは 0 です。

説明

bfd min-echo-receive-interval コマンドは BFD エコーパケットの最小受信間隔を設定します。

undo bfd min-echo-receive-interval コマンドはデフォルトに戻します。

このコマンドは BFD エコーパケットを受信する間隔を設定します。この間隔は実際の BFD エコーパケットを送信する間隔です。

例

VLAN インタフェース 11 の BFD エコーパケットの最小受信間隔を 500 ミリ秒に設定します。

<Switch> system-view

[Switch] interface vlan-interface 11

[Switch-Vlan-interface11] bfd min-echo-receive-interval 500

8.1.8 bfd min-receive-interval

Syntax

bfd min-receive-interval *interval*

undo bfd min-receive-interval

デフォルト

400 ミリ秒

View

Interface view

BFD template view

定義済みユーザロール

network-admin

パラメータ

interval: シングル Hop BFD コントロールパケットの最小受信間隔を指定します。単位はミリ秒です。設定範囲は 100～1000 ミリ秒です。

説明

bfd min-receive-interval コマンドはシングル Hop BFD コントロールパケットの最小受信間隔を設定します。

undo bfd min-receive-interval コマンドはデフォルトに戻します。

リモートエンド装置のレートを送信する BFD コントロールパケットが、ローカルエンド装置のレートを受信する BFD コントロールパケットを超過することを防止するため、このコマンドを設定します。

リモートエンド装置の実際のコントロールパケットの送信間隔は、以下の値で大きいほうとなります。

- リモートエンド装置の BFD コントロールパケットの最小送信間隔
- ローカルエンド装置の BFD コントロールパケットの最小受信間隔

例

VLAN インタフェース 11 のシングル Hop BFD コントロールパケットの最小受信間隔を 500 ミリ秒に設定します。

<Switch> system-view

[Switch] interface vlan-interface 11

[Switch-Vlan-interface11] bfd min-receive-interval 500

8.1.9 bfd min-transmit-interval

Syntax

bfd min-transmit-interval *interval*

undo bfd min-transmit-interval

デフォルト

400 ミリ秒

View

Interface view

BFD template view

定義済みユーザロール

network-admin

パラメータ

interval: シングル Hop BFD コントロールパケットの最小送信間隔を指定します。単位はミリ秒です。設定範囲は 100～1000 ミリ秒です。

説明

bfd min-transmit-interval コマンドはシングル Hop BFD コントロールパケットの最小送信間隔を設定します。

undo bfd min-transmit-interval コマンドはデフォルトに戻します。

このコマンドは BFD パケットの送信レートがエンド装置の能力を超過しないようにします。

ローカルエンド装置の実際のコントロールパケットの送信間隔は、以下の値で大きいほうとなります。

- ローカルエンド装置の BFD コントロールパケットの最小送信間隔
- リモートエンド装置の BFD コントロールパケットの最小受信間隔

例

VLAN インタフェース 11 のシングル Hop BFD コントロールパケットの最小送信間隔を 500 ミリ秒に設定します。

<Switch> system-view

[Switch] interface vlan-interface 11

[Switch-Vlan-interface11] bfd min-transmit-interval 500

8.1.10 bfd multi-hop authentication-mode

Syntax

bfd multi-hop authentication-mode { **md5** | **sha1** | **simple** } *key-id* { **cipher** | **plain** } *string*

undo bfd multi-hop authentication-mode

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

md5: MD5 アルゴリズムを指定します。

sha1: SHA1 アルゴリズムを指定します。

simple: simple 認証モードを指定します。

key-id: 認証 key ID を設定します。設定範囲は 1～255 です。

cipher: 暗号文パスワードを設定します。

plain: プレーンテキストパスワードを設定します。セキュリティのために、プレーンテキストで設定されたパスワードを含むすべての認証パスワードは暗号文で保存します。

string: パスワードを指定します。暗号文パスワードの設定範囲は 1～16 文字です。プレーンテキストパスワードの設定範囲は 33～53 文字です。大文字、小文字を区別します。

説明

bfd multi-hop authentication-mode コマンドは、マルチ Hop BFD コントロールパケットの認証モードを設定します。

undo bfd multi-hop authentication-mode コマンドは、設定をデフォルトに戻します。

BFD セッションセキュリティを強化するためにこのコマンドを使用してください。

このコマンドは BFD バージョン 0 ではサポートしていません。設定は適用されません。

例

マルチ hop BFD コントロールパケットの simple 認証モードを設定します。key ID は 1 で、パスワードは 123456 です。

<Switch> system-view

[Switch] bfd multi-hop authentication-mode simple 1 plain 123456

8.1.11 bfd multi-hop destination-port

Syntax

bfd multi-hop destination-port *port-number*

undo bfd multi-hop destination-port

デフォルト

4784

View

System view

定義済みユーザロール

network-admin

パラメータ

port-number: マルチ hop BFD コントロールパケットの宛先ポート番号を、3784 または 4784 と指定します。

説明

bfd multi-hop destination-port コマンドは、マルチ hop BFD コントロールパケットの宛先ポート番号を設定します。

undo bfd multi-hop destination-port コマンドは、設定をデフォルトに戻します。

例

マルチ hop BFD コントロールパケットの宛先ポート番号を 3784 で指定します。

<Switch> system-view

[Switch] bfd multi-hop destination-port 3784

8.1.12 bfd multi-hop detect-multiplier

Syntax

bfd multi-hop detect-multiplier *value*

undo bfd multi-hop detect-multiplier

デフォルト

5

View

System view

定義済みユーザロール

network-admin

パラメータ

value: マルチ Hop 検出時間の乗数を指定します。設定範囲は 3～50 です。

説明

bfd multi-hop detect-multiplier コマンドは、マルチ Hop 検出時間の乗数を設定します。

undo bfd multi-hop detect-multiplier コマンドは、デフォルトに戻します。

検出時間の乗数は、廃棄される同時 BFD コントロールパケットの最大数を決定します。

表 8-2 検出間隔の計算方法

モード	検出間隔
BFDセッションのasynchronousモードのコントロールパケットモード	受信側の検出時間の乗数 × 受信側の実際のパケット送信間隔
BFDセッションのdemandモードのコントロールパケットモード	送信側の検出時間の乗数 × 送信側の実際のパケット送信間隔

例

マルチ Hop 検出時間の乗数を 6 に設定します。

<Switch> system-view

[Switch] bfd multi-hop detect-multiplier 6

8.1.13 bfd multi-hop min-receive-interval

Syntax

bfd multi-hop min-receive-interval *interval*

undo bfd multi-hop min-receive-interval

デフォルト

400 ミリ秒

View

System view

定義済みユーザロール

network-admin

パラメータ

interval: マルチ Hop BFD コントロールパケットの最小受信間隔を指定します。単位はミリ秒で、設定範囲は 100～1000 ミリ秒です。

説明

bfd multi-hop min-receive-interval コマンドは、マルチ Hop BFD コントロールパケットの最小受信間隔を設定します。

undo bfd multi-hop min-receive-interval コマンドは、デフォルトに戻します。

リモートエンドのパケット送信レートがローカルエンドのパケット受信能力を超えた際は、リモートエンドは BFD コントロールパケットの送信間隔をローカルエンドのコントロールパケットの最小受信間隔に動的に調整します。

例

マルチ Hop BFD コントロールパケットの最小受信間隔を 500 ミリ秒に設定します。

<Switch> system-view

[Switch] bfd multi-hop min-receive-interval 500

8.1.14 bfd multi-hop min-transmit-interval

Syntax

bfd multi-hop min-transmit-interval *interval*

undo bfd multi-hop min-transmit-interval

デフォルト

400 ミリ秒

View

System view

定義済みユーザロール

network-admin

パラメータ

interval: マルチ Hop BFD コントロールパケットの最小送信間隔を指定します。単位はミリ秒で、設定範囲は 100～1000 ミリ秒です。

説明

bfd multi-hop min-transmit-interval コマンドは、マルチ Hop BFD コントロールパケットの最小送信間隔を設定します。

undo bfd multi-hop min-transmit-interval コマンドは、デフォルトに戻します。

リモートエンドのパケット送信レートがローカルエンドのパケット受信能力を超えた際は、リモートエンドは BFD コントロールパケットの送信間隔をローカルエンドのコントロールパケットの最小受信間隔に動的に調整します。

BFD パケットの送信レートが装置の能力を超えないことを確認するためにこのコマンドを使用してください。

ローカルエンド装置の実際の BFD コントロールパケットの送信間隔は、以下の値で大きいほうとなります。

- ローカルエンド装置の BFD コントロールパケットの最小送信間隔

- リモートエンド装置の BFD コントロールパケットの最小受信間隔

例

マルチ Hop BFD コントロールパケットの最小送信間隔を 500 ミリ秒に設定します。

<Switch> system-view

[Switch] bfd multi-hop min-transmit-interval 500

8.1.15 bfd session init-mode

Syntax

bfd session init-mode { **active** | **passive** }

undo bfd session init-mode

デフォルト

active

View

System view

定義済みユーザロール

network-admin

パラメータ

active: アクティブモードを使用します。アクティブモードでは、リモートエンド装置から BFD コントロールパケットを受信するかどうかにかかわらず、BFD は BFD コントロールパケットをリモートエンド装置に能動的に送信します。

passive: パッシブモードを使用します。パッシブモードでは、BFD は BFD コントロールパケットをリモートエンド装置に能動的に送信しません。リモートエンド装置から BFD コントロールパケットを受信した後のみ BFD コントロールパケットを送信します。

説明

bfd session init-mode コマンドは BFD セッションを確立するためにモードを設定します。

undo bfd session init-mode コマンドはデフォルトに戻します。

BFD セッションを確立するため、少なくともアクティブモードで 1 つのエンド装置を動作させる必要があります。

このコマンドは BFD バージョン 0 ではサポートしていません。設定は適用されません。

例

セッションを確立するためにパッシブモードを設定します。

<Switch> system-view

[Switch] bfd session init-mode passive

8.1.16 display bfd session

Syntax

display bfd session [**discriminator** *value* | **verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

discriminator *value*: ローカル ID を指定します。設定範囲は 1～4294967295 です。指定しない場合、すべての BFD セッションの概要を表示します。

verbose: BFD セッションの詳細情報を表示します。指定しない場合、BFD セッションの概要情報を表示します。

説明

display bfd session コマンドは BFD セッションの情報を表示します。

例

すべての IPv4 BFD セッションの情報を表示します。

<Switch> display bfd session

```
Total Session Num: 1    Up Session Num: 1    Init Mode: Active

IPv4 Session Working Under Ctrl Mode:

LD/RD         SourceAddr      DestAddr        State    Holdtime    Interface
513/513       1.1.1.1         1.1.1.2         Up       2297ms      Vlan100
```

すべての IPv4 BFD セッションの詳細情報を表示します。

<Switch> display bfd session verbose

```
Total Session Num: 1    Up Session Num: 1    Init Mode: Active

IPv4 Session Working Under Ctrl 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
```

すべての IPv6 BFD セッションの情報を表示します。

<Switch> display bfd session

```
Total Session Num: 1    Up Session Num: 1    Init Mode: Active

IPv6 Session Working Under Ctrl 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
```

すべての IPv6 BFD セッションの詳細情報を表示します。

<Switch> display bfd session verbose

```
Total Session Num: 1    Up Session Num: 1    Init Mode: Active

IPv6 Session Working Under Ctrl 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
```

表 8-3 コマンド出力

フィールド	説明
Total Session Num	BFDセッションの総数です。
Up Session Num	アクティブのBFDセッションの総数です。
Init Mode	BFDの動作モードです。active、passiveがあります。
Session Working Under Ctrl Mode	BFDセッションモードです。 ● **Ctrl**—コントロールパケットモードです。 ● **Echo**—エコーパケットモードです。
Local Discr/LD	セッションのローカルIDです。
Remote Discr/RD	セッションのリモートIDです。
Source IP/SourceAddr	セッションの送信元IPアドレスです。
Destination IP/DestAddr	セッションの宛先IPアドレスです。
Session State/State	セッションの状態です。up、downがあります。
Interface	セッションのインタフェース名です。
Min Tx Inter	最小送信間隔です。
Min Rx Inter	最小受信間隔です。
Act Tx Inter	実際の送信間隔です。
Detect Inter	実際のセッション検出タイマです。
Rx Count	受信したパケット数です。
Tx Count	送信したパケット数です。
Hold Time/Holdtime	セッションタイマが終了するまでの時間です。
Auth mode	セッション認証モードです。（simpleモードのみサポートしています）
Connect Type	インタフェースの接続タイプです。direct、indirectがあります。
Running up for	セッションがアップとなっている間隔です。

フィールド	説明
Detect Mode	検出モードです。 ● **Async**—Asynchronousモードです。 ● **Demand**—Demandモードです。 ● **Async/Echo**—エコー検出機能が有効なAsynchronousモードです。 ● **Demand/Echo**—エコー検出機能が有効なDemandモードです。
Slot	IRFスタックのメンバIDです。
Diag Info	セッションの診断情報です。

8.1.17 reset bfd session statistics

Syntax

reset bfd session statistics

View

User view

定義済みユーザロール

network-admin

説明

reset bfd session statistics コマンドは BFD セッションの統計情報を削除します。

例

BFD セッションの統計情報を削除します。

<Switch> reset bfd session statistics

8.1.18 snmp-agent trap enable bfd

Syntax

snmp-agent trap enable bfd

undo snmp-agent trap enable bfd

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

snmp-agent trap enable bfd コマンドは BFD に関する SNMP notification の送信を有効にします。

undo snmp-agent trap enable bfd コマンドは BFD に関する SNMP notification の送信を無効にします。

NMS に重大な BFD に関するイベントを通知するため、ポートセキュリティの SNMP notification を有効にします。SNMP notification を正常に送信するため、装置で SNMP の設定を行ってください。SNMP の設定については、オペレーションマニュアルのセクション 11 *システム管理* “*SNMP*” を参照してください。

例

BFD に関する SNMP notification の送信を無効にします。

<Switch> system-view

[Switch] undo snmp-agent trap enable bfd

目次

このセクションのページは **10-x-x** です。

9 章 Track 9-1
9.1 Track 設定コマンド 9-1
9.1.1 delay 9-1
9.1.2 display track 9-2
9.1.3 track bfd 9-5
9.1.4 track cfd 9-6
9.1.5 track interface 9-7
9.1.6 track interface protocol 9-8
9.1.7 track nqa 9-9

9章 Track

9.1 Track設定コマンド

9.1.1 delay

Syntax

delay { **negative** *negative-time* | **positive** *positive-time* } *

undo delay

デフォルト

track モジュールは、track エントリの状態が変化すると、直ちにアプリケーションモジュールに通知します。

View

Track view

定義済みユーザロール

network-admin

パラメータ

negative *negative-time*: track エントリの状態が Negative に変化したことをアプリケーションモジュールに通知するための遅延を指定します。*negative-time* の設定範囲は、1～300 秒の負の状態通知遅延を表します。

positive *positive-time*: track エントリの状態が Positive に変化したことをアプリケーションモジュールに通知する遅延時間を指定します。*positive-time* の設定範囲は、1～300 秒の正の状態通知の遅延を表します。

説明

delay コマンドは track モジュールがアプリケーションモジュールに track エントリの状態変化を通知するまでの待ち時間を設定します。

undo delay コマンドは通知遅延設定を削除します。

Track モジュールが直ちにアプリケーションモジュールに track エントリの状態変化を通知したが、コンバージェンスが完了していない場合、通信障害が発生する可能性があります。この問題に対処するには、通知の遅延を設定して track エントリ状態の変更の即時通知を回避します。

track エントリがアプリケーションモジュールに関連付けられていない場合、通知遅延の設定は有効になりません。

このコマンドを複数回実行すると、最新の設定が有効になります。

例

ブール OR リストに関連付けられた track エントリ 101 に対して、Negative の状態通知遅延を 50 秒に設定し、Positive の状態通知遅延を 120 秒に設定します。

<Switch> system-view

[Switch] track 101 list boolean or

[Switch-track-101] delay negative 50 positive 120

9.1.2 display track

Syntax

display track { *track-entry-number* | **all** [**negative** | **positive**] } [**brief**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

track-entry-number: track エントリの ID を指定します。設定範囲は 1～1024 です。

all: すべての track エントリの情報を表示します。

negative: **negative** の状態のトラックエントリを指定します。

positive: **positive** の状態のトラックエントリを指定します。

brief: トラックエントリに関する簡単な情報を表示します。

説明

display track コマンドは track エントリの情報を表示します。

例

すべてのトラックエントリに関する情報を表示します。

<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
```

トラックエントリに関する情報を **negative** の状態で表示します。

<Switch> display track all negative brief

```
ID   Status   Type     Remote IP/URL   Local IP       Interface
1    Negative Interface --            --            Vlan2
10   Negative Interface --            --            Vlan3
```

表 9-1 コマンド出力

フィールド	説明
Track ID	trackエントリのIDです。
State	trackエントリの状態です。 ● **Positive**—正常にtrackオブジェクトが動作しています。 ● **NotReady**—trackオブジェクトが無効です。 ● **Negative**—trackオブジェクトが異常です。
Duration	trackエントリが状態を保持する時間間隔です。

フィールド	説明
Notification delay: Positive 20, Negative 30 (in seconds)	• trackモジュールは、trackエントリ状態が20秒の遅延時間後、Positiveに変更するとアプリケーションモジュールに通知します。 • trackモジュールは、trackエントリ状態が30秒の遅延時間後、Negativeに変更するとアプリケーションモジュールに通知します。
Tracked object	• trackエントリに関連づけられたtrackオブジェクトです。
NQA entry	• trackエントリに関連づけられたNQAオペレーションです。
Reaction	• trackエントリに関連づけられたリアクションエントリです。
BFD session mode	• BFDセッションモードです。エコーモードのみサポートします。
Outgoing interface	• BFDエコーモードパケットの送信インタフェースです。
VPN instance name	• BFDセッションパケットが属しているVPNインスタンス名です。ハイフン（-）のみが表示されます。これはパブリックネットワークに属しているBFDセッションパケットを示します。
Remote IP/URL	• BFDエコーパケットのリモートIPアドレスです。
Local IP	• BFDエコーパケットのローカルIPアドレスです。
Interface	• モニタされるインタフェースです。
Protocol	モニタされるインタフェースのリンク状態あるいはレイヤ3プロトコルの状態です。 • **None**—モニタされるインタフェースのリンク状態です。 • **IPv4**—モニタされるレイヤ3インタフェースのIPv4プロトコルの状態です。 • **IPv6**—モニタされるレイヤ3インタフェースのIPv6プロトコルの状態です。
IP route	エントリに関連するルート。
VPN instance name	ルートが属するVPNインスタンスの名前。 ルートがパブリックネットワークに属している場合は、2つの連続したハイフン(--)が表示されます。
Protocol	ルートのプロトコルタイプ。 ルートが存在しない場合は、[N/A] と表示されます。

フィールド	説明
Nexthop interface	ルートのネクストホップ。 ルートが存在しない場合は、[N/A] と表示されます。
LLDP interface	監視対象LLDPインタフェース。
Type	監視オブジェクトタイプ: ● BFD. ● CFD. ● Interface. ● LLDP. ● NQA. ● Route.

関連コマンド

- **track bfd**
- **track cfd**
- **track interface**
- **track interface protocol**
- **track nqa**

9.1.3 track bfd

Syntax

track *track-entry-number* **bfd echo interface** *interface-type interface-number* **remote ip** *remote-ip-address* **local ip** *local-ip-address*

undo track *track-entry-number*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

track-entry-number: track エントリの ID を指定します。設定範囲は 1～1024 です。

interface *interface-type interface-number*: BFD エコーパケットを送信するインタフェースのタイプと番号を指定します。

remote ip *remote-ip*: BFD エコーパケットの宛先 IP アドレスを指定します。

local ip *local-ip*: BFD エコーパケットの送信元 IP アドレスを指定します。

説明

track bfd コマンドは track エントリを作成し、BFD セッションに関連づけます。

undo track コマンドは track エントリを削除します。

コマンドを実行するとトラックビューになり、通知の遅延をさらに設定できます。

トラックエントリのその他の設定を変更するには、**undo track** コマンドを実行してトラックエントリを削除し、**track bfd** コマンドを再度実行します。

トラックを BFD に関連付ける場合、VRRP グループの仮想 IP アドレスを BFD セッションのローカルまたはリモートアドレスにすることはできません。

例

track エントリ 1 を作成します。リモート IP アドレス 1.1.1.1、ローカル IP アドレス 1.1.1.2 間のリンクをモニタするため、BFD を使用します。VLAN インタフェース 2 から BFD パケットを送信します。

<Switch> system-view

[Switch] track 1 bfd echo interface vlan-interface 2 remote ip 1.1.1.1 local ip 1.1.1.2

関連コマンド

display track

9.1.4 track cfd

Syntax

track *track-entry-number* **cfd cc service-instance** *instance-id* **mep** *mep-id*

undo track *track-entry-number*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

track-entry-number: track エントリの ID を指定します。設定範囲は 1～1024 です。

service-instance *instance-id*: ID でサービスインスタンスを指定します。設定範囲は:1～32767 です。

mep *mep-id*: MEP を ID で指定します。設定範囲は 1～8191 です。

説明

track cfd コマンドは track エントリを作成し、CFD と関連づけます。

undo track コマンドは track エントリを削除します。

コマンドを実行するとトラックビューになり、通知の遅延をさらに設定できます。

track エントリの他の設定を変更するには、**undo track** コマンドを実行して track エントリを削除してから、再度 **track cfd** コマンドを実行します。

例

track エントリ 1 を作成し、CFD サービスインスタンス ID を 2、MEP ID を 3 と指定します。

<Switch> system-view

[Switch] track 1 cfd cc service-instance 2 mep 3

関連コマンド

- **cfd mep**
- **cfd service-instance**
- **display track**

9.1.5 track interface

Syntax

track *track-entry-number* **interface** *interface-type interface-number*

undo track *track-entry-number*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

track-entry-number: track エントリの ID を指定します。設定範囲は 1～1024 です。

interface-type interface-number: インタフェースのタイプと番号を指定します。

説明

track interface コマンドは track エントリを作成し、指定されたインタフェースのリンク状態に関連づけます。

undo track コマンドは track エントリを削除します。

指定したインタフェースのリンク状態に関連づけたトラックエントリを作成したとき、インタフェースのリンク状態が up である場合、track エントリの状態は Positive です。インタフェースのリンク状態が down である場合、track エントリの状態は Negative です。**display ip interface brief** コマンドはインタフェースのリンク状態を表示します。

コマンドを実行するとトラックビューになり、通知の遅延をさらに設定できます。

他の設定を修正する場合、エントリを削除し、新しいエントリを作成する必要があります。

例

track エントリ 1 を作成し、VLAN インタフェース 10 のリンク状態に関連づけます。

<Switch> system-view

[Switch] track 1 interface vlan-interface 10

関連コマンド

- **display ip interface brief** (コマンドマニュアルのセクション 4 *IP サービス*)
- **display track**

9.1.6 track interface protocol

Syntax

track *track-entry-number* **interface** *interface-type interface-number* **protocol** { **ipv4** | **ipv6** }

undo track *track-entry-number*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

track-entry-number: track エントリの ID を指定します。設定範囲は 1～1024 です。

interface-type interface-number: インタフェースのタイプと番号を指定します。

ipv4: IPv4 プロトコル状態をモニタします。インタフェースの IPv4 プロトコル状態が up である場合、track エントリの状態は Positive です。インタフェースの IPv4 プロトコル状態が down である場合、track エントリの状態は Negative です。**display ip interface brief** コマンドはインタフェースの IPv4 プロトコル状態を表示します。

ipv6: IPv6 プロトコル状態をモニタします。インタフェースの IPv6 プロトコル状態が up である場合、track エントリの状態は Positive です。インタフェースの IPv6 プロトコル状態が down である場合、track エントリの状態は Negative です。**display ipv6 interface brief** コマンドはインタフェースの IPv6 プロトコル状態を表示します。

説明

track interface protocol コマンドは track エントリを作成し、インタフェースのプロトコル状態に関連づけます。

undo track コマンドは track エントリを削除します。

コマンドを実行するとトラックビューになり、通知の遅延をさらに設定できます。

トラックエントリのその他の設定を変更するには、**undo track** コマンドを実行してトラックエントリを削除し、**track interface protocol** コマンドを再度実行します。

例

track エントリ 1 を作成し、VLAN インタフェース 2 の IPv4 プロトコル状態に関連づけます。

<Switch> system-view

[Switch] track 1 interface vlan-interface 2 protocol ipv4

関連コマンド

- **display ip interface brief** (コマンドマニュアルのセクション 4 *IP サービス*)
- **display ipv6 interface brief** (コマンドマニュアルのセクション 4 *IP サービス*)
- **display track**

9.1.7 track nqa

Syntax

track *track-entry-number* **nqa entry** *admin-name operation-tag* **reaction** *item-number*

undo track *track-entry-number*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

track-entry-number: track エントリの ID を指定します。設定範囲は 1～1024 です。

entry *admin-name operation-tag*: track エントリに関連づけられる NQA オペレーションを指定します。*admin-name* は NQA オペレーションを作成する NQA オペレーションの管理者名です。設定範囲は 1～32 文字です。大文字、小文字を区別しません。*operation-tag* は NQA オペレーションのタグです。設定範囲は 1～32 文字です。大文字、小文字を区別しません。

reaction *item-number*: track エントリに関連づけられるリアクションエントリを指定します。*item-number* はリアクションエントリの ID です。設定範囲は 1～10 です。

説明

track nqa コマンドは track エントリを作成し、NQA オペレーションのリアクションエントリに関連づけます。

undo track コマンドは track エントリを削除します。

コマンドを実行するとトラックビューになり、通知の遅延をさらに設定できます。

トラックエントリのその他の設定を変更するには、**undo track** コマンドを実行してトラックエントリを削除し、**track nqa** コマンドを再度実行します。

例

track エントリ 1 を作成し、NQA テスト **admin-test** のリアクションエントリ 3 に関連づけます。

<Switch> system-view

[Switch] track 1 nqa entry admin test reaction 3

関連コマンド

display track

QX-S5100G シリーズ Ethernet スイッチ

コマンドマニュアル

11. システム管理

本マニュアルは以下に示す章で構成されています。

01-システムの保守とデバッグ

02-NQA

03-NTP

04-PoE

05-SNMP

06-RMON

07-NETCONF

08-プロセスモニタリングとメンテナンス

09-ポートミラーリング

10-トラフィックミラーリング

11-sFlow

12-Information Center

13-NetMiester

目次

このセクションのページは **11-x-x** です。

1 章 システムの保守とデバッグ 1-1
1.1 システムの保守とデバッグ設定コマンド 1-1
1.1.1 debugging 1-1
1.1.2 display debugging 1-2
1.1.3 ping 1-3
1.1.4 ping ipv6 1-6
1.1.5 tracert 1-9
1.1.6 tracert ipv6 1-11

1章 システムの保守とデバッグ

1.1 システムの保守とデバッグ設定コマンド

1.1.1 debugging

Syntax

debugging *module-name* [*option*]

undo debugging { **all** | *module-name* [*option*] }

デフォルト

無効

View

User view

定義済みユーザロール

network-admin

パラメータ

module-name: arp、device のようなモジュール名を指定します。現在のモジュール名を表示する場合、**debugging ?**コマンドを使用します。

option: モジュールのデバッグオプションを指定します。オプションの番号と内容はモジュールによって異なります。サポートされるオプションを表示する場合、**debugging** *module-name* **?**コマンドを使用します。

all: すべてのデバッグを指定します。

説明

debugging コマンドは指定したモジュールのデバッグを有効にします。

undo debugging コマンドは指定したモジュールあるいはすべてのモジュールのデバッグを無効にします。

デバッグ情報を出力すると、メモリの消費量が激しくなります。システムのパフォーマンスを保証するため、異常な状態のモジュールのみデバッグを有効にしてください。

システムは生成されたデバッグメッセージを Information Center に送信します。ログの出力設定にもとづいて適切な宛先に送信します。Information Center の詳細は、オペレーションマニュアルのセクション 11 *システム管理* “*Information Center*”を参照してください。

例

装置管理モジュールのデバッグを有効にします。

<Switch> debugging dev

関連コマンド

display debugging

1.1.2 display debugging

Syntax

display debugging [*module-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

module-name: モジュール名を指定します。現在のモジュール名を表示する場合、**debugging ?**コマンドを使用します。指定しない場合、すべてのモジュールの有効になっているデバッグを表示します。

説明

display debugging コマンドは有効になっているデバッグを表示します。

例

有効になっているすべてのデバッグを表示します。

<Switch> display debugging

```
DEV debugging switch is on
```

関連コマンド

debugging

1.1.3 ping

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*

View

すべての view

定義済みユーザロール

network-admin

パラメータ

ip: 宛先ホストの名前が **i**、**ip**、**ipv**、**ipv6**、**l**、**ls**、**lsp** であるとき、宛先ホスト名と **ping** コマンドのパラメータを区別します。たとえば、宛先ホスト名が ip である場合、**ping** *ip* の代わりに **ping ip** *ip* の形式を使用する必要があります。

-a *source-ip*: ICMP エコー要求の送信元 IP アドレスとして装置の IP アドレスを指定します。指定しない場合、ICMP エコー要求の送信元 IP アドレスは送信インタフェースのプライマリ IP アドレスです。

-c *count*: 宛先に送信する ICMP エコー要求の数を指定します。設定範囲は 1～4294967295 です。デフォルトは 5 です。

-f: IP ヘッダの DF ビットを設定します。

-h *ttl*: ICMP エコー要求の TTL を指定します。設定範囲は 1～255 です。デフォルトは 255 です。

-i *interface-type interface-number*: ICMP エコー要求の送信元インタフェースを指定します。指定しない場合、ICMP エコー要求の送信元インタフェースとしてルートの出力インタフェースに一致するプライマリ IP アドレスを使用します。

-m *interval*: ICMP エコー要求を送信する間隔を指定します。設定範囲は 1～65535 ミリ秒です。デフォルトは 200 ミリ秒です。

-n: *host* のドメイン名解決を無効にします。*host* は宛先のホスト名を示します。指定しない場合、装置はホストをアドレスに変換します。

-p *pad*: ICMP エコー要求のパディングフィールドの値を指定します。設定範囲は 16 進数、1～8 ビットで 0～ffffffff です。指定した値が 8 ビット未満の場合、上位ビットに 0 が追加され 8 ビットに拡張されます。たとえば、*pad* が 0x2f に設定されている場合、装置が要求するパケット長にするために、パケットは 0x0000002f のパディングフィールドで埋められます。パディングの値のデフォルトは 0x01 で始まり 0xff までです。必要があれば、再度繰り返します。たとえば 0x010203…feff01….です。

-q: 統計情報の概要を表示します。指定しない場合、ping のすべての統計情報を表示します。

-r: パスの ICMP エコー要求の Hop アドレス（9 まで）を記録します。指定しない場合、パスの ICMP エコー要求の Hop アドレス（9 まで）を記録しません。

-s *packet-size*: IP パケットヘッダと ICMP パケットヘッダを除く ICMP エコー要求の長さを指定します。設定範囲は 20～9600 バイトです。デフォルトは 56 バイトです。

-t *timeout*: ICMP エコー応答のタイムアウト時間を指定します。設定範囲は 0～65535 ミリ秒です。デフォルトは 2000 ミリ秒です。タイムアウト時間内に送信元が ICMP エコー応答を受信しない場合、ICMP エコー応答がタイムアウトしたと認識します。

-tos *tos*: ICMP エコー要求の ToS を指定します。設定範囲は 0～255 です。デフォルトは 0 です。

-v: ICMP 以外のエコー応答を表示します。指定しない場合、システムは ICMP 以外のエコー応答を表示しません。

-vpn-instance *vpn-instance-name*: 宛先が属する VPN インスタンスを指定します。大文字小文字を区別し、設定範囲は 1～31 文字です。宛先がパブリックネットワークの場合、このオプションは指定しません。

host: 宛先の IP アドレスあるいはホスト名を指定します。ホスト名の設定範囲は 1～253 文字です。大文字、小文字を区別しません。英字、数字、ハイフン（-）、アンダーライン（_）、ドット（.）を含むことができます。

説明

ping コマンドは IP ネットワーク内の宛先装置が到達可能かどうかを検証し、関連する統計情報を表示します。

ping コマンドで宛先ホストの名前を使用する場合、装置の DNS の設定を行う必要があります。そうでなければ **ping** コマンドは失敗します。

ping コマンドを実行中、**Ctrl+C** を押下することで中止することができます。

例

IP アドレス 1.1.2.2 の装置が到達可能かどうかを検証します。

<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
```

IP アドレス 1.1.2.2 の装置が到達可能かどうかを検証します。統計情報のみを表示します。

<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
```

IP アドレス 1.1.2.2 の装置が到達可能かどうかを検証します。パスの ICMP パケットが通過する Hop アドレスを表示します。

<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
```

出力は以下のことを示します。

- 宛先装置へ到達可能です。
- ルートは 1.1.1.1 <-> {1.1.1.2; 1.1.2.1} <-> 1.1.2.2 です。

表 1-1 コマンド出力

フィールド	説明
Ping 1.1.2.2 (1.1.2.2): 56 data bytes, press CTRL_C to break	IPアドレス1.1.2.2の装置に到達可能かどうかを検証します。各ICMPエコー要求のパケット長は56バイトです。pingを中止する場合、**Ctrl+C**を押下します。

フィールド	説明
56 bytes from 1.1.2.2: icmp_seq=0 ttl=254 time=4.685 ms	IPアドレス1.1.2.2の装置からICMPエコー応答を受信しました。タイムアウト時間内にエコー応答がない場合、表示されません。 ● **bytes**—ICMPエコー応答のバイト数です。 ● **icmp_seq**—セグメントが紛失、順番が異常、繰り返ししているかどうかを確認するために使用されるパケットシーケンスです。 ● **ttl**—ICMPエコー応答のTTLです。 ● **time**—応答時間です。
RR:	ICMPエコー要求を通過したルータです。遠いところから順番に表示されます。宛先にもっとも近いルータが最初に表示されます。
--- Ping statistics for 1.1.2.2 ---	pingで送受信した統計情報です。
5 packet(s) transmitted	送信したICMPエコー要求の数です。
5 packet(s) received	受信したICMPエコー要求の数です。
0.0% packet loss	送信したパケットに対して応答がないパケットの割合です。
round-trip min/avg/max/std-dev = 4.685/4.761/4.834/0.058 ms	最小/平均/最大/標準の応答時間です。単位はミリ秒です。

1.1.4 ping ipv6

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*

View

すべての view

定義済みユーザロール

network-admin

パラメータ

-a *source-ipv6*: ICMPv6 エコー要求の送信元 IPv6 アドレスとして装置の IPv6 アドレスを指定します。指定しない場合、ICMPv6 エコー要求の送信元 IPv6 アドレスは送信インタフェースの IPv6 アドレスです。（RFC3484 でアドレス選択ルールが定義されています）

-c *count*: 宛先に送信する ICMPv6 エコー要求の数を指定します。設定範囲は 1～4294967295 です。デフォルトは 5 です。

-i *interface-type interface-number*: ICMPv6 エコー要求の送信元インタフェースを指定します。宛先アドレスがマルチキャストアドレス、あるいはリンクローカルアドレスである場合、このパラメータを指定する必要があります。指定しない場合、ICMPv6 エコー要求の送信元インタフェースとしてルートの出力インタフェースに一致するプライマリ IP アドレスを使用します。

-m *interval*: ICMPv6 エコー応答を送信する間隔を指定します。設定範囲は 1～65535 ミリ秒です。デフォルトは 1000 ミリ秒です。

-q: 統計情報の概要を表示します。指定しない場合、ping のすべての統計情報を表示します。

-s *packet-size*: IPv6 パケットヘッダと ICMPv6 パケットヘッダを除く ICMPv6 エコー要求の長さを指定します。設定範囲は 20～9600 バイトです。デフォルトは 56 バイトです。

-t *timeout*: ICMPv6 エコー応答のタイムアウト時間を指定します。設定範囲は 0～65535 ミリ秒です。デフォルトは 2000 ミリ秒です。

-v: ICMPv6 エコー応答の詳細情報を表示します。（dst フィールドと idx フィールドを含みます）指定しない場合、システムは ICMPv6 エコー応答の概要情報のみを表示します。（dst フィールドと idx フィールドを含みません）

-vpn-instance *vpn-instance-name*: 宛先が属する VPN インスタンスを指定します。大文字小文字を区別し、設定範囲は 1～31 文字です。宛先がパブリックネットワークの場合、このオプションは指定しません。

host: 宛先の IPv6 アドレスあるいはホスト名を指定します。ホスト名の設定範囲は 1～253 文字です。大文字、小文字を区別しません。英字、数字、ハイフン（-）、アンダーライン（_）、ドット（.）を含むことができます。

説明

ping ipv6 コマンドは IPv6 ネットワーク内の宛先装置が到達可能かどうかを検証し、関連する統計情報を表示します。

ping ipv6 コマンドで宛先ホストの名前を使用する場合、装置の DNS の設定を行う必要があります。そうでなければ **ping ipv6** コマンドは失敗します。

ping ipv6 コマンドを実行中、**Ctrl+C** を押下することで中止することができます。

例

IPv6 アドレス 2001::2 の装置が到達可能かどうかを検証します。

<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
```

IPv6 アドレス 2001::2 の装置が到達可能かどうかを検証します。統計情報のみを表示します。

<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
```

IPv6 アドレス 2001::2 の装置が到達可能かどうかを検証します。詳細情報を表示します。

<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
```

表 1-2 コマンド出力

フィールド	説明
Ping6(56 data bytes) 2001::1 --> 2001::2, press CTRL_C to break	IPv6アドレス2001::1からIPv6アドレス2001::2に到達可能かどうかを検証します。 各ICMPv6エコー要求のパケット長は56バイトです。**ping ipv6**を中止する場合、**Ctrl+C**を押下します。

フィールド	説明
56 bytes from 2001::2, icmp_seq=1 hlim=64 dst=2001::1 idx=3 time=62.000 ms	IPv6アドレス2001::2からICMPv6エコー応答を受信しました。 ● データの長さは56バイトです。 ● パケットシーケンスは1です。 ● Hopリミットは64です。 ● 宛先アドレスは2001::1です。このフィールドを表示する場合、**-v**を指定する必要があります。 ● パケット受信インタフェースのインデックスは3です。このフィールドを表示する場合、**-v**を指定する必要があります。 ● 応答時間は62ミリ秒です。
--- Ping6 statistics for 2001::2 ------	ping ipv6で送受信した統計情報です。
5 packet(s) transmitted	送信したICMPv6エコー要求の数です。
5 packet(s) received	受信したICMPv6エコー要求の数です。
0.0% packet loss	送信したパケットに対して応答がないパケットの割合です。
round-trip min/avg/max/ std-dev =4.000/25.000/62.000/20.000 ms	最小/平均/最大/標準の応答時間です。単位はミリ秒です。

1.1.5 tracert

Syntax

tracert [**-a** *source-ip* | **-f** *first-ttl* | **-m** *max-ttl* | **-p** *port* | **-q** *packet-number* | **-vpn-instance** *vpn-instance-name* | **-w** *timeout*] * *host*

View

すべての view

定義済みユーザロール

network-admin

パラメータ

-a *source-ip*: プローブパケットの送信元 IP アドレスとして装置の IP アドレスを指定します。指定しない場合、プローブパケットの送信元 IP アドレスは送信インタフェースのプライマリ IP アドレスです。

-f *first-ttl*: 宛先に送信された最初のパケットの TTL を指定します。設定範囲は 1～255 です。デフォルトは 1 です。この値は *max-ttl* 以下の値でなければなりません。

-m *max-ttl*: プローブパケットで許可される最大 Hop 数を指定します。設定範囲は 1～255 です。デフォルトは 30 です。この値は *first-ttl* 以上の値でなければなりません。

-p *port*: 宛先の無効の UDP ポートを指定します。設定範囲は 1～65535 です。デフォルトは 33434 です。

-q *packet-number*: ホップごとに送信されるプローブパケット数を指定します。設定範囲は 1～65535 です。デフォルトは 3 です。

-vpn-instance *vpn-instance-name*: 宛先が属する VPN インスタンスを指定します。大文字小文字を区別し、設定範囲は 1～31 文字です。宛先がパブリックネットワークの場合、このオプションは指定しません。

-w *timeout*: プローブパケットの応答パケットのタイムアウト時間を指定します。設定範囲は 1～65535 ミリ秒です。デフォルトは 5000 ミリ秒です。

host: 宛先の IP アドレスあるいはホスト名を指定します。ホスト名の設定範囲は 1～253 文字です。大文字、小文字を区別しません。英字、数字、ハイフン（-）、アンダーライン（_）、ドット（.）を含むことができます。

説明

tracert コマンドはパケットが送信元から宛先に向かう間に通過するルートを追跡します。

ping コマンドでネットワークの故障を識別したのち、**tracert** コマンドで故障したノードの位置を見つけることができます。

tracert コマンドの出力情報には、パケットが送信元から宛先に向かう間に通過するすべてのルートの IP アドレスが含まれます。ICMP エラーメッセージで装置が応答しない場合、アスタリスク（*.*.*）が表示されます。（宛先が到達不能あるいは ICMP タイムアウト/宛先到達不能パケットの送信が無効であることを示します。）

tracert コマンドを実行中、**Ctrl+C** を押下することで中止することができます。

例

パケットが送信元から宛先（IP アドレス 1.1.2.2）へ向かうルートを表示します。

<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) 580 ms 470 ms 80 ms
```

表 1-3 コマンド出力

フィールド	説明
traceroute to 1.1.2.2(1.1.2.2)	現在の装置からIPアドレスが1.1.2.2の装置へ向かうIPパケットのルートを表示します。
hops at most	プローブパケットの最大Hop数です。このフィールドを表示する場合、**-m**を指定する必要があります。

フィールド	説明
bytes each packet	プローブパケットのバイト数です。
press CTRL_C to break	**tracert**コマンドを実行中、中止する場合、**Ctrl+C**を押下します。
2　1.1.2.2 (1.1.2.2) 580 ms 470 ms 80 ms	TTLが2のプローブパケットの結果です。2番目のホップは以下の情報が含まれます。 ● 最初のHopのドメイン名です。ドメイン名が設定されていない場合、IPアドレスが表示されます。 ● ホップのIPアドレスです。IPアドレスは括弧で表示されます。 ● プローブパケットのラウンドトリップ時間です。 各プローブが送信したパケット数を表示する場合、**-q**を指定する必要があります。

1.1.6 tracert ipv6

Syntax

tracert ipv6 [**-f** *first-hop* | **-m** *max-hops* | **-p** *port* | **-q** *packet-number* | **-vpn-instance** *vpn-instance-name* | **-w** *timeout*] * *host*

View

すべての view

定義済みユーザロール

network-admin

パラメータ

-f *first-hop*: 宛先に送信された最初のパケットの TTL を指定します。設定範囲は 1～255 です。デフォルトは 1 です。この値は *max-hops* 以下の値でなければなりません。

-m max-hops: プローブパケットで許可される最大 Hop 数を指定します。設定範囲は 1～255 です。デフォルトは 30 です。この値は *first-hop* 以上の値でなければなりません。

-p *port*: 宛先の無効の UDP ポートを指定します。設定範囲は 1～65535 です。デフォルトは 33434 です。

-q *packet-number*: ホップごとに送信されるプローブパケット数を指定します。設定範囲は 1～65535 です。デフォルトは 3 です。

-vpn-instance *vpn-instance-name*: 宛先が属する VPN インスタンスを指定します。大文字小文字を区別し、設定範囲は 1～31 文字です。宛先がパブリックネットワークの場合、このオプションは指定しません。

-w *timeout*: プローブパケットの応答パケットのタイムアウト時間を指定します。設定範囲は 1～65535 ミリ秒です。デフォルトは 5000 ミリ秒です。

host: 宛先の IPv6 アドレスあるいはホスト名を指定します。ホスト名の設定範囲は 1～253 文字です。大文字、小文字を区別しません。英字、数字、ハイフン（-）、アンダーライン（_）、ドット（.）を含むことができます。

説明

tracert ipv6 コマンドは IPv6 パケットが送信元から宛先に向かう間に通過するルートを追跡します。

ping ipv6 コマンドでネットワークの故障を識別したのち、**tracert ipv6** コマンドで故障したノードの位置を見つけることができます。

tracert ipv6 コマンドの出力情報には、パケットが送信元から宛先に向かう間に通過するすべてのレイヤ 3 の装置の IPv6 アドレスが含まれます。ICMPv6 エラーメッセージで装置が応答しない場合、アスタリスク（*.*.*）が表示されます。（宛先が到達不能あるいは ICMPv6 タイムアウト/宛先到達不能パケットの送信が無効であることを示します。）

tracert ipv6 コマンドを実行中、**Ctrl+C** を押下することで中止することができます。

例

パケットが送信元から宛先（IPv6 アドレス 2001:3::2）へ向かうルートを表示します。

<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  0.861 ms  0.718 ms  0.679 ms
 3  2001:3::2  0.822 ms  0.731 ms  0.708 ms
```

表 1-4 コマンド出力

フィールド	説明
traceroute to 2001:3::2	現在の装置からIPv6アドレスが2001:3:2の装置へ向かうIPv6パケットのルートを表示します。
hops at most	プローブパケットの最大Hop数です。このフィールドを表示する場合、**-m**を指定する必要があります。
byte packets	プローブパケットのバイト数です。
2　2001:2::2　0.861 ms　0.718 ms　0.679 ms	TTLが2のプローブパケットの結果です。2番目のホップは以下の情報が含まれます。 ● ホップのIPv6アドレスです。 ● プローブパケットのラウンドトリップ時間です。 各プローブが送信したパケット数を表示する場合、**-q**を指定する必要があります。

目次

このセクションのページは **11-x-x** です。

2 章 NQA 2-1
2.1 NQA クライアント設定コマンド 2-1
2.1.1 advantage-factor 2-1
2.1.2 codec-type 2-2
2.1.3 data-fill 2-2
2.1.4 data-size 2-4
2.1.5 description 2-5
2.1.6 destination ip 2-6
2.1.7 destination port 2-7
2.1.8 display nqa history 2-7
2.1.9 display nqa result 2-9
2.1.10 display nqa statistics 2-15
2.1.11 filename 2-22
2.1.12 frequency 2-23
2.1.13 history-record enable 2-24
2.1.14 history-record keep-time 2-25
2.1.15 history-record number 2-26
2.1.16 next-hop ip 2-26
2.1.17 nqa 2-27
2.1.18 nqa agent enable 2-28
2.1.19 nqa schedule 2-29
2.1.20 operation (FTP operation view) 2-30
2.1.21 operation (HTTP/HTTPS operation view) 2-31
2.1.22 operation (HTTP operation view) 2-33
2.1.23 password 2-34
2.1.24 probe count 2-35
2.1.25 probe packet-interval 2-36
2.1.26 probe packet-number 2-37
2.1.27 probe packet-timeout 2-37
2.1.28 probe timeout 2-38
2.1.29 reaction checked-element probe-fail (for trap) 2-39
2.1.30 reaction checked-element probe-fail (for trigger) 2-41
2.1.31 reaction trap 2-42
2.1.32 resolve-target 2-43
2.1.33 route-option bypass-route 2-44
2.1.34 source interface (ICMP echo operation view) 2-45

2.1.35 source ip 2-46
2.1.36 source port 2-47
2.1.37 statistics hold-time 2-47
2.1.38 statistics interval 2-48
2.1.39 statistics max-group 2-49
2.1.40 tos 2-50
2.1.41 ttl 2-51
2.1.42 type 2-52
2.1.43 url 2-53
2.1.44 username 2-54
2.1.45 version 2-55
2.1.46 vpn-instance 2-56
2.2 NQA サーバ設定コマンド 2-57
2.2.1 display nqa server 2-57
2.2.2 nqa server enable 2-58
2.2.3 nqa server tcp-connect 2-59
2.2.4 nqa server udp-echo 2-60

2章 NQA

2.1 NQAクライアント設定コマンド

2.1.1 advantage-factor

Syntax

advantage-factor *factor*

undo advantage-factor

デフォルト

0

View

Voice operation view

定義済みユーザロール

network-admin

パラメータ

factor: アドバンテージファクタを指定します。設定範囲は 0～20 です。

説明

advantage-factor コマンドは MOS（Mean Opinion Scores）値と ICPIF（Calculated Planning Impairment Factor）値をカウントするのに使用されるアドバンテージファクタを設定します。

undo advantage-factor コマンドはデフォルトに戻します。

音声品質の評価は、ユーザの音声品質の許容度に依存します。音声品質に高い許容度を持つユーザの場合、アドバンテージファクタの設定を行う **advantage-factor** コマンドを使用します。システムが ICPIF 値を計算する場合、音声品質の評価用に ICPIF と MOS の値を修正するため、アドバンテージファクタが取りはずされます。

例

音声テストのアドバンテージファクタを 10 に設定します。

<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

Syntax

codec-type { **g711a** | **g711u** | **g729a** }

undo codec-type

デフォルト

G.711 A-law

View

Voice operation view

定義済みユーザロール

network-admin

パラメータ

g711a: G.711 A-law コーデックタイプを指定します。

g711u: G.711 μ-law コーデックタイプを指定します。

g729a: G.729 A-law コーデックタイプを指定します。

説明

codec-type コマンドは音声テストのコーデックタイプを設定します。

undo codec-type コマンドはデフォルトに戻します。

例

音声テストのコーデックタイプを g729a に設定します。

<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

Syntax

data-fill *string*

undo data-fill

デフォルト

00010203040506070809

View

ICMP/UDP echo operation view

UDP jitter/voice operation view

定義済みユーザロール

network-admin

パラメータ

string: 文字列を指定します。設定範囲は 1～200 文字です。大文字、小文字を区別します。

説明

data-fill コマンドは各プローブパケットのペイロードに埋め込まれる文字列を設定します。

undo data-fill コマンドはデフォルトに戻します。

ペイロード長が埋め込みデータより小さい場合、文字列の最初の部分を使用します。たとえば、埋め込みデータが **abcd** で、テストパケットのデータサイズが 3 バイトの場合、**abc** がパケットに埋め込まれます。

ペイロード長が埋め込みデータより大きい場合、一杯になるまで文字列を繰り返し埋め込みます。たとえば、埋め込みデータが **abcd** で、テストパケットのデータサイズが 6 バイトの場合、**abcdab** がパケットに埋め込まれます。

テストタイプに依存して文字列が埋め込まれます。

- ICMP エコーテストでは、設定された文字列は ICMP エコー要求の全ペイロードに埋め込まれます。
- UDP エコーテストでは、UDP パケットのペイロードの最初の 5 バイトは特定の用途に使用されます。設定された文字列はペイロードの残りの部分を埋め込むのに使用されます。
- UDP ジッタテストでは、UDP パケットのペイロードの最初の 68 バイトは特定の用途に使用されます。設定された文字列はペイロードの残りの部分を埋め込むのに使用されます。
- 音声テストでは、UDP パケットのペイロードの最初の 16 バイトは特定の用途に使用されます。設定された文字列はペイロードの残りの部分を埋め込むのに使用されます。

例

ICMP エコー要求のペイロードに埋め込まれる文字列 **abcd** を設定します。

<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

Syntax

data-size *size*

undo data-size

デフォルト

異なるテストのプローブパケットのデフォルトのペイロードサイズを表 2-1 に示します。

表 2-1 プローブパケットのデフォルトのペイロードサイズ

テストタイプ	コーデックタイプ	デフォルトサイズ（バイト）
ICMP echo	—	100
UDP echo	—	100
UDP jitter	—	100
Voice	G.711 A-law	172
Voice	G.711 μ-law	172
Voice	G.729 A-law	32

View

ICMP/UDP echo operation view

UDP jitter/voice operation view

定義済みユーザロール

network-admin

パラメータ

size: 各プローブパケットのペイロードサイズを指定します。以下に設定範囲を示します。

- ICMP エコーあるいは UDP エコーテストのプローブパケットの設定範囲は 20～65507 バイトです。
- UDP ジッタテストのプローブパケットの設定範囲は 68～65507 バイトです。
- 音声テストのプローブパケットの設定範囲は 16～65507 バイトです。

説明

data-size コマンドは ICMP エコーテストの各 ICMP エコー要求のペイロードサイズ、あるいは UDP エコー、UDP ジッタ、音声テストのペイロードサイズを設定します。

undo data-size コマンドはデフォルトに戻します。

ICMP エコーテストではコマンドは各エコー要求のペイロードサイズを設定します。

UDP エコーテスト、UDP ジッタ、音声テストではコマンドは各エコーUDP パケットのペイロードサイズを設定します。

例

各 ICMP エコー要求のペイロードサイズを 80 バイトに設定します。

<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

Syntax

description *text*

undo description

デフォルト

設定なし

View

すべての NQA operation view

定義済みユーザロール

network-admin

パラメータ

text: 文字列を指定します。設定範囲は 1～200 文字です。大文字、小文字を区別します。

説明

description コマンドはテストタイプや目的などの NQA テストの説明を設定します。

undo description コマンドは説明を削除します。

例

NQA テストの説明を **icmp-probe** に設定します。

<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

Syntax

destination ip *ip-address*

undo destination ip

デフォルト

設定なし

View

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

UDP jitter/voice operation view

定義済みユーザロール

network-admin

パラメータ

ip-address: テストの宛先 IPv4 アドレスを指定します。

説明

destination ip コマンドはテストの宛先 IPv4 アドレスを設定します。

undo destination ip コマンドは宛先 IPv4 アドレスを削除します。

例

ICMP エコーテストの宛先 IPv4 アドレスを 10.1.1.1 に設定します。

<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

Syntax

destination port *port-number*

undo destination port

デフォルト

設定なし

View

TCP/UDP echo operation view

UDP jitter/voice operation view

定義済みユーザロール

network-admin

パラメータ

port-number: テストの宛先ポート番号を指定します。設定範囲は 1～65535 です。

説明

destination port コマンドはテストの宛先ポート番号を設定します。

undo destination port コマンドは宛先ポート番号を削除します。

例

UDP エコーテストの宛先ポート番号を 9000 に設定します。

<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

Syntax

display nqa history [*admin-name operation-tag*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

admin-name operation-tag: 管理者名とテストタグで NQA テストを指定します。*admin-name* は NQA テストを作成する管理者の名前を示します。*operation-tag* はテストタグを示します。*admin-name*、*operation-tag* の設定範囲は 1～32 文字です。大文字、小文字を区別しません。ハイフン（-）を使用することができません。NQA テストを指定しない場合、すべての NQA テストの履歴記録を表示します。

説明

display nqa history コマンドは NQA テストの履歴記録を表示します。

display nqa history コマンドは UDP ジッタテストと音声テストの結果あるいは統計情報を表示しません。UDP ジッタテストと音声テストを確認する場合、**display nqa result** コマンドあるいは **display nqa statistics** コマンドを使用します。

例

管理者名が **administrator**、オペレーティングタグが **test** の NQA テストグループの履歴記録を表示します。

<Switch> display nqa history administrator tracert

```
NQA entry (admin administrator, tag tracert) history records:
Index      TTL  Response  Hop IP         Status         Time
1          2    328       4.1.1.1        Succeeded      2013-09-09 14:46:06.2
1          2    328       4.1.1.1        Succeeded      2013-09-09 14:46:05.2
1          2    328       4.1.1.1        Succeeded      2013-09-09 14:46:04.2
1          1    328       3.1.1.2        Succeeded      2013-09-09 14:46:03.2
1          1    328       3.1.1.1        Succeeded      2013-09-09 14:46:02.2
1          1    328       3.1.1.1        Succeeded      2013-09-09 14:46:01.2
```

表 2-2 コマンド出力

フィールド	説明
Index	履歴記録のIDです。
TTL	プローブパケットのTTLです。
Response	テストが成功した場合、ラウンドトリップの時間を表示します。テストがタイムアウトしたとき、タイムアウト時間を表示します。テストが完了しない場合、0を表示します。単位はミリ秒です。

フィールド	説明
Status	テスト結果の状態です。 ● **Succeeded**－成功しました。 ● **Unknown error**－未知のエラーです。 ● **Internal error**－内部エラーです。 ● **Timeout**－タイムアウトしました。
Time	テストが完了したときの時間です。

2.1.9 display nqa result

Syntax

display nqa result [*admin-name operation-tag*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

admin-name operation-tag: 管理者名とテストタグで NQA テストを指定します。*admin-name* は NQA テストを作成する管理者の名前を示します。*operation-tag* はテストタグを示します。*admin-name*、*operation-tag* の設定範囲は 1～32 文字です。大文字、小文字を区別しません。ハイフン（-）を使用することができません。NQA テストを指定しない場合、すべての NQA テストの最新の結果を表示します。

説明

display nqa result コマンドは、NQA テストの最新の結果を表示します。

例

管理者名 admin、テストタグ test の TCP テストの最新の結果を表示します。

<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
```

管理者名 admin、テストタグ test の UDP ジッタテストの最新の結果を表示します。

<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
```

管理者名 admin、テストタグ test の音声テストの最新の結果を表示します。

<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
```

表 2-3 コマンド出力

フィールド	説明
Data collecting in progress	テストの進捗状況です。
Send operation times	テスト数です。
Receive response times	受信した応答パケットの数です。
Min/Max/Average round trip time	最小/最大/平均ラウンドトリップタイムです。単位はミリ秒です。
Square-Sum of round trip time	ラウンドトリップタイムの2乗和です。
Last succeeded probe time	連続した最後のプローブが完了した時間です。テストでプローブが連続していない場合、0と表示されます。 このフィールドはUDPジッタ、音声テストで無効です。
Last packet received time	連続した最後の応答パケットを受信した時間です。プローブで応答パケットを受信しない場合、0と表示されます。 このフィールドはUDPジッタ、音声テストで有効です。
Packet loss ratio	平均パケット損失レートです。
Failures due to timeout	テストでタイムアウトが発生した回数です。
Failures due to disconnect	ピアが切断した数です。
Failures due to no connection	ピアとの接続に失敗した数です。
Failures due to internal error	内部エラーによる故障の数です。
Failures due to other errors	他のエラーによる故障の数です。
Packets out of sequence	異なる順番のパケットによる故障の数です。
ICMP-jitter results	ICMPジッタテスト結果です。 このフィールドはUDPジッタのみ有効です。
Packets arrived late	プローブがタイムアウトしたのち応答パケットを受信した数です。
UDP-jitter results	UDPジッタテストの結果です。 このフィールドはUDPジッタテストのみ有効です。
Voice results	音声テストの結果です。 このフィールドは音声テストのみ有効です。
RTT number	応答パケットを受信した数です。
Min positive SD	送信元から宛先への最小ポジティブジッタです。
Min positive DS	宛先から送信元への最小ポジティブジッタです。

フィールド	説明
Max positive SD	送信元から宛先への最大ポジティブジッタです。
Max positive DS	宛先から送信元への最大ポジティブジッタです。
Positive SD number	送信元から宛先へのポジティブジッタの数です。
Positive DS number	宛先から送信元へのポジティブジッタの数です。
Positive SD sum	送信元から宛先へのポジティブジッタの合計数です。
Positive DS sum	宛先から送信元へのポジティブジッタの合計数です。
Positive SD average	送信元から宛先への平均ポジティブジッタです。
Positive DS average	宛先から送信元への平均ポジティブジッタです。
Positive SD square-sum	送信元から宛先へのポジティブジッタの2乗和です。
Positive DS square-sum	宛先から送信元へのポジティブジッタの2乗和です。
Min negative SD	送信元から宛先へのネガティブジッタの絶対値の最小値です。
Min negative DS	宛先から送信元へのネガティブジッタの絶対値の最小値です。
Max negative SD	送信元から宛先へのネガティブジッタの絶対値の最大値です。
Max negative DS	宛先から送信元へのネガティブジッタの絶対値の最大値です。
Negative SD number	送信元から宛先へのネガティブジッタの数です。
Negative DS number	宛先から送信元へのネガティブジッタの数です。
Negative SD sum	送信元から宛先へのネガティブジッタの絶対値の合計です。
Negative DS sum	宛先から送信元へのネガティブジッタの絶対値の合計です。
Negative SD average	送信元から宛先へのネガティブジッタの絶対値の平均です。
Negative DS average	宛先から送信元へのネガティブジッタの絶対値の平均です。
Negative SD square-sum	送信元から宛先へのネガティブジッタの2乗和です。
Negative DS square-sum	宛先から送信元へのネガティブジッタの2乗和です。

フィールド	説明
One way results	片方向遅延です。 このフィールドはUDPジッタテスト、音声テストで有効です。
Max SD delay	送信元から宛先への最大遅延です。
Max DS delay	宛先から送信元への最大遅延です。
Min SD delay	送信元から宛先への最小遅延です。
Min DS delay	宛先から送信元への最小遅延です。
Number of SD delay	送信元から宛先への遅延の数です。
Number of DS delay	宛先から送信元への遅延の数です。
Sum of SD delay	送信元から宛先への遅延の合計です。
Sum of DS delay	宛先から送信元への遅延の合計です。
Square-Sum of SD delay	送信元から宛先への遅延の2乗和です。
Square-Sum of DS delay	宛先から送信元への遅延の2乗和です。
SD lost packets	送信元から宛先への損失したパケット数です。
DS lost packets	宛先から送信元への損失したパケット数です。
Lost packets for unknown reason	不明な理由で損失したパケット数です。
Voice scores	音声パラメータです。 このフィールドは音声テストで有効です。
MOS value	音声テストの計算されたMOS値です。
ICPIF value	音声テストの計算されたICPIF値です。
TTL	受信した応答パケットのTTLです。
Hop IP	送信した応答パケットのノードのIPアドレスです。
Time	NQAクライアントが応答パケットを受信した時間です。

2.1.10 display nqa statistics

Syntax

display nqa statistics [*admin-name operation-tag*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

admin-name operation-tag: 管理者名とテストタグで NQA テストを指定します。*admin-name* は NQA テストを作成する管理者の名前を示します。*operation-tag* はテストタグを示します。*admin-name*、*operation-tag* の設定範囲は 1～32 文字です。大文字、小文字を区別しません。ハイフン（-）を使用することができません。NQA テストを指定しない場合、すべての NQA テストの統計情報を表示します。

説明

display nqa statistics コマンドは NQA テストの統計情報を表示します。

NQA テストが完了した後、統計情報が作成されます。テストが完了する前に **display nqa statistics** コマンドを実行した場合、統計情報はすべて 0 で表示されます。

リアクションエントリが設定されている場合、**statistics interval** コマンドで指定された期間、リアクションエントリをモニタリングした結果を表示します。以下の場合、ハイフン（-）が結果として表示されます。

- しきい値タイプが平均値
- 音声テストのモニタリングが ICPIF あるいは MOS

例

管理者名 admin、テストタグ test の TCP テストの統計情報を表示します。

<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
```

管理者名 admin、テストタグ test の UDP ジッタテストの統計情報を表示します。

<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
```

管理者名 admin、テストタグ test の音声テストの統計情報を表示します。

<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              -               -            -
```

表 2-4 コマンド出力

フィールド	説明
No.	統計情報のグループIDです。
Start time	テストが開始した時間です。
Life time	テストの所要時間です。
Send operation times	送信したプローブパケットの数です。
Receive response times	受信した応答パケットの数です。
Min/Max/Average round trip time	最小/最大/平均ラウンドトリップタイムです。単位はミリ秒です。
Square-Sum of round trip time	ラウンドトリップタイムの2乗和です。
Packet loss ratio	平均パケット損失レートです。
Failures due to timeout	テストでタイムアウトが発生した回数です。
Failures due to disconnect	ピアが切断した数です。
Failures due to no connection	ピアとの接続に失敗した数です。
Failures due to internal error	内部エラーによる故障の数です。
Failures due to other errors	他のエラーによる故障の数です。
Packets out of sequence	異なる順番のパケットによる故障の数です。
Packets arrived late	プローブがタイムアウトしたのち応答パケットを受信した数です。

フィールド	説明
UDP-jitter results	UDPジッタテストの結果です。このフィールドはUDPジッタテストのみ有効です。
Voice results	音声テストの結果です。このフィールドは音声テストのみ有効です。
RTT number	応答パケットを受信した数です。
Min positive SD	送信元から宛先への最小ポジティブジッタです。
Min positive DS	宛先から送信元への最小ポジティブジッタです。
Max positive SD	送信元から宛先への最大ポジティブジッタです。
Max positive DS	宛先から送信元への最大ポジティブジッタです。
Positive SD number	送信元から宛先へのポジティブジッタの数です。
Positive DS number	宛先から送信元へのポジティブジッタの数です。
Positive SD sum	送信元から宛先へのポジティブジッタの合計数です。
Positive DS sum	宛先から送信元へのポジティブジッタの合計数です。
Positive SD average	送信元から宛先への平均ポジティブジッタです。
Positive DS average	宛先から送信元への平均ポジティブジッタです。
Positive SD square-sum	送信元から宛先へのポジティブジッタの2乗和です。
Positive DS square-sum	宛先から送信元へのポジティブジッタの2乗和です。
Min negative SD	送信元から宛先へのネガティブジッタの絶対値の最小値です。
Min negative DS	宛先から送信元へのネガティブジッタの絶対値の最小値です。
Max negative SD	送信元から宛先へのネガティブジッタの絶対値の最大値です。
Max negative DS	宛先から送信元へのネガティブジッタの絶対値の最大値です。
Negative SD number	送信元から宛先へのネガティブジッタの数です。
Negative DS number	宛先から送信元へのネガティブジッタの数です。
Negative SD sum	送信元から宛先へのネガティブジッタの絶対値の合計です。

フィールド	説明
Negative DS sum	宛先から送信元へのネガティブジッタの絶対値の合計です。
Negative SD average	送信元から宛先へのネガティブジッタの絶対値の平均です。
Negative DS average	宛先から送信元へのネガティブジッタの絶対値の平均です。
Negative SD square-sum	送信元から宛先へのネガティブジッタの2乗和です。
Negative DS square-sum	宛先から送信元へのネガティブジッタの2乗和です。
One way results	片方向遅延です。 このフィールドはUDPジッタテスト、音声テストで有効です。
Max SD delay	送信元から宛先への最大遅延です。
Max DS delay	宛先から送信元への最大遅延です。
Min SD delay	送信元から宛先への最小遅延です。
Min DS delay	宛先から送信元への最小遅延です。
Number of SD delay	送信元から宛先への遅延の数です。
Number of DS delay	宛先から送信元への遅延の数です。
Sum of SD delay	送信元から宛先への遅延の合計です。
Sum of DS delay	宛先から送信元への遅延の合計です。
Square-Sum of SD delay	送信元から宛先への遅延の2乗和です。
Square-Sum of DS delay	宛先から送信元への遅延の2乗和です。
SD lost packets	送信元から宛先への損失したパケット数です。
DS lost packets	宛先から送信元への損失したパケット数です。
Lost packets for unknown reason	不明な理由で損失したパケット数です。
Voice scores	音声パラメータです。 このフィールドは音声テストで有効です。
Max MOS value	最大MOS値です。
Min MOS value	最小MOS値です。

フィールド	説明
Max ICPIF value	最大ICPIF値です。
Min ICPIF value	最小ICPIF値です。
Reaction statistics	カウント期間中のリアクションエントリに関する統計情報です。
Index	リアクションエントリのIDです。
Checked Element	モニタリングされる要素です。
Threshold Type	しきい値タイプです。
Checked Num	データ収集用にモニタリングされているターゲット数です。
Over-threshold Num	しきい値違反の数です。

表 2-5 に DHCP/DLSw/DNS/FTP/HTTP/SNMP/TCP/UDP エコーテストのしきい値モニタリングフィールドの説明を示します。

表 2-5 DHCP/DLSw/DNS/FTP/HTTP/SNMP/TCP/UDP エコーテストのしきい値モニタリングフィールドの説明

モニタリングされる性能メトリック	しきい値タイプ	収集データ	モニタリングされているターゲット数	しきい値違反数
probe-duration	accumulate	カウント期間のプローブ	完了したプローブ数	カウント期間中にしきい値を超過したプローブ数
	average	–	–	–
	consecutive	カウント期間のプローブ	完了したプローブ数	カウント期間中にしきい値を超過したプローブ数
probe-fail	accumulate	カウント期間のプローブ	完了したプローブ数	プローブ失敗数
	consecutive	カウント期間のプローブ	完了したプローブ数	プローブ失敗数

表 2-5 に UDP ジッタ/音声テストのしきい値モニタリングフィールドの説明を示します。

表 2-6 UDP ジッタ/音声テストのしきい値モニタリングフィールドの説明

モニタリングされる性能メトリック	しきい値タイプ	収集データ	モニタリングされているターゲット数	しきい値違反数
RTT	accumulate	カウント期間のプローブ	送信したパケット数	ラウンドトリップ中にしきい値を超過したパケット数
	average	–	–	–
jitter-DS/jitter-SD	accumulate	カウント期間のプローブ	送信したパケット数	1方向ジッタ時間中にしきい値を超過したパケット数
	average	–	–	–
OWD-DS/OWD-SD	–	カウント期間のプローブ	送信したパケット数	1方向ジッタ時間中にしきい値を超過したパケット数
packet-loss	accumulate	カウント期間のプローブ	送信したパケット数	パケット損失数
ICPIF/MOS（音声テストのみ有効）	–	–	–	–

関連コマンド

statistics interval

2.1.11 filename

Syntax

filename *filename*

undo filename

デフォルト

設定なし

View

FTP operation view

定義済みユーザロール

network-admin

パラメータ

filename: FTP サーバと FTP クライアント間で転送するファイル名を指定します。設定範囲は 1～200 文字です。大文字、小文字を区別します。スラッシュ（/）は含むことができません。

説明

filename コマンドは FTP サーバと FTP クライアント間で転送するファイル名を指定します。

undo filename コマンドはデフォルトに戻します。

例

FTP サーバと FTP クライアント間で転送するファイル名を **config.txt** に設定します。

<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

Syntax

frequency *interval*

undo frequency

デフォルト

2 つの連続する音声テスト間隔は 60000 ミリ秒です。他のテストの 2 つの連続するテスト間隔は 0 ミリ秒です。1 回のテストのみが実行されます。

View

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

UDP jitter/voice operation view

定義済みユーザロール

network-admin

パラメータ

interval: 2 つの連続するテスト間隔を指定します。設定範囲は 0～604800000 ミリ秒です。0 を指定した場合、テストは 1 回だけ実行され、統計情報は作成しません。

説明

frequency コマンドは NQA テストを繰り返す間隔を設定します。

undo frequency コマンドはデフォルトに戻します。

テスト間隔になってもテストが完了しないとき、次のテストが開始します。

例

ICMP エコーテストを繰り返す間隔を 1000 ミリ秒に設定します。

<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

Syntax

history-record enable

undo history-record enable

デフォルト

無効

View

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

定義済みユーザロール

network-admin

説明

history-record enable コマンドは NQA テストの履歴記録を保存することを有効にします。

undo history-record enable コマンドは NQA テストの履歴記録を保存することを無効にします。

NQA テストの履歴記録を表示する場合、**display nqa history** コマンドを使用します。

undo history-record enable コマンドは NQA テストの既存の履歴記録も削除します。

例

NQA テストの履歴記録を保存することを有効にします。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type icmp-echo

[Switch-nqa-admin-test-icmp-echo] history-record enable

関連コマンド

display nqa history

2.1.14 history-record keep-time

Syntax

history-record keep-time *keep-time*

undo history-record keep-time

デフォルト

120 分

View

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

定義済みユーザロール

network-admin

パラメータ

keep-time: 履歴記録を保存する期間を指定します。設定範囲は 1～1440 分です。

説明

history-record keep-time コマンドは NQA テストの履歴記録の有効期限を指定します。

undo history-record keep-time コマンドはデフォルトに戻します。

NQA テストが完了したとき、タイマが開始します。すべての記録は有効期限になったとき、削除されます。

例

ICMP エコーテストの履歴記録の有効期限を 100 分に設定します。

<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

Syntax

history-record number *number*

undo history-record number

デフォルト

50

View

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

定義済みユーザロール

network-admin

パラメータ

number: NQA テストで履歴記録を保存できる最大数を指定します。設定範囲は 0～50 です。

説明

history-record number コマンドは NQA テストで履歴記録を保存できる最大数を設定します。

undo history-record number コマンドはデフォルトに戻します。

NQA テストの履歴記録の数が最大数を超過した場合、もっとも古い履歴記録が削除されます。

例

ICMP エコーテストで履歴記録を保存できる最大数を 10 に設定します。

<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

Syntax

next-hop ip *ip-address*

undo next-hop ip

デフォルト

設定なし

View

ICMP echo operation view

定義済みユーザロール

network-admin

パラメータ

ip-address: ネクストホップの IP アドレスを指定します。

説明

next-hop ip コマンドは ICMP エコーテストのネクストホップの IP アドレスを設定します。

undo next-hop ip コマンドはネクストホップの IP アドレスを削除します。

ネクストホップの IP アドレスが設定されていない場合、装置は ICMP エコーパケットのネクストホップの IP アドレスを決定するためルーティングテーブルを検索します。

例

ICMP エコーテストのネクストホップの IP アドレスを 10.1.1.1 に設定します。

<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

Syntax

nqa entry *admin-name operation-tag*

undo nqa { **all** | **entry** *admin-name operation-tag* }

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

admin-name operation-tag: 管理者名とテストタグで NQA テストを指定します。*admin-name* は NQA テストを作成する管理者の名前を示します。*operation-tag* はオペレーションタグを示します。*admin-name*、*operation-tag* の設定範囲は 1～32 文字です。大文字、小文字を区別しません。ハイフン（-）を使用することができません。

all: すべての NQA テストを削除します。

説明

nqa コマンドは NQA テストを作成し、その view に移行します。NQA テストがすでに存在する場合、その view に移行します。

undo nqa コマンドはテストを削除します。

例

管理者 **admin** とテストタグ **test** の NQA テストを作成し、NQA operation view に移行します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test]

2.1.18 nqa agent enable

Syntax

nqa agent enable

undo nqa agent enable

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

nqa agent enable コマンドは NQA クライアントを有効にします。

undo nqa agent enable コマンドは NQA クライアントを無効にし、すべてのテストを停止します。

例

NQA クライアントを有効にします。

<Switch> system-view

[Switch] nqa agent enable

関連コマンド

nqa server enable

2.1.19 nqa schedule

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*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

admin-name operation-tag: 管理者名とテストタグで NQA テストを指定します。*admin-name* は NQA テストを作成する管理者の名前を示します。*operation-tag* はオペレーションタグを示します。*admin-name*、*operation-tag* の設定範囲は 1～32 文字です。大文字、小文字を区別しません。ハイフン（-）を使用することができません。

start-time: NQA テストの開始日時を指定します。

hh:mm:ss: NQA テストの開始時間を指定します。

yyyy/mm/dd: NQA テストの開始日を指定します。デフォルトは現在のシステム時間です。yyy の設定範囲は 2000～2035 です。

mm/dd/yyyy: NQA テストの開始日を指定します。デフォルトは現在のシステム時間です。yyy の設定範囲は 2000～2035 です。

now: すぐにテストを開始します。

lifetime: テストの有効期限を指定します。

lifetime: 動作期間を指定します。設定範囲は 1～2147483647 秒です。

forever: **undo nqa schedule** コマンドを使用して手動で停止するまでテストを実行します。

recurring: 開始時間に自動でテストを開始し、指定した期間、実行し続けます。指定しない場合、指定した期間で 1 回のみ実行します。

説明

nqa schedule コマンドは NQA テストのスケジューリングのパラメータを設定します。

undo nqa schedule コマンドはテストを停止します。

NQA テストは開始日時と終了日時（開始日時＋動作期間）で動作します。開始日時がシステム時間より前である場合、テストはすぐさま開始します。開始日時と終了日時の両方がシステム時間より前である場合、テストは開始しません。現在のシステム時間を表示する場合、**display clock** コマンドを使用します。

スケジュールされた NQA テストの operation view あるいは operation type view に移行することはできません。

例

管理者 **admin** とテストタグ **test** の NQA テストをスケジューリングします。2008 年 8 月 8 日の 08 時 08 分 08 秒に開始し、1000 秒間テストを行うように設定します。

<Switch> system-view

[Switch] nqa schedule admin test start-time 08:08:08 2008/08/08 lifetime 1000 recurring

関連コマンド

- **destination ip**
- **display clock**（オペレーションマニュアルのセクション 1 *はじめに* “*装置管理*”）
- **nqa entry**
- **type**

2.1.20 operation (FTP operation view)

Syntax

operation { **get** | **put** }

undo operation

デフォルト

get

View

FTP operation view

定義済みユーザロール

network-admin

パラメータ

get: FTP サーバからファイルを取得します。

put: FTP サーバにファイルを転送します。

説明

operation コマンドは FTP テストのオペレーションタイプを指定します。

undo operation コマンドはデフォルトに戻します。

filename コマンドで **put** オペレーションを実行するとき、NQA クライアント上にファイルが存在していることを確認してください。

FTP サーバからファイルを取得する場合、FTP サーバの URL に指定されたファイルが存在していることを確認してください。NQA クライアントは FTP サーバから取得したファイルを保存しません。

FTP テストではファイルサイズが小さいファイルを使用してください。大きいサイズのファイルは、タイムアウトでテストが失敗したり、ネットワークの帯域幅以上を独占して他のサービスに影響を与えたりする可能性があります。

例

FTP テストのオペレーションタイプを **put** に指定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type ftp

[Switch-nqa-admin-test-ftp] operation put

関連コマンド

- **password**
- **username**

2.1.21 operation (HTTP/HTTPS operation view)

Syntax

operation { **get** | **post** | **raw** }

undo operation

デフォルト

get

View

HTTP operation view

HTTP/HTTPS template view

定義済みユーザロール

network-admin

パラメータ

get: HTTP サーバあるいは HTTPS サーバからファイルを取得します。

post: HTTP サーバあるいは HTTPS サーバにファイルを転送します。

raw: RAW 要求を HTTP あるいは HTTPS サーバに送信します。

説明

operation コマンドは HTTP テストのオペレーションタイプを指定します。

undo operation コマンドはデフォルトに戻します。

HTTP あるいは HTTPS テストでは、HTTP あるいは HTTPS 要求をプローブパケットとして使用します。

HTTP の **get** あるいは **post** オペレーションの HTTP 要求の内容は **url** コマンドによって指定された URL から取得されます。

raw テストの場合、要求の内容は raw 要求ビューで設定されます。**raw-request** コマンドを使用すると、raw 要求ビューに移行します。

例

HTTP テストのオペレーションのタイプを **raw** に指定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type http

[Switch-nqa-admin-test-http] operation raw

HTTP テンプレート view で、HTTP テストのオペレーションのタイプを **raw** に設定します。

<Switch> system-view

[Switch] nqa template http httptplt

[Switch-nqatplt-http-httptplt] operation raw

関連コマンド

- **password**

- **username**

2.1.22 operation (HTTP operation view)

Syntax

operation { **get** | **post** }

undo operation

デフォルト

get

View

HTTP operation view

定義済みユーザロール

network-admin

パラメータ

get: HTTP サーバからファイルを取得します。

post: HTTP サーバにファイルを転送します。

説明

operation コマンドは HTTP テストのオペレーションタイプを指定します。

undo operation コマンドはデフォルトに戻します。

HTTP テストはプローブパケットとして HTTP 要求を使用します。

HTTP の **get** あるいは **post** オペレーションの HTTP 要求の内容は **url** コマンドによって指定された URL から取得されます。

例

HTTP テストのオペレーションのタイプを **post** に指定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type http

[Switch-nqa-admin-test-http] operation post

関連コマンド

- **password**
- **username**

2.1.23 password

Syntax

password { **cipher** | **simple** } *string*

undo password

デフォルト

設定なし

View

FTP/HTTP operation view

定義済みユーザロール

network-admin

パラメータ

cipher: 暗号パスワードを指定します。

simple: プレーンパスワードを指定します。セキュリティのため、プレーンテキストで設定されたパスワードを含めたすべてのパスワードは暗号テキストで保存されます。

string: パスワードを指定します。大文字、小文字を区別します。**simple** を指定した場合の設定範囲は 1～32 文字です。**cipher** を指定した場合の設定範囲は 1～73 文字です。

説明

password コマンドは FTP あるいは HTTP ログインパスワードを設定します。

undo password コマンドは設定を削除します。

例

FTP ログインパスワードを **ftpuser** に設定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type ftp

[Switch-nqa-admin-test-ftp] password simple ftpuser

関連コマンド

- **operation**
- **username**

2.1.24 probe count

Syntax

probe count *times*

undo probe count

デフォルト

1

View

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

UDP jitter operation view

定義済みユーザロール

network-admin

パラメータ

times: NQA テスト（プローブ）の検査回数を指定します。設定範囲は 1～15 です。

説明

probe count コマンドは NQA テストの検査回数を設定します。

undo probe count コマンドはデフォルトに戻します。

以下に異なるタイプのテストを実行する方法を示します。

- TCP あるいは DLSw テストは接続を設定します。
- UDP ジッタテストは多くのプローブパケットを送信します。多くのプローブパケットは **probe packet-number** コマンドによって設定されます。
- FTP テストはファイルをアップロードあるいはダウンロードします。
- HTTP テストは Web ページを取得します。
- DHCP テストは DHCP を介して IP アドレスを取得します。
- DNS テストはドメイン名を IP アドレスに変換します。
- ICMP エコーテストは ICMP エコー要求を送信します。
- UDP エコーテストは UDP パケットを送信します。
- SNMP テストは 1 つの SNMPv1 パケット、1 つの SNMPv2c パケット、1 つの SNMPv3 パケットを送信します。
- フレーム損失、遅延、スループットテストはネットワークのフレーム損失率、遅延、スループットをテストするため宛先にテストフレームを送信します。

テストが複数のプローブを実行する場合、NQA クライアントは以下の状況で新しいプローブを開始します。

- NQA クライアントが最後のプローブで送信したパケットの応答を受信します。
- プローブのタイムアウト時間が終了します。

このコマンドは音声、UDP ジッタテストで無効です。これらのテストは 1 つのプローブのみ実行します。

例

ICMP エコーテストを実行する検査回数を 10 に設定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type icmp-echo

[Switch-nqa-admin-test-icmp-echo] probe count 10

2.1.25 probe packet-interval

Syntax

probe packet-interval *interval*

undo probe packet-interval

デフォルト

20 ミリ秒

View

UDP jitter/voice operation view

定義済みユーザロール

network-admin

パラメータ

interval: パケットを送信する間隔を指定します。設定範囲は 10～60000 ミリ秒です。

説明

probe packet-interval コマンドはプローブのパケットを送信する間隔を設定します。

undo probe packet-interval コマンドはデフォルトに戻します。

例

UDP ジッタテストのパケットを送信する間隔を 100 ミリ秒に設定します。

<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

2.1.26 probe packet-number

Syntax

probe packet-number *packet-number*

undo probe packet-number

デフォルト

UDP ジッタテストは 10 のパケットを送信します。音声テストは 1000 のパケットを送信します。

View

UDP jitter/voice operation view

定義済みユーザロール

network-admin

パラメータ

packet-number: プローブごとに送信するパケット数を指定します。

- UDP ジッタテストの設定範囲は 10～1000 です。
- 音声テストの設定範囲は 10～60000 です。

説明

probe packet-number コマンドは UDP ジッタテスト、音声テストで送信するパケットの数を設定します。

undo probe packet-number コマンドはデフォルトに戻します。

例

UDP ジッタテストで 100 パケットを送信するように設定します。

<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

2.1.27 probe packet-timeout

Syntax

probe packet-timeout *timeout*

undo probe packet-timeout

デフォルト

UDP ジッタテストの応答タイムアウト時間は 3000 ミリ秒です。

音声テストの応答タイムアウト時間は 5000 ミリ秒です。

View

UDP jitter/voice operation view

定義済みユーザロール

network-admin

パラメータ

timeout: UDP ジッタテスト、音声テストの応答を待つタイムアウト時間を指定します。設定範囲は 10～3600000 ミリ秒です。

説明

probe packet-timeout コマンドは UDP ジッタテスト、音声テストの応答を待つタイムアウト時間を設定します。

undo probe packet-timeout コマンドはデフォルトに戻します。

例

UDP ジッタテストの応答を待つタイムアウト時間を 100 ミリ秒に設定します。

<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

2.1.28 probe timeout

Syntax

probe timeout *timeout*

undo probe timeout

デフォルト

3000 ミリ秒

View

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

定義済みユーザロール

network-admin

パラメータ

timeout: プローブのタイムアウト時間を指定します。

- FTP テスト、HTTP テストの設定範囲は 10～86400000 ミリ秒です。
- DHCP テスト、DNS テスト、DLSw テスト、ICMP エコーテスト、SNMP テスト、TCP テスト、UDP エコーテストの設定範囲は 10～3600000 ミリ秒です。

説明

probe timeout コマンドはプローブのタイムアウト時間を設定します。

undo probe timeout コマンドはデフォルトに戻します。

プローブの時間以内にテストが完了しない場合、プローブがタイムアウトします。

例

DHCP テストのプローブタイムアウト時間を 10000 ミリ秒に設定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type dhcp

[Switch-nqa-admin-test-dhcp] probe timeout 10000

2.1.29 reaction checked-element probe-fail (for trap)

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*

デフォルト

設定なし

View

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

定義済みユーザロール

network-admin

パラメータ

item-number: リアクションエントリに ID を割り当てます。設定範囲は 1～10 です。

threshold-type: しきい値タイプを指定します。

accumulate *accumulate-occurrences*: プローブが失敗する総数を確認します。設定範囲は 1～15 です。

consecutive *consecutive-occurrences*: 連続してテストに失敗する最大数を指定します。設定範囲は 1～16 です。

action-type: トリガとなるアクションを指定します。デフォルトのアクションは **none** です。

none: ターミナル端末に結果を表示します。

trap-only: ターミナル端末に結果を表示し、NMS に SNMP トラップメッセージを送信します。DNS テストでは無効です。

説明

reaction checked-element probe-fail コマンドはテストのプローブの失敗をモニタするためのリアクションエントリを設定します。

undo reaction コマンドは指定されたリアクションエントリを削除します。

リアクションを作成した後、修正することはできません。リアクションエントリの属性を変更する場合、**undo reaction** コマンドを使用して最初にエントリを削除し、新しいリアクションエントリを再度設定してください。

例

ICMP エコーテストのプローブ失敗をモニタするため、リアクションエントリ 1 を作成します。NQA テストを開始する前に、リアクションエントリの初期状態は無効です。プローブが失敗した回数が 10 以上になった場合、エントリの状態をしきい値超過に設定します。しきい値が下回った場合、エントリの状態をしきい値以下に設定します。一度リアクションエントリの状態が変更するとトラップメッセージを作成し、NMS に送信します。

<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

ICMP エコーテストのプローブ失敗をモニタするため、リアクションエントリ 2 を作成します。NQA テストを開始する前に、リアクションエントリの初期状態は無効です。連続してプローブが失敗した回数が 10 以上になった場合、エントリの状態をしきい値超過に設定します。しきい値が下回った場合、エントリの状態をしきい値以下に設定します。一度リアクションエントリの状態が変更するとトラップメッセージを作成し、NMS に送信します。

<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

2.1.30 reaction checked-element probe-fail (for trigger)

Syntax

reaction *item-number* **checked-element probe-fail threshold-type consecutive** *consecutive-occurrences* **action-type trigger-only**

undo reaction *item-number*

デフォルト

設定なし

View

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

定義済みユーザロール

network-admin

パラメータ

item-number: リアクションエントリに ID を割り当てます。設定範囲は 1～10 です。

threshold-type: しきい値タイプを指定します。

consecutive *consecutive-occurrences*: 連続してテストに失敗する最大数を指定します。設定範囲は 1～16 です。

action-type: トリガとなるアクションを指定します。

trigger-only: 一定の条件に対応するために他のモジュールを起動します。

説明

reaction checked-element probe-fail コマンドはプローブの失敗をモニタするため、リアクションエントリを設定します。

undo reaction コマンドは指定したリアクションエントリを削除します。

リアクションを作成した後、修正することはできません。リアクションエントリの属性を変更する場合、**undo reaction** コマンドを使用して最初にエントリを削除し、新しいリアクションエントリを再度設定してください。

例

リアクションエントリ 1 を作成します。連続してプローブが 3 回失敗した場合、コラボレーションを起動します。

<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

関連コマンド

track (コマンドマニュアルのセクション 10 *高可用性 “Track”*)

2.1.31 reaction trap

Syntax

reaction trap { **probe-failure** *consecutive-probe-failures* | **test-complete** | **test-failure** [*accumulate-probe-failures*] }

undo reaction trap { **probe-failure** | **test-complete** | **test-failure** }

デフォルト

設定なし

View

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

UDP jitter/voice operation view

定義済みユーザロール

network-admin

パラメータ

probe-failure *consecutive-probe-failures*: 連続してテストが失敗した後、NMS にトラップを送信するよう設定します。*consecutive-probe-failures* はテストにおける連続失敗数を設定します。設定範囲は 1～15 です。システムは複数のトラップを送信できるように各テストで連続して失敗した回数をカウントします。

test-complete: テストが完了したことを通知するためにトラップを送信します。

test-failure *accumulate-probe-failures*: プローブの失敗回数の総数が *accumulate-probe-failures* 以上になった場合、トラップを送信します。設定範囲は 1～15

です。システムは、1 つのトラップのみ送信するため、最後にテストを完了した後、プローブが失敗した総数をカウントします。

説明

reaction trap コマンドは指定した状況下で NMS にトラップを送信するように設定します。

undo reaction trap コマンドはデフォルトに戻します。

UDP ジッタテスト、音声テストは **test-complete** パラメータのみ有効です。

例

ICMP エコーテストで連続して 5 回以上失敗した場合、トラップを送信するように設定します。

<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

2.1.32 resolve-target

Syntax

resolve-target *domain-name*

undo resolve-target

デフォルト

設定なし

View

DNS operation view

定義済みユーザロール

network-admin

パラメータ

domain-name: 解決されるドメイン名を指定します。設定範囲は 1～255 文字です。ドットで区切り、大文字、小文字を区別します。英字、数字、ハイフン（-）、アンダーライン（_）を含むことができます（たとえば、aabbcc.com です）。各部分の設定範囲は 1～63 文字です。連続したドット（.）は使用できません。

説明

resolve-target コマンドは DNS テストのドメイン名を設定します。

undo resolve-target コマンドはデフォルトに戻します。

例

解決されるドメイン名 **domain1** を設定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type dns

[Switch-nqa-admin-test-dns] resolve-target domain1

2.1.33 route-option bypass-route

Syntax

route-option bypass-route

undo route-option bypass-route

デフォルト

無効

View

ICMP echo/TCP/UDP echo operation view

DLSw/DNS/FTP/HTTP/SNMP operation view

UDP jitter/voice operation view

定義済みユーザロール

network-admin

説明

route-option bypass-route コマンドはダイレクトな宛先への接続性を確認するため、ルーティングテーブルバイパス機能を有効にします。

undo route-option bypass-route コマンドはルーティングバイパス機能を無効にします。

ルーティングテーブルバイパス機能が有効であるとき、以下のイベントが発生します。

- ルーティングテーブルは検索されません。パケットはダイレクトに接続されたネットワークの宛先に直接送信されます。
- テストパケットの TTL が 1 に設定されます。**ttl** コマンドで設定された値は適用されません。

例

ルーティングテーブルバイパス機能を有効にします。

<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

2.1.34 source interface (ICMP echo operation view)

Syntax

source interface *interface-type interface-number*

undo source interface

デフォルト

ICMP エコー要求パケットは送信元 IP アドレスとして送信インタフェースのプライマリ IP アドレスを使用します。

View

ICMP echo operation view

定義済みユーザロール

network-admin

パラメータ

interface-type interface-number: インタフェースのタイプと番号を指定します。

説明

source interface コマンドは ICMP エコー要求パケットの送信元 IP アドレスとして指定したインタフェースの IP アドレスを指定します。

undo source interface コマンドはデフォルトに戻します。

指定したインタフェースはアップ状態にする必要があります。インタフェースがダウンしている場合、ICMP エコー要求は送信することができません。

source ip コマンドと **source interface** コマンドの両方を設定した場合、最後に行った設定が適用されます。

例

ICMP エコー要求パケットの送信元 IP アドレスとして VLAN インタフェース 1 の IP アドレスを設定します。

<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

関連コマンド

source ip

2.1.35 source ip

Syntax

source ip *ip-address*

undo source ip

デフォルト

ICMP エコー要求パケットは送信元 IP アドレスとして送信インタフェースのプライマリ IP アドレスを使用します。

View

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/FTP/HTTP/SNMP operation view

UDP jitter/voice operation view

定義済みユーザロール

network-admin

パラメータ

ip-address: プローブパケットの送信元 IP アドレスを指定します。

説明

source ip コマンドはプローブパケットの送信元 IP アドレスを設定します。

undo source ip コマンドは指定された送信元アドレスを削除します。

指定された送信元 IP アドレスはローカルインタフェースの IP アドレスで、インタフェースがアップである必要があります。そうでなければプローブパケットは送信できません。

ICMP エコーテストで **source ip** コマンドと **source interface** コマンドの両方を設定した場合、最後に行った設定が適用されます。

例

ICMP エコー要求の送信元 IP アドレスを 10.1.1.1 に設定します。

<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

関連コマンド

source interface

2.1.36 source port

Syntax

source port *port-number*

undo source port

デフォルト

設定なし

View

UDP echo operation view

SNMP operation view

UDP jitter/voice operation view

定義済みユーザロール

network-admin

パラメータ

port-number: 送信元ポート番号を指定します。設定範囲は 1～65535 です。

説明

source port コマンドはプローブパケットの送信元ポートを設定します。

undo source port コマンドは設定された送信元ポートを削除します。

例

UDP エコーテストのプローブパケットで送信元ポートを 8000 に設定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type udp-echo

[Switch-nqa-admin-test-udp-echo] source port 8000

2.1.37 statistics hold-time

Syntax

statistics hold-time *hold-time*

undo statistics hold-time

デフォルト

120 分

View

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

UDP jitter/voice operation view

定義済みユーザロール

network-admin

パラメータ

hold-time: 保持時間を指定します。設定範囲は 1～1440 分です。

説明

statistics hold-time コマンドは NQA テストの統計情報グループの保持時間を設定します。

undo statistics hold-time コマンドはデフォルトに戻します。

保持時間が終了したとき、統計情報グループは削除されます。

例

ICMP エコーテストの統計情報グループの保持時間を 3 分に設定します。

<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

2.1.38 statistics interval

Syntax

statistics interval *interval*

undo statistics interval

デフォルト

60 分

View

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

UDP jitter/voice operation view

定義済みユーザロール

network-admin

パラメータ

interval: 統計情報を収集する間隔を指定します。設定範囲は 1～35791394 分です。

説明

statistics interval コマンドは NQA テストで統計情報を収集する間隔を設定します。

undo statistics interval コマンドはデフォルトに戻します。

NQA は指定した間隔で NQA テストを行い、テスト結果の統計情報を計算します。これらの統計情報は統計情報グループを作ります。統計情報グループの情報を表示する場合、**display nqa statistics** コマンドを使用します。

例

ICMP エコーテストで統計情報を収集する間隔を 2 分に設定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type icmp-echo

[Switch-nqa-admin-test-icmp-echo] statistics interval 2

2.1.39 statistics max-group

Syntax

statistics max-group *number*

undo statistics max-group

デフォルト

2

View

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

UDP jitter/voice operation view

定義済みユーザロール

network-admin

パラメータ

number: 統計情報グループの最大数を指定します。設定範囲は 0～100 です。統計情報の収集を無効にする場合、0 に設定します。

説明

statistics max-group コマンドは保存できる統計情報グループの最大数を設定します。

undo statistics max-group コマンドはデフォルトに戻します。

統計情報グループの数が最大数に到達し、新しいグループが保存されたとき、もっとも古い統計情報が削除されます。

例

ICMP エコーテストで保存できる統計情報グループの最大数を 5 に設定します。

<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

2.1.40 tos

Syntax

tos *value*

undo tos

デフォルト

0

View

すべての operation view

定義済みユーザロール

network-admin

パラメータ

value: ToS を指定します。設定範囲は 0～255 です。

説明

tos コマンドはプローブパケットの IP ヘッダの ToS を設定します。

undo tos コマンドはデフォルトに戻します。

例

ICMP エコーテストでプローブパケットの IP ヘッダの ToS を 1 に設定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type icmp-echo

[Switch-nqa-admin-test-icmp-echo] tos 1

2.1.41 ttl

Syntax

ttl *value*

undo ttl

デフォルト

20

View

ICMP echo/TCP/UDP echo operation view

DLSw/DNS/FTP/HTTP/SNMP operation view

UDP jitter/voice operation view

定義済みユーザロール

network-admin

パラメータ

value: プローブパケットの TTL を指定します。設定範囲は 1～255 です。

説明

ttl コマンドはプローブパケットの TTL を指定します。

undo ttl コマンドはデフォルトに戻します。

route-option bypass-route コマンドはプローブパケットの TTL を 1 に設定します。**route-option bypass-route** コマンドと **ttl** コマンドを同時に実行した場合、**ttl** コマンドは適用されません。

例

ICMP エコーテストでプローブパケットの TTL を 16 に設定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type icmp-echo

[Switch-nqa-admin-test-icmp-echo] ttl 16

2.1.42 type

Syntax

type { **dhcp** | **dlsw** | **dns** | **ftp** | **http** | **icmp-echo** | **snmp** | **tcp** | **udp-echo** | **udp-jitter** | **voice** }

デフォルト

設定なし

View

NQA operation view

定義済みユーザロール

network-admin

パラメータ

dhcp: DHCP テストタイプを指定します。

dlsw: DLSw テストタイプを指定します。

dns: DNS テストタイプを指定します。

ftp: FTP テストタイプを指定します。

http: HTTP テストタイプを指定します。

icmp-echo: ICMP エコーテストタイプを指定します。

snmp: SNMP テストタイプを指定します。

tcp: TCP テストタイプを指定します。

udp-echo: UDP エコーテストタイプを指定します。

udp-jitter: UDP ジッタテストタイプを指定します。

voice: 音声テストタイプを指定します。

説明

type コマンドは NQA テストのテストタイプを設定し、operation type view に移行します。

例

FTP テストのテストタイプを設定し、FTP operation view に移行します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type ftp

[Switch-nqa-admin-test-ftp]

2.1.43 url

Syntax

url *url*

undo url

デフォルト

設定なし

View

FTP/HTTP operation view

定義済みユーザロール

network-admin

パラメータ

url: 宛先サーバの URL を指定します。設定範囲は 1～255 文字です。大文字、小文字を区別します。スペース、クエスチョンマーク（?）は使用できません。以下の表に異なるテストの URL のフォーマットとパラメータを示します。

テスト	URL フォーマット	パラメータの説明
HTTPテスト	*http://host/resource* *http://host:port/resource*	hostパラメータの設定範囲は1～255文字です。ドットで区切られ、大文字、小文字を区別します。英字、数字、ハイフン（-）、アンダーライン（_）を含むことができます。たとえばaabbcc.comです。各部分の設定範囲は1～63文字です。連続してドット（.）を設定することができません。ファイル名のパラメータの詳細は、オペレーションマニュアルのセクション1*はじめに*”*ファイルシステム管理*”を参照してください。
FTPテスト	*ftp://host/filename* *ftp://host:port/filename*	

説明

url コマンドは宛先 HTTP サーバあるいは宛先 FTP サーバの URL を指定します。

undo url コマンドは URL を削除します。

例

HTTP テストの URL を **http://www.company.com/index.htm** に設定します。

<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

2.1.44 username

Syntax

username *username*

undo username

デフォルト

設定なし

View

FTP/HTTP operation view

定義済みユーザロール

network-admin

パラメータ

username: ユーザ名を指定します。設定範囲は 1～32 文字です。

説明

username コマンドは FTP あるいは HTTP ログインのユーザ名を指定します。

undo username コマンドは設定を削除します。

例

FTP ログインのユーザ名を **administrator** に設定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type ftp

[Switch-nqa-admin-test-ftp] username administrator

関連コマンド

- **operation**
- **password**

2.1.45 version

Syntax

version { **v1.0** | **v1.1** }

undo version

デフォルト

1.0

View

HTTP operation view

定義済みユーザロール

network-admin

パラメータ

v1.0: HTTP バージョン 1.0 を使用します。

v1.1: HTTP バージョン 1.1 を使用します。

説明

version コマンドは HTTP テストで使用する HTTP バージョンを指定します。

undo version コマンドはデフォルトに戻します。

例

HTTP テストで使用する HTTP バージョンを 1.1 に指定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type http

[Switch-nqa-admin-test-http] version v1.1

2.1.46 vpn-instance

Syntax

vpn-instance *vpn-instance-name*

undo vpn-instance

デフォルト

パブリックネットワークでテスト可能

View

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

UDP tracert operation view

ICMP jitter/path jitter/UDP jitter/voice operation view

Any NQA template view

定義済みユーザロール

network-admin

パラメータ

vpn-instance-name: VPN インスタンスの名前を指定します。大文字小文字を区別し、設定範囲は 1～31 文字です。

説明

vpn-instance コマンドは、VPN インスタンステストを適用します。

undo vpn-instance コマンドは、設定をデフォルトに戻します。

VPN を指定した後、NQA は指定した VPN で接続性をテストします。

例

ICMP エコーテストを **vpn1** に適用します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type icmp-echo

[Switch-nqa-admin-test-icmp-echo] vpn-instance vpn1

FTP テンプレートビューで、FTP テストを **vpn1** に適用します。

<Switch> system-view

[Switch] nqa template ftp ftptplt

[Switch-nqatplt-ftp-ftptplt] vpn-instance vpn1

2.2 NQAサーバ設定コマンド

⚠ **重要：**

UDP ジッタテスト、TCP テスト、UDP エコーテスト、音声テストを行うため、NQA サーバを設定します。

2.2.1 display nqa server

Syntax

display nqa server

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display nqa server コマンドは NQA サーバの状態を表示します。

例

NQA サーバの状態を表示します。

<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    -
```

表 2-7 コマンド出力

フィールド	説明
NQA server status	NQAサーバが有効かどうかを示します。
TCP connect	NQAサーバのTCPリスニングサービスの情報です。

フィールド	説明
UDP echo	NQAサーバのUDPリスニングサービスの情報です。
IP Address	NQAサーバのTCP/UDPリスニングサービスで指定されたIPアドレスです。
Port	NQAサーバのTCP/UDPリスニングサービスでの指定されたポート番号です。
Tos	NQAサーバが送信する応答パケットのToSの値です。
VPN instance	このフィールドは現在のソフトウェアバージョンでサポートしていません。

関連コマンド

- **nqa server enable**
- **nqa server tcp-connect**
- **nqa server udp-echo**

2.2.2 nqa server enable

Syntax

nqa server enable

undo nqa server enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

nqa server enable コマンドは NQA サーバを有効にします。

undo nqa server enable コマンドは NQA サーバを無効にします。

例

NQA サーバを有効にします。

<Switch> system-view

[Switch] nqa server enable

関連コマンド

- **display nqa server**
- **nqa server tcp-connect**
- **nqa server udp-echo**

2.2.3 nqa server tcp-connect

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* [**vpn-instance** *vpn-instance-name*]

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

ip-address: TCP リスニングサービスの IP アドレスを指定します。

port-number: TCP リスニングサービスのポート番号を指定します。設定範囲は 1～65535 です。

vpn-instance *vpn-instance-name*: VPN インスタンスを名前で指定します。大文字、小文字を区別し、設定範囲は 1～31 文字です。このオプションを指定しない場合、NQA サーバはパブリックネットワーク上の IP アドレスで TCP サービスをリッスンします。

tos *tos*: 応答パケットの IP ヘッダの ToS を指定します。設定範囲は 0～255 です。デフォルトは 0 です。

説明

nqa server tcp-connect コマンドは NQA サーバが指定された IP アドレスとポート番号をリスニングし、応答するため、TCP リスニングサービスを設定します。

undo nqa server tcp-connect コマンドは TCP リスニングサービスを削除します。

このコマンドは NQA サーバ上で TCP テストのみに使用されます。

NQA サーバの TCP リスニングサービスの IP アドレスとポート番号を設定するとき、以下の制限とガイドラインに従ってください。

- IP アドレスとポート番号は NQA サーバで固有に設定し、NQA クライアントの設定に一致するようにしてください。
- IP アドレスは NQA サーバのインタフェースの IP アドレスにする必要があります。そうでなければ、設定は無効となります。
- NQA テストを正常に実行し、既存のサービスへの影響を防ぐため、TCP リスニングサービスで 1～1023 の well-known ポートを設定しないでください。

例

NQA サーバで TCP リスニングサービスを設定します。IP アドレス 169.254.10.2、ポート番号 9000 をリスニングし、応答するように設定します。

<Switch> system-view

[Switch] nqa server tcp-connect 169.254.10.2 9000

関連コマンド

- **display nqa server**
- **nqa server enable**

2.2.4 nqa server udp-echo

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* [**vpn-instance** *vpn-instance-name*]

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

ip-address: UDP リスニングサービスの IP アドレスを指定します。

port-number: UDP リスニングサービスのポート番号を指定します。設定範囲は 1～65535 です。

vpn-instance *vpn-instance-name*: VPN インスタンスを名前で指定します。大文字小文字を区別し、設定範囲は 1～31 文字です。このオプションを指定しない場合、NQA サーバはパブリックネットワーク上の IP アドレスで UDP サービスをリッスンします。

tos *tos*: 応答パケットの IP ヘッダの ToS を指定します。設定範囲は 0～255 です。デフォルトは 0 です。

説明

nqa server udp-echo コマンドは NQA サーバが指定された IP アドレスとポート番号をリスニングし、応答するため、UDP リスニングサービスを設定します。

undo nqa server udp-echo コマンドは UDP リスニングサービスを削除します。

このコマンドは NQA サーバ上で UDP ジッタテスト、UDP エコーテスト、音声テストのみに使用されます。

NQA サーバの UDP リスニングサービスの IP アドレスとポート番号を設定するとき、以下の制限とガイドラインに従ってください。

- IP アドレスとポート番号は NQA サーバで固有に設定し、NQA クライアントの設定に一致するようにしてください。
- IP アドレスは NQA サーバのインタフェースの IP アドレスにする必要があります。そうでなければ、設定は無効となります。
- NQA テストを正常に実行し、既存のサービスへの影響を防ぐため、UDP リスニングサービスで 1～1023 の well-known ポートを設定しないでください。

例

NQA サーバで UDP リスニングサービスを設定します。IP アドレス 169.254.10.2、ポート番号 9000 をリスニングし、応答するように設定します。

<Switch> system-view

[Switch] nqa server udp-echo 169.254.10.2 9000

関連コマンド

- **display nqa server**
- **nqa server enable**

目次

このセクションのページは **11-x-x** です。

3 章 NTP 3-1
3.1 NTP 設定コマンド 3-1
3.1.1 display ntp-service sessions 3-1
3.1.2 display ntp-service status 3-7
3.1.3 display ntp-service trace 3-10
3.1.4 ntp-service acl 3-11
3.1.5 ntp-service authentication enable 3-13
3.1.6 ntp-service authentication-keyid 3-14
3.1.7 ntp-service broadcast-client 3-15
3.1.8 ntp-service broadcast-server 3-16
3.1.9 ntp-service dscp 3-17
3.1.10 ntp-service enable 3-18
3.1.11 ntp-service inbound enable 3-18
3.1.12 ntp-service max-dynamic-sessions 3-19
3.1.13 ntp-service multicast-client 3-20
3.1.14 ntp-service multicast-server 3-21
3.1.15 ntp-service refclock-master 3-23
3.1.16 ntp-service reliable authentication-keyid 3-24
3.1.17 ntp-service source 3-25
3.1.18 ntp-service unicast-peer 3-26
3.1.19 ntp-service unicast-server 3-28

3章 NTP

3.1 NTP設定コマンド

3.1.1 display ntp-service sessions

Syntax

display ntp-service sessions [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

verbose: すべての IPv4 NTP アソシエーションの詳細情報を表示します。指定しない場合、NTP アソシエーションの概要情報を表示します。

説明

display ntp-service sessions コマンドはすべての IPv4 NTP アソシエーションの情報を表示します。

装置が NTP ブロードキャストモードあるいはマルチキャストサーバモードで動作しているとき、**display ntp-service sessions** コマンドはブロードキャストサーバあるいはマルチキャストサーバに対応する IPv4 NTP アソシエーションの情報を表示しませんが、アソシエーションの総数がカウントされます。

例

すべての NTP アソシエーションの概要情報を表示します。

<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
```

表 3-1 コマンド出力

フィールド	説明
source	• 参照クロックがローカルクロックであるとき、**LOCAL**(*number*)と表示されます。ローカルクロックのIPアドレスは127.127.1.*number*です。*number*はNTPプロセス番号です。値の範囲は0～3です。 • 参照クロックが別の装置であるとき、NTPサーバのIPアドレスが表示されます。このフィールドが**0.0.0.0**である場合、NTPサーバのIPアドレスは正常に解決されていません。

reference	NTPサーバの参照クロックIDです。
	• 参照クロックがローカルクロックであるとき、straフィールドに関連した値が表示されます。
	  • straフィールドの値が0あるいは1である場合、**LOCL**と表示されます。
	  • straフィールドが別の値である場合、ローカルクロックのIPアドレスを表示します。
	• 参照クロックがネットワーク上の他の装置のクロックである場合、このフィールドは装置のIPアドレスになります。装置がIPv6をサポートしている場合、装置のIPv6アドレスの最初の32ビットのMD5ダイジェストを表示します。**INIT**と表示される場合、ローカル装置はNTPサーバと接続を確立していません。

stra	クロックソースのstratumレベルです。stratumレベルはクロックの正確さを示します。値の範囲は1～16です。値が大きくなると精度が減少します。クロックの精度は1がもっとも高く、stratumが16は同期化されておらず、参照クロックを使用することができません。
reach	クロックソースの到達可能回数です。0はクロックソースが到達不能であることを示します。
poll	ポーリング間隔です。連続する2つのNTPメッセージ間の最大間隔です。

フィールド	説明
now	最後のNTPメッセージを受信、あるいはローカルクロックが最後に更新されてから現在までの時間です。 デフォルトの時間の単位は秒です。 ● 時間の長さが2048秒を超えると、分で表示されます。 ● 時間の長さが300分を超えると時間で表示されます。 ● 時間の長さが96時間を越えると日の単位で表示されます。 ● 時間の長さが999日を越えると年の単位で表示されます。 最後のNTPメッセージを受信した時間あるいはローカルクロックが最後に更新された時間が、現在時間より遅れている場合、ハイフン（-）が表示されます。
offset	リファレンスクロックに対するシステムクロックのオフセットです。単位はミリ秒です。
delay	ローカル装置からクロックソースまでのラウンドトリップ遅延です。単位はミリ秒です。
disper	リファレンスソースに対するローカルクロックの最大誤差です。単位はミリ秒です。
[12345]	● **1**—システムが選択したクロックソースです（現在のリファレンスソースです）。システムクロックstratumレベルは15以下です。 ● **2**—クロックソースのstratumレベルは15以下です。 ● **3**—クロックソースはクロック選定アルゴリズムに残りしました。 ● **4**—クロックソースはクロックソースの候補です。 ● **5**—クロックソースは設定されたコマンドで作成されました。
Total sessions	アソシエーションの総数です。

すべての IPv4 NTP アソシエーションの詳細情報を表示します。

<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
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
```

表 3-2 コマンド出力

フィールド	説明
Clock source	NTPサーバのIPアドレスです。**0.0.0.0**が表示される場合、NTPサーバのIPアドレスは正常に解決されていません。
Clock stratum	NTPサーバのstratumレベルです。stratumレベルはクロックの正確さを示します。値の範囲は1～16です。値が大きくなると精度が減少します。クロックの精度は1がもっとも高く、stratumが16は同期化されておらず、参照クロックを使用することができません。

フィールド	説明

Clock status	アソシエーションに対応するクロックソースの状態です。
	• **configured**—アソシエーションが設定コマンドで作成されました。
	• **dynamic**—ダイナミックにアソシエーションが確立されました。
	• **master**—クロックソースは現在のシステムのプライマリ参照ソースです。
	• **selected**—クロックソースはクロック選定アルゴリズムに残りました。
	• **candidate**—クロックソースはクロックソースの候補です
	• **sane**—クロックソースは認証にパスしました。参照クロックとして使用されています。
	• **insane**—クロックソースは認証に失敗しました。あるいは認証にパスしましたが参照クロックして使用されていません。
	• **valid**—クロックソースが有効です。クロックソースは以下の要件に従います。
	  • クロックソースは認証にパスし、同期しています。
	  • stratumレベルが有効です。
	  • ルート遅延とルート拡散が範囲内にあります。
	• **invalid**—クロックソースが無効です。
	• **unsynced**—クロックソースが同期されていないか、stratumレベルが無効です。

Reference clock ID	NTPサーバの参照クロックのIDです。
	• 参照クロックがローカルクロックであるとき、クロックstratumフィールドに関連した値が表示されます。
	  • クロックstratumフィールドの値が0あるいは1である場合、**LOCL**と表示されます。
	  • クロックstratumフィールドが別の値である場合、ローカルクロックのIPアドレスを表示します。
	参照クロックがネットワーク上の他の装置のクロックである場合、このフィールドは装置のIPアドレスになります。装置がIPv6をサポートしている場合、装置のIPv6アドレスの最初の32ビットのMD5ダイジェストを表示します。**INIT**と表示される場合、ローカル装置はNTPサーバと接続を確立していません。

フィールド	説明
Local mode	ローカル装置の動作モードです。 • **unspec**—このモードは不特定です。 • **active**—アクティブモードです。 • **passive**—パッシブモードです。 • **client**—クライアントモードです。 • **server**—サーバモードです。 • **broadcast**—ブロードキャストあるいはマルチキャストサーバモードです。 • **bclient**—ブロードキャストあるいはマルチキャストクライアントモードです。
local poll interval	ローカル装置のポーリング間隔です。値は2の乗数で表示されます。たとえば、6が表示されている場合、ローカル装置のポーリング間隔は26あるいは64秒です。
Peer mode	ピアの装置の動作モードです。 • **unspec**—このモードは不特定です。 • **active**—アクティブモードです。 • **passive**—パッシブモードです。 • **client**—クライアントモードです。 • **server**—サーバモードです。 • **broadcast**—ブロードキャストあるいはマルチキャストサーバモードです。 • **bclient**—ブロードキャストあるいはマルチキャストクライアントモードです。
peer poll interval	ピアの装置のポーリング間隔です。値は2の乗数で表示されます。たとえば、6が表示されている場合、ローカル装置のポーリング間隔は26あるいは64秒です。
Offset	参照クロックに対するシステムクロックのオフセットです。単位はミリ秒です。
roundtrip delay	ローカル装置からクロックソースまでのラウンドトリップ遅延です。単位はミリ秒です。
dispersion	参照ソースに対するシステムクロックの最大誤差です。
Root roundtrip delay	ローカル装置からプライマリ参照ソースまでのラウンドトリップ遅延です。単位はミリ秒です。
root dispersion	プライマリ参照クロックに対するシステムクロックの最大誤差です。単位はミリ秒です。
Reachabilities	クロックソースの到達可能回数です。0は、このクロックソースが到達不可能であることを示します。

フィールド	説明
sync distance	上位レベルのクロックに対する同期距離です。単位は秒です。ばらつきとラウンドトリップ遅延の値から計算されます。
Precision	システムクロックの精度です。
version	NTPバージョンです。値の範囲は1～4です。
source interface	送信元インタフェースです。 送信元インタフェースが指定されていない場合、**Not specified**と表示されます。
Reftime	NTPメッセージの参照タイムスタンプです。
Orgtime	NTPメッセージの発生タイムスタンプです。
Rcvtime	NTPメッセージの受信タイムスタンプです。
Xmttime	NTPメッセージの送信タイムスタンプです。
Filter order	情報順序のサンプルです。
Reference clock status	ローカルクロックの状態です。このフィールドは参照クロックとしてローカルクロックを設定する**ntp-service refclock-master**コマンドを使用したときに表示されます。 ローカルクロックのreachフィールドが255であるとき、**working normally**と表示されます。そうでない場合、**working abnormally**と表示されます。QX-S5100Gシリーズは**ntp-service refclock-master**コマンドをサポートしていません。
Total sessions	アソシエーションの総数です。

3.1.2 display ntp-service status

Syntax

display ntp-service status

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display ntp-service status コマンドは NTP サービスの状態を表示します。

例

クロックの同期後の NTP サービスの状態を表示します。

<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^-10
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: 8 s
```

クロックを同期していないときの NTP サービスの状態を表示します。

<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^-10#
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
```

表 3-3 コマンド出力

フィールド	説明
Clock status	システムクロックの状態です。 • **synchronized**—システムクロックが同期されています。 • **unsynchronized**—システムクロックが同期されていません。
Clock stratum	システムクロックのstratumレベルです。

フィールド	説明
System peer	選択されたNTPサーバのIPアドレスです。
Local mode	ローカル装置の動作モードです。 • **unspec**—このモードは不特定です。 • **active**—アクティブモードです。 • **passive**—パッシブモードです。 • **client**—クライアントモードです。 • **server**—サーバモードです。 • **broadcast**—ブロードキャストあるいはマルチキャストサーバモードです。 • **bclient**—ブロードキャストあるいはマルチキャストクライアントモードです。
Reference clock ID	IPv4 NTPサーバの場合、以下を示します。 ローカル装置がリモートNTPサーバに同期されているとき、このフィールドはリモートサーバのIPアドレスを表示します。 ローカル装置が参照ソースとしてローカルクロックを使用するとき、このフィールドはローカルクロックを表示します。 • ローカルクロックのstratumフィールドの値が1である場合、**Local**と表示されます。 • クロックstratumフィールドが別の値である場合、ローカルクロックのIPアドレスを表示します。 IPv6 NTPサーバの場合、以下を示します。 ローカル装置がリモートIPv6 NTPサーバに同期されているとき、このフィールドはリモートサーバのIPv6アドレスの最初の32ビットのMD5ダイジェストを表示します。 ローカル装置が参照ソースとしてローカルクロックを使用するとき、このフィールドはローカルクロックを表示します。 • ローカルクロックのstratumフィールドの値が1である場合、**Local**と表示されます。 • クロックstratumフィールドが別の値である場合、ローカルクロックのIPv6アドレスの最初の32ビットのMD5ダイジェストを表示します。

フィールド	説明
Leap indicator	アラーム状態です。 • **00**—正常です。 • **01**—leap秒です。一日の最後の分が61秒であることを示します。 • **10**— leap秒です。一日の最後の分が59秒であることを示します。 • **11**—クロックが同期されていません。
Clock jitter	システムクロックと参照クロック間の相違です。単位は秒です。
Stability	クロック周波数の安定性です。値が低い場合、安定性が高いことを示します。
Clock precision	システムクロックの精度です。
Root delay	ローカル装置からプライマリ参照ソースまでのラウンドトリップ遅延です。単位はミリ秒です。
Root dispersion	プライマリ参照クロックに対するシステムクロックの最大誤差です。単位はミリ秒です。
Reference time	参照タイムスタンプです。

3.1.3 display ntp-service trace

Syntax

display ntp-service trace

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display ntp-service trace コマンドはローカル装置からプライマリ参照ソース間の NTP サーバの概要情報を表示します。

例

ローカル装置からプライマリ参照ソース間の NTP サーバの概要情報を表示します。

<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
```

出力は、サーバ 127.0.0.1 がサーバ 3000::32 に同期しており、サーバ 3000::32 がローカルクロックに同期していることを示します。

表 3-4 コマンド出力

フィールド	説明
Server	NTPサーバのIPアドレスです。
Stratum	NTPサーバのstratumレベルです。
jitter	上位レベルクロックに対するクロックオフセットのRMS（Root mean square）です。単位は秒です。
synch distance	上位レベルのNTPサーバに対する同期間隔です。単位は秒です。ばらつきとラウンドトリップ遅延の値から計算されます。
RefID	プライマリ参照ソースの識別子です。プライマリ参照クロックのstratumレベルが0であるとき、**Local**と表示されます。そうでなければプライマリ参照クロックのIPアドレスが表示されます。

関連コマンド

- **ntp-service source**
- **ntp-service unicast-server**
- **ntp-service unicast-peer**

3.1.4 ntp-service acl

Syntax

ntp-service { **peer** | **query** | **server** | **synchronization** } **acl** *ipv4-acl-number*

undo ntp-service { **peer** | **query** | **server** | **synchronization** } [**acl** *ipv4-acl-number*]

デフォルト

peer

View

System view

定義済みユーザロール

network-admin

パラメータ

peer: タイム要求とピア装置からの NTP 制御クエリ（アラーム、認証状態、タイムサーバ情報など）を許可します。ローカル装置がピアの装置と同期することを許可します。

query: ピア装置からローカル装置の NTP 制御クエリのみ許可します。

server: タイム要求とピア装置からの NTP 制御クエリを許可します。ローカル装置がピアの装置と同期することを許可しません。

synchronization: ACL にパスするアドレスのシステムからのタイム要求のみ許可します。

acl *ipv4-acl-number*: IPv4 ACL を指定します。ACL に一致するピアの装置は NTP サービスアクセス制御権があります。*ipv4-acl-number* は ACL 番号を示します。標準 IPv4 ACL の設定範囲は 2000～2999 です。拡張 IPv4 ACL の設定範囲は 3000～3999 です。

説明

ntp-service acl コマンドはローカル装置の IPv4 NTP サービスにアクセスするため、ピアの NTP サービスアクセス制御権を設定します。

undo ntp-service acl コマンドは IPv4 NTP サービスの NTP サービスアクセス制御権を削除します。

IPv4 ACL 要求によって NTP アクセスを制御することができます。**peer**、**server**、**synchronization**、**query** の順番でアクセス制御権の制限が高くなります。

装置は以下のルールで IPv4 NTP 要求を処理します。

- IPv4 NTP サービスアクセス制御権が設定されていない場合、**peer** はローカル装置とピアの装置に与えられます。
- ピアの装置の IP アドレスが複数のアクセス制御権のため IPv4 ACL の **permit** 条件に一致する場合、もっとも制限のないアクセス制御権がピアの装置に与えられます。**deny** 条件あるいは IPv4 ACL に一致しない場合、アクセス制御権は与えられません。
- アクセス制御権の IPv4 ACL が作成されていない場合、関連するアクセス制御権は与えられません。
- すべてのアクセス制御権の IPv4 ACL が作成されていない場合、**peer** が与えられます。
- すべてのアクセス制御権の IPv4 ACL がルールに含まれていない場合、アクセス制御権は与えられません。

ntp-service acl コマンドは NTP が動作するシステムで最低限のセキュリティを提供します。より安全な方法は NTP 認証です。

例

サブネット 10.10.0.0/16 のピアの装置がローカル装置にフルアクセスできるように設定します。

<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

関連コマンド

- **ntp-service authentication enable**
- **ntp-service authentication-keyid**
- **ntp-service reliable authentication-keyid**

3.1.5 ntp-service authentication enable

Syntax

ntp-service authentication enable

undo ntp-service authentication enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

ntp-service authentication enable コマンドは NTP 認証を有効にします。

undo ntp-service authentication enable コマンドは NTP 認証を無効にします。

認証された NTP サーバに NTP クライアントが同期できるように、クロック同期のセキュリティが必要なネットワークで NTP 認証を有効にしてください。

NTP サーバを認証するため、認証キーを設定し、トラステッドキーとして指定します。

例

NTP 認証を有効にします。

<Switch> system-view

[Switch] ntp-service authentication enable

関連コマンド

- **ntp-service authentication-keyid**

- **ntp-service reliable authentication-keyid**

3.1.6 ntp-service authentication-keyid

Syntax

ntp-service authentication-keyid *keyid* **authentication-mode md5** { **cipher** | **simple** } *string **

undo ntp-service authentication-keyid *keyid*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

keyid: 認証キーを識別するため、キーID を指定します。設定範囲は 1～4294967295 です。

authentication-mode: 認証アルゴリズムを指定します。

- **md5**: 認証に MD5 アルゴリズムを使用します。

cipher: 暗号テキスト認証キーを設定します。

simple: プレーンテキスト認証キーを設定します。セキュリティのためプレーンテキストで設定された認証キーを含むすべての認証キーは暗号テキストで保存されます。

string: 認証キーを指定します。大文字、小文字を区別します。プレーンテキスト認証キーの設定範囲は 1～32 文字です。暗号テキスト認証キーの設定範囲は 1～73 文字です。

説明

ntp-service authentication-keyid コマンドは NTP 認証キーを設定します。

undo ntp-service authentication-keyid コマンドは NTP 認証キーを削除します。

高いセキュリティが要求されるネットワークでは、NTP 認証は NTP が動作するシステムで有効にする必要があります。この機能はクライアントーサーバキー認証を使用してネットワークのセキュリティを拡張します。認証に失敗した装置にクライアントが同期することを禁止します。

ピアの装置のメッセージのキーID は認証でキーを識別します。

正しい NTP 認証を保証するため、タイムサーバとクライアントでキーID、認証アルゴリズム、キーを同一にしてください。

NTP 認証キーを指定した後、トラステッドキーとして設定するため **ntp-service reliable authentication-keyid** コマンドを使用します。キーを削除した後、キーは自動で非トラステッドキーに変更します。この場合、**undo ntp-service reliable authentication-keyid** コマンドを実行する必要はありません。

このコマンドを使用して最大 128 のキーを設定することができます。

例

キーの ID が 10、キーの値が **BetterKey** のプレーンテキスト MD5 認証キーを設定します。

<Switch> system-view

[Switch] ntp-service authentication enable

[Switch] ntp-service authentication-keyid 10 authentication-mode md5 simple BetterKey

関連コマンド

- **ntp-service authentication enable**
- **ntp-service reliable authentication-keyid**

3.1.7 ntp-service broadcast-client

Syntax

ntp-service broadcast-client

undo ntp-service broadcast-client

デフォルト

装置は NTP アソシエーションモードで動作しません。

View

Interface view

定義済みユーザロール

network-admin

説明

ntp-service broadcast-client コマンドは NTP ブロードキャストクライアントモードで動作するように設定し、現在のインタフェースで NTP ブロードキャストパケットを受信します。

undo ntp-service broadcast-client コマンドは設定を削除します。

コマンドを設定した後、装置は NTP ブロードキャストが送信した NTP メッセージを受信し、受信した NTP メッセージをもとに同期します。

このコマンドによって、装置のインタフェースがブロードキャストクライアントモードで動作するように設定されている場合、アグリゲーショングループにインタフェースを追加することができません。アグリゲーショングループにインタフェースを追加する場合、コマンドの設定を削除してください。

例

NTP ブロードキャストクライアントモードで動作するように設定し、VLAN インタフェース 1 で NTP ブロードキャストパケットを受信します。

<Switch> system-view

[Switch] interface vlan-interface 1

[Switch-Vlan-interface1] ntp-service broadcast-client

関連コマンド

ntp-service broadcast-server

3.1.8 ntp-service broadcast-server

Syntax

ntp-service broadcast-server [**authentication-keyid** *keyid* | **version** *number*] *

undo ntp-service broadcast-server

デフォルト

装置は NTP アソシエーションモードで動作しません。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

authentication-keyid *keyid*: ブロードキャストメッセージをクライアントに送信するために使用するキーID を指定します。設定範囲は 1～4294967295 です。指定しない場合、ローカル装置は NTP 認証が有効のブロードキャストクライアントを同期できません。

version *number*: NTP バージョンを指定します。設定範囲は 1～4 です。デフォルトは 4 です。

説明

ntp-service broadcast-server コマンドは NTP ブロードキャストサーバモードで動作するように設定し、現在のインタフェースで NTP ブロードキャストパケットを送信します。

undo ntp-service broadcast-server コマンドは設定を削除します。

コマンドを設定した後、装置は定期的に NTP メッセージをブロードキャストアドレス 255.255.255.255 に送信します。

このコマンドによって、装置のインタフェースがブロードキャストサーバモードで動作するように設定されている場合、アグリゲーショングループにインタフェースを追加することができません。アグリゲーショングループにインタフェースを追加する場合、コマンドの設定を削除してください。

例

NTP ブロードキャストサーバモードで動作するように設定し、VLAN インタフェース 1 で暗号キーID が 4、NTP のバージョンが 4 の NTP ブロードキャストメッセージを送信します。

<Switch> system-view

[Switch] interface vlan-interface 1

[Switch-Vlan-interface1] ntp-service broadcast-server authentication-keyid 4 version 4

関連コマンド

ntp-service broadcast-client

3.1.9 ntp-service dscp

Syntax

ntp-service dscp *dscp-value*

undo ntp-service dscp

デフォルト

48

View

System view

定義済みユーザロール

network-admin

パラメータ

dscp-value: IPv4 NTP パケットの DSCP を設定します。設定範囲は 0～63 です。

説明

ntp-server dscp コマンドは IPv4 NTP パケットの DSCP を設定します。

undo ntp-server dscp コマンドはデフォルトに戻します。

パケットの優先度を識別するため、DSCP は IPv4 パケットの ToS フィールドに含まれます。

例

IPv4 NTP パケットの DSCP を 30 に設定します。

<Switch> system-view

[Switch] ntp-service dscp 30

3.1.10 ntp-service enable

Syntax

ntp-service enable

undo ntp-service enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

ntp-service enable コマンドは NTP サービスを有効にします。

undo ntp-service enable コマンドは NTP サービスを無効にします。

例

NTP サービスを有効にします。

<Switch> system-view

[Switch] ntp-service enable

3.1.11 ntp-service inbound enable

Syntax

ntp-service inbound enable

undo ntp-service inbound enable

デフォルト

有効

View

Interface view

定義済みユーザロール

network-admin

説明

ntp-service inbound enable コマンドはインタフェースで NTP メッセージの処理を有効にします。

undo ntp-service inbound enable コマンドはデフォルトに戻します。

以下の場合、インタフェースで **undo ntp-service inbound enable** コマンドを実行してください。

- 装置のインタフェースが対応するサブネットで、ピアの装置と同期しません。
- 装置がインタフェースと一致しているサブネットでピアの装置によって同期しません。

例

VLAN インタフェース 1 で NTP メッセージの処理を無効にします。

<Switch> system-view

[Switch] interface vlan-interface 1

[Switch-Vlan-interface1] undo ntp-service inbound enable

3.1.12 ntp-service max-dynamic-sessions

Syntax

ntp-service max-dynamic-sessions *number*

undo ntp-service max-dynamic-sessions

デフォルト

100

View

System view

定義済みユーザロール

network-admin

パラメータ

number: ダイナミック NTP アソシエーションの最大数を設定します。設定範囲は 0～100 です。

説明

ntp-service max-dynamic-sessions コマンドはダイナミック NTP アソシエーションの最大数を設定します。

undo ntp-service max-dynamic-sessions コマンドはデフォルトに戻します。

装置はスタティックアソシエーションとダイナミックアソシエーションを含めて共通で最大 128 のアソシエーションを設定することができます。スタティックアソシエーションは NTP コマンドを使用して手動で作成されたユーザのアソシエーションを参照します。ダイナミックアソシエーションはシステムの動作中に一時的に作成されたアソシエーションです。

ntp-service max-dynamic-sessions コマンドは、ダイナミックアソシエーションが多くのシステムリソースを占有しないように制限させるため、ダイナミックアソシエーションの最大数を制限します。

例

ダイナミック NTP アソシエーションの最大数を 50 に設定します。

<Switch> system-view

[Switch] ntp-service max-dynamic-sessions 50

関連コマンド

display ntp-service sessions

3.1.13 ntp-service multicast-client

Syntax

ntp-service multicast-client [*ip-address*]

undo ntp-service multicast-client [*ip-address*]

デフォルト

装置は NTP アソシエーションモードで動作しません。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

ip-address: マルチキャスト IP アドレスを指定します。デフォルトは 224.0.1.1 です。マルチキャストサーバとクライアントは同一のマルチキャスト IP アドレスに設定する必要があります。

説明

ntp-service multicast-client コマンドは NTP マルチキャストクライアントモードで動作するように設定し、現在のインタフェースで NTP マルチキャストパケットを受信します。

undo ntp-service multicast-client コマンドは設定を削除します。

コマンドを設定した後、装置は宛先アドレスとして指定したマルチキャストアドレスを使用し NTP メッセージを受信します。

このコマンドによって、装置のインタフェースがマルチキャストクライアントモードで動作するように設定されている場合、アグリゲーショングループにインタフェースを追加することができません。アグリゲーショングループにインタフェースを追加する場合、コマンドの設定を削除してください。

例

NTP マルチキャストクライアントモードで動作するように設定します。VLAN インタフェース 1 で NTP マルチキャストパケットを受信し、マルチキャストアドレスを 224.0.1.1 に設定します。

<Switch> system-view

[Switch] interface vlan-interface 1

[Switch-Vlan-interface1] ntp-service multicast-client 224.0.1.1

関連コマンド

ntp-service multicast-server

3.1.14 ntp-service multicast-server

Syntax

ntp-service multicast-server [*ip-address*] [**authentication-keyid** *keyid* | **ttl** *ttl-number* | **version** *number*] *

undo ntp-service multicast-server [*ip-address*]

デフォルト

装置は NTP アソシエーションモードで動作しません。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

ip-address: マルチキャスト IP アドレスを指定します。デフォルトは 224.0.1.1 です。マルチキャストサーバとクライアントは同一のマルチキャスト IP アドレスに設定する必要があります。

authentication-keyid *keyid*: マルチキャストメッセージをクライアントに送信するために使用するキーID を指定します。設定範囲は 1～4294967295 です。指定しない場合、ローカル装置は NTP 認証が有効のマルチキャストクライアントを同期できません。

ttl *ttl-number*: NTP マルチキャストメッセージの TTL を指定します。設定範囲は 1～255 です。デフォルトは 16 です。

version *number*: NTP バージョンを指定します。設定範囲は 1～4 です。デフォルトは 4 です。

説明

ntp-service multicast-server コマンドは NTP マルチキャストサーバモードで動作するように設定し、現在のインタフェースで NTP マルチキャストパケットを送信します。

undo ntp-service multicast-server コマンドは設定を削除します。

コマンドを設定した後、装置は定期的に NTP メッセージをマルチキャストアドレスに送信します。

このコマンドによって、装置のインタフェースがマルチキャストサーバモードで動作するように設定されている場合、アグリゲーショングループにインタフェースを追加することができません。アグリゲーショングループにインタフェースを追加する場合、コマンドの設定を削除してください。

例

NTP マルチキャストサーバモードで動作するように設定し、VLAN インタフェース 1 で暗号キーID が 4､NTP のバージョンが 4 の NTP マルチキャストメッセージをマルチキャストアドレス 224.0.1.1 に送信します。

<Switch> system-view

[Switch] interface vlan-interface 1

[Switch-Vlan-interface1] ntp-service multicast-server 224.0.1.1 version 4 authentication-keyid 4

関連コマンド

ntp-service multicast-client

3.1.15 ntp-service refclock-master

Syntax

ntp-service refclock-master [*ip-address*] [*stratum*]

undo ntp-service refclock-master [*ip-address*]

デフォルト

装置は参照クロックとしてローカルクロックを使用しません。

View

System view

定義済みユーザロール

network-admin

パラメータ

ip-address: ローカルクロックの IP アドレス 127.127.1.u を指定します。ここで u は NTP プロセス ID です。設定範囲は 0～3 です。デフォルトは 127.127.1.0 です。

stratum: ローカルクロックの stratum レベルを指定します。設定範囲は 1～15 です。デフォルトは 8 です。stratum レベルの値が低いほど高いクロックの精度を持ちます。

説明

ntp-service refclock-master コマンドは参照ソースとしてローカルクロックを設定します。

undo ntp-service refclock-master コマンドは設定を削除します。

通常、原子時計などの信頼できるタイムソースから時刻を取得する NTP サーバは、stratum 1 を持ち、ネットワーク内の他の装置に時刻同期を提供するプライマリタイムサーバとして動作します。各サーバの精度は stratum であり、最上位レベル（プライマリサーバ）が 1 つとして割り当てられ、stratum の下位レベル（セカンダリサーバ）が前のレベルより 1 つ大きいレベルとして割り当てられます。

ネットワーク内の装置が信頼できるタイムソースと同期できない場合は、次のタスクを実行できます。

- ネットワークから比較的正確なクロックを持つ装置を選択します。
- 装置のローカルクロックを基準クロックとして使用して、ネットワーク内の他の装置を同期させます。

コマンドは、タイムエラーを回避するために注意して使用してください。コマンドを実行する前に、ローカルクロック時間を正しい値に設定することをお勧めします。

例

ローカルクロックを stratum レベル 2 の参照ソースとして指定します。

<Switch> system-view

[Switch] ntp-service refclock-master 2

3.1.16 ntp-service reliable authentication-keyid

Syntax

ntp-service reliable authentication-keyid *keyid*

undo ntp-service reliable authentication-keyid *keyid*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

keyid: 認証キーを指定します。設定範囲は 1～4294967295 です。

説明

ntp-service reliable authentication-keyid コマンドは作成された認証キーをトラステッドキーとして指定します。

undo ntp-service reliable authentication-keyid コマンドは設定を削除します。

NTP 認証が有効であるとき、クライアントは信頼された認証キーを提供するサーバにのみ同期することができます。

このコマンドを使用する前に、NTP 認証が有効で認証キーが設定されていることを確認してください。キーを削除した後、キーは自動で非トラステッドキーに変更します。この場合、**undo ntp-service reliable authentication-keyid** コマンドを実行する必要はありません。

例

NTP 認証を有効にし、キーの ID が 37、キーの値が **BetterKey** の MD5 アルゴリズムの認証キーを設定します。

<Switch> system-view

[Switch] ntp-service authentication enable

[Switch] ntp-service authentication-keyid 37 authentication-mode md5 simple BetterKey

トラステッドキーとして指定します。

[Switch] ntp-service reliable authentication-keyid 37

関連コマンド

- **ntp-service authentication enable**
- **ntp-service authentication-keyid**

3.1.17 ntp-service source

Syntax

ntp-service source *interface-type interface-number*

undo ntp-service source

デフォルト

NTP メッセージのインタフェースは指定されていません。装置は以下の処理を行います。

- NTP メッセージの送信インタフェースをルーティングテーブルから検索します。
- NTP メッセージの送信元 IP アドレスとして送信インタフェースのプライマリ IP アドレスを使用します。

View

System view

定義済みユーザロール

network-admin

パラメータ

interface-type interface-number: インタフェースのタイプと番号を指定します。

説明

ntp-service source コマンドは NTP メッセージの送信元インタフェースを指定します。

undo ntp-service source コマンドはデフォルトに戻します。

NTP メッセージの送信元インタフェースを指定する場合、装置は NTP メッセージを送信するとき、指定されたインタフェースのプライマリ IP アドレスとして NTP メッセージの送信元 IP アドレスを設定します。

装置が NTP 要求に応答するとき、NTP 応答の送信元 IP アドレスは常に NTP 要求を受信したインタフェースの IP アドレスです。

応答メッセージの宛先アドレスにローカル装置のインタフェースの IP アドレスを使用しない場合、NTP メッセージの送信元インタフェースとして別のインタフェースを指定するため **ntp-service source** コマンドを使用します。

NTP メッセージの送信元インタフェースは以下の方法で指定することができます。

- NTP クライアント/サーバモードでは、**ntp-service unicast-server** コマンドで、NTP メッセージの送信元インタフェースを指定した場合、**ntp-service unicast-server**

コマンドで指定したインタフェースはNTPメッセージの送信元インタフェースとして動作します。

- NTP シンメトリックアクティブ/パッシブモードでは、**ntp-service unicast-peer** コマンドで、NTP メッセージの送信元インタフェースを指定した場合、**ntp-service unicast-peer** コマンドで指定したインタフェースは NTP メッセージの送信元インタフェースとして動作します。
- NTP マルチキャストモードでは、**ntp-service multicast-server** コマンドが設定された場合、マルチキャスト NTP メッセージの送信元インタフェースは、NTP マルチキャストメッセージの送信元インタフェースとして動作します。
- NTP ブロードキャストモードでは、**ntp-service broadcast-server** コマンドが設定された場合、ブロードキャスト NTP メッセージの送信元インタフェースは、NTP ブロードキャストメッセージの送信元インタフェースとして動作します。

指定した送信元インタフェースが down している場合、装置は NTP メッセージを送信しません。

例

NTP メッセージの送信元インタフェースとして VLAN インタフェース 1 を指定します。

<Switch> system-view

[Switch] ntp-service source vlan-interface 1

3.1.18 ntp-service unicast-peer

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*]

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

peer-name: シンメトリックーパッシブピアのホスト名を指定します。設定範囲は 1～253 文字です。大文字、小文字を区別しません。

ip-address: シンメトリックーパッシブピアの IP アドレスを指定します。ブロードキャストアドレス、マルチキャストアドレス、ローカルクロックの IP アドレスでなくユニキャストアドレスにする必要があります。

vpn-instance *vpn-instance-name*: シンメトリックーパッシブピアが属する VPN インスタンスを指定します。大文字小文字を区別し、設定範囲は 1～31 文字です。シンメトリックーパッシブピアがパブリックネットワークの場合、このオプションは指定しません。

authentication-keyid *keyid*: NTP メッセージをピアに送信するために使用するキーの ID を指定します。設定範囲は 1～4294967295 です。指定しない場合、ローカル装置とピアは互いに認証しません。

maxpoll *maxpoll-interval*: 最大ポーリング間隔を指定します。設定範囲は 4～17 です。デフォルトは 6（2^6 秒）です。ポーリング間隔は指定した値のべき乗となります。たとえば 8 を指定した場合、ポーリング間隔は 2^8 秒（256 秒）となります。

minpoll *minpoll-interval*: 最小ポーリング間隔を指定します。設定範囲は 4～17 です。デフォルトは 6（2^6 秒）です。ポーリング間隔は指定した値のべき乗となります。たとえば 4 を指定した場合、ポーリング間隔は 2^4 秒（16 秒）となります。

priority: 同一条件のもとで最初の選択として、*ip-address* あるいは *peer-name* で指定されたピアを指定します。

source *interface-type interface-number*: NTP メッセージの送信元インタフェースを指定します。ローカル装置がピアに NTP メッセージを送信する場合、送信元 IP アドレスはインタフェースのプライマリ IP アドレスです。*interface-type interface-number* はインタフェースのタイプと番号を示します。指定しない場合、出力インタフェースをルーティングテーブルから検索し、NTP メッセージの送信元 IP アドレスとして出力インタフェースのプライマリ IP アドレスを使用します。

version *number*: NTP バージョンを指定します。設定範囲は 1～4 です。デフォルトは 4 です。

説明

ntp-service unicast-peer コマンドは装置のシンメトリックーパッシブピアを指定します。

undo ntp-service unicast-peer コマンドは装置の指定されたシンメトリックーパッシブピアを削除します。

装置のパッシブピアを指定するとき、装置と装置のパッシブピアは互いに同期することができます。クロックが同期されている場合、高い stratum レベルのクロックは、低い stratum レベルのクロックに同期されます。

例

装置のシンメトリックーパッシブピアとして IP アドレス 10.1.1.1 の装置を指定します。NTP バージョンを 4、NTP メッセージの送信元インタフェースを VLAN インタフェース 1 に設定します。

<Switch> system-view

[Switch] ntp-service unicast-peer 10.1.1.1 version 4 source-interface vlan-interface 1

関連コマンド

- **ntp-service authentication enable**
- **ntp-service authentication-keyid**
- **ntp-service reliable authentication-keyid**

3.1.19 ntp-service unicast-server

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*]

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

server-name: NTP サーバのホスト名を指定します。設定範囲は 1～253 文字です。大文字、小文字を区別しません。

ip-address: NTP サーバの IP アドレスを指定します。ブロードキャストアドレス、マルチキャストアドレス、ローカルクロックの IP アドレスでなくユニキャストアドレスにする必要があります。

vpn-instance *vpn-instance-name*: NTP サーバが属する VPN インスタンスを指定します。大文字小文字を区別し、設定範囲は 1～31 文字です。NTP サーバがパブリックネットワークの場合、このオプションは指定しません。

authentication-keyid *keyid*: NTP メッセージを NTP サーバに送信するために使用するキーの ID を指定します。設定範囲は 1～4294967295 です。指定しない場合、ローカル装置と NTP サーバは互いに認証しません。

maxpoll *maxpoll-interval*: 最大ポーリング間隔を指定します。設定範囲は 4～17 です。デフォルトは 6（2^6 秒）です。ポーリング間隔は指定した値のべき乗となります。たとえば 8 を指定した場合、ポーリング間隔は 2^8 秒（256 秒）となります。

minpoll *minpoll-interval*: 最小ポーリング間隔を指定します。設定範囲は 4～17 です。デフォルトは 6（2^6 秒）です。ポーリング間隔は指定した値のべき乗となります。たとえば 4 を指定した場合、ポーリング間隔は 2^4 秒（16 秒）となります。

priority: 同一条件のもとで最初の選択として、NTP サーバを指定します。

source *interface-type interface-number*: NTP メッセージの送信元インタフェースを指定します。ローカル装置が NTP サーバに NTP メッセージを送信する場合、送信元 IP アドレスはインタフェースのプライマリ IP アドレスです。*interface-type interface-number* はインタフェースのタイプと番号を示します。指定しない場合、出力インタフェースをルーティングテーブルから検索し、NTP メッセージの送信元 IP アドレスとして出力インタフェースのプライマリ IP アドレスを使用します。

version *number*: NTP バージョンを指定します。設定範囲は 1～4 です。デフォルトは 4 です。

説明

ntp-service unicast-server コマンドは装置の NTP サーバを指定します。

undo ntp-service unicast-server コマンドは装置から指定された NTP サーバを削除します。

装置の NTP サーバを指定するとき、装置は NTP サーバに同期されますが、NTP サーバは装置に同期されません。

例

装置の NTP サーバ 10.1.1.1 を指定します。NTP バージョンを 4 で動作するように装置を設定します。

<Switch> system-view

[Switch] ntp-service unicast-server 10.1.1.1 version 4

関連コマンド

- **ntp-service authentication enable**
- **ntp-service authentication-keyid**
- **ntp-service reliable authentication-keyid**

目次

このセクションのページは **11-x-x** です。

4 章 PoE 4-1
4.1 PoE 設定コマンド 4-1
4.1.1 apply poe-profile 4-1
4.1.2 apply poe-profile interface 4-2
4.1.3 display poe device 4-3
4.1.4 display poe interface 4-4
4.1.5 display poe interface power 4-8
4.1.6 display poe-profile 4-10
4.1.7 display poe pse 4-11
4.1.8 display poe pse interface 4-13
4.1.9 display poe pse interface power 4-15
4.1.10 display poe-profile interface 4-17
4.1.11 poe enable 4-17
4.1.12 poe high-inrush enable 4-19
4.1.13 poe max-power 4-22
4.1.14 poe pd-description 4-22
4.1.15 poe pd-policy priority 4-23
4.1.16 poe priority 4-24
4.1.17 poe-profile 4-25
4.1.18 poe track 4-27
4.1.19 poe update 4-28
4.1.20 poe utilization-threshold 4-29

4章 PoE

4.1 PoE設定コマンド

4.1.1 apply poe-profile

Syntax

apply poe-profile { **index** *index* | **name** *profile-name* }

undo apply poe-profile { **index** *index* | **name** *profile-name* }

デフォルト

設定なし

View

PI view

定義済みユーザロール

network-admin

パラメータ

index *index*: PoE（Power over Ethernet）プロファイルのインデックス番号を指定します。設定範囲は 1～100 です。

name *profile-name*: PoE プロファイルの名前を指定します。設定範囲は 1～15 文字です。大文字、小文字を区別します。

説明

apply poe-profile コマンドは 1 つの電力インタフェース（PI）に PoE プロファイルを適用します。

undo apply poe-profile コマンドは 1 つの電力インタフェース（PI）から PoE プロファイルの適用を削除します。

例

GigabitEthernet 1/0/1 に PoE プロファイル forIPphone を適用します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] apply poe-profile name forIPphone

関連コマンド

- **apply poe-profile interface**

- **display poe-profile**

4.1.2 apply poe-profile interface

Syntax

apply poe-profile { **index** *index* | **name** *profile-name* } **interface** *interface-range*

undo apply poe-profile { **index** *index* | **name** *profile-name* } **interface** *interface-range*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

index *index*: PoE プロファイルのインデックス番号を指定します。設定範囲は 1～100 です。

name *profile-name*: PoE プロファイルの名前を指定します。設定範囲は 1～15 文字です。大文字、小文字を区別します。

interface-range: Ethernet インタフェースの設定範囲を指定します。形式は *interface-type interface-number* [**to** *interface-type interface-number*] です。*interface-type interface-number* はインタフェースタイプと番号です。開始インタフェース番号は終了インタフェース番号よりも小さい値にする必要があります。指定した範囲内のインタフェースが PoE をサポートしていない場合、PoE プロファイルが適用されたとき、インタフェースは無視されます。

説明

apply poe-profile interface コマンドは電力インタフェース（PI）に PoE プロファイルを適用します。

undo apply poe-profile interface コマンドは電力インタフェース（PI）から PoE プロファイルのアプリケーションを削除します。

例

GigabitEthernet 1/0/1 に PoE プロファイル forIPphone を適用します。

<Switch> system-view

[Switch] apply poe-profile name forIPphone interface gigabitethernet 1/0/1

GigabitEthernet 1/0/2～GigabitEthernet 1/0/6 にインデックス番号 1 の PoE プロファイルを適用します。

<Switch> system-view

[Switch] apply poe-profile index 1 interface gigabitethernet 1/0/2 to gigabitethernet 1/0/6

関連コマンド

- **apply poe-profile**
- **display poe-profile interface**

4.1.3 display poe device

Syntax

display poe device [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

slot *slot-number*: IRF スタックメンバ装置のメンバ ID を指定します。指定しない場合、IRF スタックユニットのすべての PSE の情報を表示します。

説明

display poe device コマンドは PSE（電力供給装置）情報の概要を表示します。

例

PSE 情報の概要を表示します。

<Switch> display poe device

```
Slot  1:
PSE ID    Slot No.  SSlot No. PortNum   MaxPower(W)    State   Model
4         1         0         48        370.0          Off     LSPPSE48A
```

表 4-1 コマンド出力

フィールド	説明
PSE ID	PSEのIDです。
Slot No.	PSEのスロット番号です。

フィールド	説明
SSlot No.	PSEのサブスロット番号です。
PortNum	PSEの電力インタフェースの番号です。
MaxPower(W)	PSEの最大電力です。
State	PSEの状態です。 ● **On**—PSEが電力を供給しています。 ● **Off**— PSEが電力を供給していません。 ● **Faulty**— PSEが故障しています。
Model	PSEモデルです。

4.1.4 display poe interface

Syntax

display poe interface [*interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface-type interface-number: インタフェースのタイプと番号を指定します。指定しない場合、すべての電力インタフェースの電力供給情報を表示します。

説明

display poe interface コマンドは PI（電力インタフェース）の電力供給の情報を表示します。

例

GigabitEthernet 1/0/1 の電力供給の情報を表示します。

<Switch> display poe interface gigabitethernet 1/0/1

```
PoE Status                    : Enabled
Power Priority                : Critical
Oper                          : On
IEEE Class                    : 1
```

```
Detection Status              : Delivering power
Power Mode                    : Signal
Current Power                 : 11592    mW
Average Power                 : 11610    mW
Peak Power                    : 11684    mW
Max Power                     : 15400    mW
Electric Current              : 244      mA
Voltage                       : 51.7     V
PD Description                : IP Phone For Room 101
```

表 4-2 コマンド出力

フィールド	説明
PoE status	PoEの状態です。 ● **Enabled**－有効です。 ● **Disabled**－無効です。
Power Priority	PI（電力インタフェース）の電力供給優先度です。 ● **Critical (highest)**－criticalです（もっとも優先度が高いです）。 ● **High**－highです。 ● **Low**－lowです。
Oper	PIの動作状態です。 ● **Off**—PoEが無効です。 ● **On**—電力が正しくPIに供給されています。 ● **Power-lack**—優先度がcriticalのPIへの保証余力電力が不十分です。 ● **Power-deny**—PSEは供給電力を拒否しています。PD（電力受電装置）が必要な電力が設定された電力よりも高いです。 ● **Power-itself**—PDが別の供給電力を使用しています。 ● **Power-limit**—PDが必要な電力が設定された電力よりも多いですが、PSEは設定された電力にもとづいてPDに電力を供給しています。
IEEE Class	PD（電力受電装置）のクラスです。0、1、2、3、4があります。 PSEがPDクラスをサポートしていない場合、ハイフン（-）を表示します。

フィールド	説明
Detection Status	PIの電力検出状態です。 ● **Disabled**—PoE機能が無効です。 ● **Searching**—PIがPDを検索しています。 ● **Delivering power**—PIがPDに電力を供給しています。 ● **Fault**—試験中に故障が発生しました。 ● **Test**—PIが試験を行っています。 ● **Other fault**—故障によってPSEがアイドル状態に移行しました。 ● **PD disconnected**—PDが接続されていません。
Power Mode	PIの電力給電モードです。 ● **Signal**—装置は信号線を経由して電力を供給しています。 ● **Spare**—装置は予備線を経由して電力を供給しています。
Current Power	PIの現在の供給電力です。PDの消費電力と電力供給ロスが含まれます。
Average Power	PIの平均電力です。
Peak Power	PIのピーク電力です。
Max Power	PIで供給可能な最大電力です。
Electric Current	PIの供給電流です。
Voltage	PIの供給電圧です。
PD Description	PIIに接続されたPDのタイプと説明です。

すべての PI の電力供給情報を表示します。

<Switch> display poe interface

```
Interface    PoE      Priority  CurPower  Oper     IEEE  Detection
                                (W)               Class Status
GE1/0/1        Enabled   Low       4.4      On        1     Delivering Power
GE1/0/2        Enabled   Critical  0.0      On        -     Disabled
GE1/0/3        Enabled   Low       0.0      On        -     Disabled
GE1/0/4        Enabled   Critical  0.0      On        -     Searching
GE1/0/5        Enabled   Low       4.0      On        2     Delivering Power
GE1/0/6        Enabled   Low       0.0      On        -     Disabled
GE1/0/7        Disabled  Low       0.0      Off       -     Fault
  ---  On State Ports: 2; Used: 8.4(W); Remaining: 171.6(W)  ---
```

表 4-3 コマンド出力

フィールド	説明
Interface	PI（電力インタフェース）のインタフェース名です。
PoE	PoEの状態です。 ● **Enabled**－有効です。 ● **Disabled**－無効です。
Priority	PI（電力インタフェース）の電力供給優先度です。 ● **Critical (highest)**－criticalです（もっとも優先度が高いです）。 ● **High**－highです。 ● **Low**－lowです。
CurPower	PIの現在の供給電力です。
Oper	PIの動作状態です。 ● **Off**—PoEが無効です。 ● **On**—電力が正しくPIに供給されています。 ● **Power-lack**—優先度がcriticalのPIへの保証余力電力が不十分です。 ● **Power-deny**—PSEは供給電力を拒否しています。PD（電力受電装置）が必要な電力が設定された電力よりも高いです。 ● **Power-itself**—PDが別の供給電力を使用しています。 ● **Power-limit**—PDが必要な電力が設定された電力よりも多いですが、PSEは設定された電力にもとづいてPDに電力を供給しています。
IEEE Class	PD（電力受電装置）のクラスです。0、1、2、3、4があります。 PSEがPDクラスをサポートしていない場合、ハイフン（-）を表示します。
Detection Status	PIの電力検出状態です。 ● **Disabled**—PoE機能が無効です。 ● **Searching**—PIがPDを検索しています。 ● **Delivering Power**—PIがPDに電力を供給しています。 ● **Fault**—試験中に故障が発生しました。 ● **Test**—PIが試験を行っています。 ● **Other fault**—故障によってPSEがアイドル状態に移行しました。 ● **PD disconnected**—PDが接続されていません。

フィールド	説明
On State Ports	電力を供給しているPIの数です。
Used	現在のPIの消費電力です。
Remaining	システムにおける余力電力です。

4.1.5 display poe interface power

Syntax

display poe interface power [*interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface-type interface-number: インタフェースのタイプと番号を指定します。指定しない場合、すべての PI の電力情報を表示します。

説明

display poe interface power コマンドは PI（電力インタフェース）の電力情報を表示します。

例

GigabitEthernet 1/0/1 の電力情報を表示します。

<Switch> display poe interface power gigabitethernet 1/0/1

```
Interface    Current   Peak      Max       PD Description
             (W)       (W)       (W)
 GE1/0/1       15.0      15.3      30.0      Access Point on Room 509 for Peter
```

すべての PI の電力情報を表示します。

<Switch> display poe interface power

```
Interface    Current   Peak      Max       PD Description
             (W)       (W)       (W)
 GE1/0/1      0.0       0.0       30.0
 GE1/0/2      0.0       0.0       30.0
```

```
GE1/0/3     0.0      0.0      30.0
GE1/0/4     0.0      0.0      30.0       IP Phone in Room 609 for Peter John
GE1/0/5     0.0      0.0      30.0       IP Phone in Room 709 for Jack
GE1/0/6     0.0      0.0      30.0       IP Phone in Room 809 for Alien
GE1/0/7     0.0      0.0      30.0
GE1/0/8     7.6      7.8      30.0
GE1/0/9     0.0      0.0      30.0
GE1/0/10    5.3      5.3      30.0
GE1/0/11    0.0      0.0      30.0
GE1/0/12    0.0      0.0      30.0
GE1/0/13    0.0      0.0      30.0
GE1/0/14    0.0      0.0      30.0
GE1/0/15    0.0      0.0      30.0
GE1/0/16    0.0      0.0      30.0
GE1/0/17    0.0      0.0      30.0
GE1/0/18    0.0      0.0      30.0
GE1/0/19    0.0      0.0      30.0
GE1/0/20    0.0      0.0      30.0
GE1/0/21    0.0      0.0      30.0
GE1/0/22    0.0      0.0      30.0
GE1/0/23    0.0      0.0      30.0
GE1/0/24    0.0      0.0      30.0
  ---  On State Ports: 2; Used: 12.9(W); Remaining: 357.1(W)  ---
```

表 4-4 コマンド出力

フィールド	説明
Interface	PIのインタフェース名です。
CurPower	PIの現在の供給電力です。
PeakPower	PIのピーク電力です。
MaxPower	PIで供給可能な最大電力です。
PD Description	PIに接続されたPDのタイプと説明です。
Ports On	電力を供給しているPIの数です。
Used	現在のPIの消費電力です。
Remaining	システムにおける余力電力です。

4.1.6 display poe-profile

Syntax

display poe-profile [**index** *index* | **name** *profile-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

index *index*: PoE プロファイルのインデックス番号を指定します。設定範囲は 1～100 です。

name *profile-name*: PoE プロファイルの名前を指定します。設定範囲は 1～15 文字です。大文字、小文字を区別します。

説明

display poe-profile コマンドは PoE プロファイルの情報を表示します。

プロファイルを指定しない場合、すべての PoE プロファイルの情報を表示します。

例

すべての PoE プロファイルの情報を表示します。

<Switch> display poe-profile

```
PoE Profile     Index   ApplyNum  Interfaces    Configuration
forIPphone      1       6         GE1/0/1          poe enable
                                  GE1/0/2          poe priority critical
                                  GE1/0/3
                                  GE1/0/4
forAP           2       2         GE1/0/5        poe enable
                                  GE1/0/6         poe max-power 14000
  ---  Total PoE profiles: 3, total ports: 0  ---
```

インデックス番号 1 の PoE プロファイルの情報を表示します。

<Switch> display poe-profile index 1

```
PoE Profile     Index   ApplyNum  Interfaces   Configuration
forIPphone      1       6         GE1/0/1        poe enable
                                  GE1/0/2        poe priority critical
                                  GE1/0/3
                                  GE1/0/4
                                  GE1/0/5
```

```
                                    GE1/0/6
  ---  Total ports: 0  ---
```

表 4-5 コマンド出力

フィールド	説明
PoE Profile	PoEプロファイルの名前です。
Index	PoEプロファイルのインデックス番号です。
ApplyNum	PoEプロファイルが適用されているPIの数です。
Interfaces	PoE設定が適用されているPIのインタフェース名です。
Configuration	PoEプロファイルの設定です。
Total PoE profiles	PoEプロファイルの数です。
Total ports	すべてのPoEプロファイルが適用されているPIの数です。

4.1.7 display poe pse

Syntax

単一 PSE 装置：

display poe pse

複数 PSE 装置：

display poe pse [*pse-id*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

pse-id: PSE（電力供給装置）の ID を指定します。指定しない場合、すべての PSE の情報を表示します。

説明

display poe pse コマンドは PSE の情報を表示します。

例

PSE の詳細情報を表示します。

<Switch> display poe pse

```
PSE ID                        : 4
Slot No.                      : 1
SSlot No.                     : 0
PSE Model                     : LSPPSE8A
PSE Status                    : Enabled
Power Priority                : Low
Current Power                 : 0.0     W
Average Power                 : 0.0     W
Peak Power                    : 0.0     W
Max Power                     : 125.0   W
Remaining Guaranteed Power    : 125.0   W
PSE CPLD Version              : -
PSE Software Version          : 188
PSE Hardware Version          : 0
Legacy PD Detection           : Disabled
Power Utilization Threshold   : 80
PD Power Policy               : Disabled
PD Disconnect-Detection Mode  : DC
```

表 4-6 コマンド出力

フィールド	説明
PSE ID	PSEのIDです。
PSE Status	PSEのPoE状態です。 ● **Enabled**－有効です。 ● **Disabled**－無効です。
Power Priority	PSEの電力優先度です。
Current Power	PSEの現在の電力です。
Average Power	PSEの平均電力です。
Peak Power	PSEのピーク電力です。
Max Power	PSEで供給可能な最大電力です。
Remaining Guaranteed Power	PSEの保証余力電力です。 保証余力電力はPSEで供給可能な電力から、PSEのすべての優先度がcriticalのPIの最大電力の合計を引いた値です。

フィールド	説明
PSE CPLD Version	PSE CPLDのバージョン番号です。
PSE Software Version	PSEソフトウェアバージョンです。
PSE Hardware Version	PSEハードウェアバージョンです。
Legacy PD Detection	IEEE非準拠のPD検出機能の状態です。 ● **Enabled**－有効です。 ● **Disabled**－無効です。
Power Utilization Threshold	PSE電力アラームしきい値です。
PD Power Policy	PD電力管理ポリシーモードです。
PD Disconnect Detection Mode	PD切断検出モードです。

4.1.8 display poe pse interface

Syntax

display poe pse *pse-id* **interface**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

pse *pse-id*: PSE（電力供給装置）の ID を指定します。PSE ID とスロットのマッピングを表示する場合、**display poe device** コマンドを使用します。

説明

display poe pse interface コマンドは PSE のすべての PI の PoE 状態を表示します。

例

PSE 4 のすべての PI の状態を表示します。

<Switch> display poe pse 4 interface

```
 Interface   PoE     Priority  CurPower  Oper        IEEE     Detection
                               (W)                   Class    Status
 GE1/0/1     Enabled  Low       4.4      On           1        Delivering Power
```

```
GE1/0/2    Enabled   Critical  0.0    Power-lack    -       Disabled
GE1/0/3    Enabled   Low       0.0    Power-deny    -       Disabled
GE1/0/4    Enabled   Critical  0.0     On           -       Searching
GE1/0/5    Enabled   Low       4.0     Power-limit  2       Delivering Power
GE1/0/6    Enabled   Low       0.0     Power-itself -       Disabled
GE1/0/7    Disabled  Low       0.0     Off          -       Fault
  --- On State Ports: 2; Used: 8.4(W); Remaining: 171.6 (W) ---
```

表 4-7 コマンド出力

フィールド	説明
Interface	PIのインタフェース名です。
PoE	PIのPoE状態です。 ● **Enabled**－有効です。 ● **Disabled**－無効です。
Priority	PIの優先度です。 ● **Critical (highest)**－criticalです。 ● **High**－highです。 ● **Low**－lowです。
CurPower	PIの現在の電力です。
Oper	PIの動作状態です。 ● **Off**—PoEが無効です。 ● **On**—電力が正しくPIに供給されています。 ● **Power-lack**—優先度がcriticalのPIへの保証余力電力が不十分です。 ● **Power-deny**—PSEは供給電力を拒否しています。PD（電力受電装置）が必要な電力が設定された電力よりも高いです。 ● **Power-itself**—PDが別の供給電力を使用しています。 ● **Power-limit**—PDが必要な電力が設定された電力よりも多いですが、PSEは設定された電力にもとづいてPDに電力を供給しています。
IEEE Class	PD（電力受電装置）のクラスです。0、1、2、3、4があります。 PSEがPDクラスをサポートしていない場合、ハイフン（-）を表示します。

フィールド	説明
Detection Status	PIの電力検出状態です。 • **Disabled**—PoE機能が無効です。 • **Searching**—PIがPDを検索しています。 • **Delivering power**—PIがPDに電力を供給しています。 • **Fault**—試験中に故障が発生しました。 • **Test**—PIが試験を行っています。 • **Other fault**—故障によってPSEがアイドル状態に移行しました。 • **PD disconnected**—PDが接続されていません。
On State Ports	電力を供給しているPIの数です。
Used	PSEのPIの消費電力です。
Remaining	PSEの余力電力です。

4.1.9 display poe pse interface power

Syntax

display poe pse *pse-id* **interface power**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

pse *pse-id*: PSE（電力供給装置）の ID を指定します。PSE ID とスロットのマッピングを表示する場合、**display poe device** コマンドを使用します。

説明

display poe pse interface power コマンドは PSE の PI の情報を表示します。

例

PSE 4 の PI の電力情報を表示します。

<Switch> display poe pse 4 interface power

```
Interface    Current   Peak     Max      PD Description
```

```
            (W)       (W)       (W)
GE1/0/1      0.0       0.0       30.0
GE1/0/2      0.0       0.0       30.0
GE1/0/3      0.0       0.0       30.0
GE1/0/4      0.0       0.0       30.0
GE1/0/5      0.0       0.0       30.0
GE1/0/6      0.0       0.0       30.0
GE1/0/7      0.0       0.0       30.0
GE1/0/8      0.0       0.0       30.0
GE1/0/9      0.0       0.0       30.0
GE1/0/10     0.0       0.0       30.0
GE1/0/11     0.0       0.0       30.0
GE1/0/12     0.0       0.0       30.0
GE1/0/13     0.0       0.0       30.0
GE1/0/14     0.0       0.0       30.0
GE1/0/15     0.0       0.0       30.0
GE1/0/16     0.0       0.0       30.0
GE1/0/17     0.0       0.0       30.0
GE1/0/18     0.0       0.0       30.0
GE1/0/19     0.0       0.0       30.0
GE1/0/20     0.0       0.0       30.0
GE1/0/21     0.0       0.0       30.0
GE1/0/22     0.0       0.0       30.0
GE1/0/23     0.0       0.0       30.0
GE1/0/24     0.0       0.0       30.0
  ---  On State Ports: 0; Used: 0.0(W); Remaining: 370.0(W)  ---
```

表 4-8 コマンド出力

フィールド	説明
Interface	PIのインタフェース名です。
Current	PIの現在の電力です。
Peak	PIのピーク電力です。
Max	PIで供給可能な最大電力です。
PD Description	PIに接続されたPDの説明です。
Ports On	電力を供給しているPIの数です。
Used	すべてのPIの消費電力です。

フィールド	説明
Remaining	PSEの余力電力です。

4.1.10 display poe-profile interface

Syntax

display poe-profile interface *interface-type interface-number*

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface-type interface-number: インタフェースのタイプと番号を指定します。

説明

display poe-profile interface コマンドは PI に適用された PoE プロファイルの情報を表示します。

例

GigabitEthernet 1/0/1 の PoE プロファイルの情報を表示します。

<Switch> display poe-profile interface gigabitethernet 1/0/1

```
PoEProfile     Index   ApplyNum  Interface   Effective configuration
forIPphone      1       6         GE1/0/1     poe enable
                                                poe priority critical
```

Effective configuration フィールドは適用されている設定を表示します。ほかのフィールドの説明は表 4-5 を参照してください。

4.1.11 poe enable

Syntax

poe enable

undo poe enable

デフォルト

有効

View

PI view

PoE profile view

定義済みユーザロール

network-admin

説明

poe enable コマンドは PI（電力インタフェース）で PoE を有効にします。

undo poe enable コマンドは PI で PoE を無効にします。

既に PoE プロファイルが PI に適用されている場合、PoE profile view で PI を設定する前に、PoE プロファイルの適用を削除してください。

PI が設定されている場合、PI view で PI を設定する前に、設定を削除してください。

例

PI view で PoE を有効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] poe enable

PoE profile view で PI の PoE を有効にします。

<Switch> system-view

[Switch] poe-profile abc

[Switch-poe-profile-abc-1] poe enable

関連コマンド

- **display poe interface**
- **poe-profile**

4.1.12 poe high-inrush enable

🕮 **メモ:**

S5100X シリーズの PoE ポートでは、'poe standard'と'poe high-inrush enable'コマンドから一つだけ選択して有効化することができます。同じ装置内で両方のコマンドを使用するためには、以下の手順に従って設定してください。設定手順を守らない場合、意図したモードで稼働されない場合があります。

- high-inrush 機能を、装置で有効にして使用する場合：
  1. 'undo poe high-inrush'を実行して、high-inrush 機能を一時無効化にします。
  2. 'poe high-inrush'を実行して high-inrush 機能を有効化してください。
     1〜2 の手順で設定を行ったとき、全てのポートが high-inrush 機能が有効の状態で稼働します。
  3. 各ポートで、'poe standard'の設定を行います。
     802.3 at モードで使用するポートでは、high-inrush 機能は有効となります。
     802.3 bt モードで使用するポートでは、high-inrush 機能は無効となります。

- high-inrush 機能を、装置で無効にして使用する場合：
  1. 'undo poe high-inrush'を実行して、high-inrush 機能を無効化にします。
     'undo poe high-inrush'の実行により、全てのポートが'802.3 bt'モードで稼働します。
  2. 各ポートで、'poe standard'の設定を行います。
     '802.3 at'モードで使用するポートは'poe standard at'の設定が必要です。
     '802.3 bt'モードで使用するポートは、1 の手順ですでに稼働はしていますが、'poe standard bt'の設定は明示的に必要です。

●手順例 1
GigabitEthernet1/0/1：poe standard at
GigabitEthernet 1/0/2：poe standard bt
その他のポート：poe high-inrush enable を無効化

デフォルトから上記の設定を行う場合は以下の手順で設定します。

(1)poe-high-inrush enable を無効化します。
<Switch> system-view
[Switch] undo poe high-inrush enable pse 4

(2) Ten-GigabitEthernet1/0/1 に poe standard at を設定します。
<Switch> interface GigabitEthernet1/0/1
[Switch-Ten-GigabitEthernet1/0/1] poe standard at

(3) GigabitEthernet 1/0/2 に poe standard bt を設定します。
<Switch> interface Ten-GigabitEthernet1/0/2

[Switch-GigabitEthernet1/0/1] poe standard bt

- 手順例 2

GigabitEthernet1/0/1：poe standard at
その他のポート：poe high-inrush enable を無効化

上記の設定を行う場合は以下の手順で設定します。
また、本設定は前提条件として、GigabitEthernet1/0/1 に poe standard at を設定しています。

前提条件
[Switch-GigabitEthernet1/0/1] poe standard at

(1) poe-high-inrush enable を適用した後に、無効化します。
<Switch> system-view
[Switch] poe high-inrush enable pse4
[Switch] undo poe high-inrush enable pse 4

(2) GigabitEthernet1/0/1 に poe standard at を再設定します。
<Switch> interface GigabitEthernet1/0/1
[Switch-GigabitEthernet1/0/1] poe standard at

- 手順例 3

GigabitEthernet1/0/1：poe standard at
-GigabitEthernet 1/0/2：poe standard bt
その他のポート：poe high-inrush enable を有効化

上記の設定を行う場合は以下の手順で設定します。

(1) poe-high-inrush enable を無効化します。
<Switch> system-view
[Switch] undo poe high-inrush enable pse 4

(2)poe-high-inrush enable を有効化します。
<Switch> system-view
[Switch] poe high-inrush enable pse 4

(3) GigabitEthernet1/0/1 に poe standard at を設定します。
<Switch> interface GigabitEthernet1/0/1
[Switch-GigabitEthernet1/0/1] poe standard at

(4) GigabitEthernet 1/0/2 に poe standard bt を設定します。
<Switch> interface Ten-GigabitEthernet1/0/2

[Switch-GigabitEthernet1/0/1] poe standard bt

Syntax

poe high-inrush enable pse *pse-id*

undo poe high-inrush enable pse *pse-id*

デフォルト

無効

View

Interface view

定義済みユーザロール

network-admin

パラメータ

pse *pse-id*: ID で PSE を指定します。

説明

poe high-inrush enable コマンドは PD の突入電流を許可します。

undo poe high-inrush enable コマンドは PD の突入電流を無効にします。

PD の起動時に突入電流が発生し、PSE の自己保護を引き起こすことがあります。その結果、PSE は PD への電力供給を停止します。PD への電源供給を継続するには、PD が消費する突入電流を許可するようにこの機能を設定します。このコマンドの設定を変更する場合は注意してください。

IEEE 802.3af および IEEE 802.3at は、突入電流の仕様を定義します。この装置は、突入電流の IEEE 802.3af および IEEE 802.3at 仕様をサポートします。

本コマンドを設定している場合は 30W で給電されます。

例

PD による突入電流を許可します。

<Switch> system-view

[Switch] interface GigabitEthernet 1/0/1

[Switch-GigabitEthernet1/0/1] interface poe high-inrush enable pse 4

関連コマンド

- **display poe interface**
- **display poe pse**

4.1.13 poe max-power

Syntax

poe max-power *max-power*

undo poe max-power

デフォルト

30000 ミリ W

View

PI view

PoE profile view

定義済みユーザロール

network-admin

パラメータ

max-power: 最大電力を指定します。設定範囲は 1000～30000 ミリ W です。

説明

poe max-power コマンドは PI の最大電力を設定します。

undo poe max-power コマンドはデフォルトに戻します。

例

PI view で PI の最大電力を 12000 ミリ W に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] poe max-power 12000

PoE profile view で PI の最大電力を 12000 ミリ W に設定します。

<Switch> system-view

[Switch] poe-profile abc

[Switch-poe-profile-abc-1] poe max-power 12000

4.1.14 poe pd-description

Syntax

poe pd-description *text*

undo poe pd-description

デフォルト

設定なし

View

PI view

定義済みユーザロール

network-admin

パラメータ

text: PI に接続された PD の説明を指定します。設定範囲は 1～80 文字です。大文字、小文字を区別します。

説明

poe pd-description コマンドは PI に接続された PD の説明を設定します。

undo poe pd-description コマンドはデフォルトに戻します。

例

PI に接続された PD の説明を IP Phone for Room 101 に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] poe pd-description IP Phone For Room 101

4.1.15 poe pd-policy priority

Syntax

poe pd-policy priority

undo poe pd-policy priority

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

poe pd-policy priority コマンドは PI の電力管理を有効にします。

undo poe pd-policy priority コマンドはデフォルトに戻します。

PSE が過負荷の状態で、PI の電力管理が無効である場合、PSE は新しい PD に電力を供給しません。

PSE が過負荷の状態で、PI の電力管理が有効である場合、PSE は PI の優先度にもとづいて新しい PD に電力を割り当てます。

例

PI の電力管理を有効にします。

<Switch> system-view

[Switch] poe pd-policy priority

関連コマンド

poe priority

4.1.16 poe priority

Syntax

poe priority { **critical** | **high** | **low** }

undo poe priority

デフォルト

low

View

PI view

PoE profile view

定義済みユーザロール

network-admin

パラメータ

critical: 電力供給の優先度を critical に指定します。優先度が critical の PI は保証されたモードで動作します。優先度が critical の PI に接続された PD は最初に電力が供給されます。

high: 電力供給の優先度を high に指定します。

low: 電力供給の優先度を low に指定します。

説明

poe priority コマンドは PI の電力供給の優先度を設定します。

undo poe priority コマンドはデフォルトに戻します。

PoE 電力が不十分であるとき、電力は最初に高い優先度の PI に供給します。

同一の電力供給の優先度を持つ PI がある場合、もっとも小さい ID の PI に最初に電力が供給されます。

既に PoE プロファイルが PI に適用されている場合、PoE profile view で PI を設定する前に、PoE プロファイルの適用を削除してください。

PI が設定されている場合、PI view で PI を設定する前に、設定を削除してください。

例

PI view で PI の電力供給の優先度を critical に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] poe priority critical

PoE profile view で PI の電力供給の優先度を critical に設定します。

<Switch> system-view

[Switch] poe-profile abc

[Switch-poe-profile-abc-1] poe priority critical

[Switch-poe-profile-abc-1] quit

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] apply poe-profile name abc

関連コマンド

poe pd-policy priority

4.1.17 poe-profile

Syntax

poe-profile *profile-name* [*index*]

undo poe-profile { **index** *index* | **name** *profile-name* }

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

profile-name: PoE プロファイルの名前を指定します。設定範囲は 1～15 文字です。大文字、小文字を区別します。PoE 設定ファイル名は英字から始まり、以下の予約語を含むことができません。undo、all、name、interface、user、poe、disable、max-power、mode、priority、enable

index: PoE プロファイルのインデックス番号を指定します。設定範囲は 1～100 です。

説明

poe-profile コマンドは PoE プロファイルを作成し、PoE profile view に移行します。既に PoE プロファイルが存在する場合、その view に移行します。

undo poe-profile コマンドは指定した PoE プロファイルを削除します。

バッチで PI を設定する場合、PoE プロファイルを使用します。

PoE プロファイルのインデックスを指定しない場合、システムは自動的にインデックスを PoE プロファイルに割り当てます。自動的に割り当てるインデックス番号は 1 から開始します。

既に PoE プロファイルが PI に適用されている場合、PoE profile view で PI を設定する前に、**undo apply poe-profile** コマンドで PoE プロファイルの適用を削除してください。

例

PoE プロファイルを作成します。PoE プロファイル名を abc、インデックス番号を 3 に指定します。

<Switch> system-view

[Switch] poe-profile abc 3

[Switch-poe-profile-abc-3]

PoE プロファイルを作成します。PoE プロファイル名を def に指定し、インデックス番号を指定しません。

<Switch> system-view

[Switch] poe-profile def

[Switch-poe-profile-def-1]

関連コマンド

- **apply poe-profile**
- **poe enable**
- **poe max-power**
- **poe priority**

4.1.18 poe track

🕮 メモ：

poe track は、Version 7.4.61 を含む以降のソフトウェアからサポートしています。

Syntax

poe track *track-entry-number* **action** { **alarm** | **alarm-reboot-pd** }

undo poe track

デフォルト

PI は Track エントリに関連付けられていません。

View

PI view

定義済みユーザロール

network-admin

パラメータ

track-entry-number:トラックのエントリ ID を 1 から 1024 の範囲で指定します。

action: トラックのエントリ状態が positive から negative に変化したときに実行するアクションを指定します。

alarm: SNMP 通知とログを出力します。

alarm-reboot-pd: SNMP 通知とログを出力し、PI に接続されている PD を再起動します。

説明

poe track コマンドは、トラックエントリを使用してデバイスと PD 間のリンクステータスを監視し、トラックエントリの状態が positive から negative に変化したときに指定されたアクションを行います。Track の詳細については、詳細はセクション 9 *高可用性 オペレーションマニュアル*の”*Track*”を参照してください。

PI ビューでこのコマンドを複数回設定すると、最新の設定が有効になります。

例

#GigabitEthernet 1/0/1 をトラックエントリ 1 に関連付け、トラックエントリの状態が正から負に変化したときにシステムが SNMP 通知を出力してログを記録できるようにします。

<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] poe track 1 action alarm

4.1.19 poe update

Syntax

poe update { **full** | **refresh** } *filename* [**pse** *pse-id*]

View

System view

定義済みユーザロール

network-admin

パラメータ

full: full モードで PSE ファームウェアをアップグレードします。

refresh: refresh モードで PSE ファームウェアをアップグレードします。

filename: アップグレードファイルの名前を指定します。設定範囲は 1～64 文字です。大文字、小文字を区別します。指定したファイルは装置のファイルシステムのルートディレクトリに格納する必要があります。

pse *pse-id*: PSE（電力供給装置）の ID を指定します。PSE を指定しない場合、IRF スタックユニットのすべてのメンバ装置の PSE をアップグレードします。

説明

poe update コマンドは装置が動作中のときに PSE ファームウェアをアップグレードします。

一般的に、refresh モードでファームウェアをアップグレードすることができます。以下の状況のときのみ、full モードでファームウェアをアップグレードすることができます。

- **Refresh モード**－PSE ファームウェアを削除しないでアップグレードします。通常の場合、Refresh モードで PSE ファームウェアをアップグレードしてください。
- **Full モード**－現在の PSE ファームウェアを削除し、新しい PSE ファームウェアをアップグレードします。現在の PSE ファームウェアに不備があり、PSE コマンドを実行できない場合、Full モードで PSE ファームウェアをアップグレードしてください。

例

サービス中の PSE 4 のファームウェアをアップグレードします。

<Switch> system-view

[Switch] poe update refresh POE-168.bin pse 4

4.1.20 poe utilization-threshold

Syntax

poe utilization-threshold *value* **pse** *pse-id*

undo poe utilization-threshold pse *pse-id*

デフォルト

80%

View

System view

定義済みユーザロール

network-admin

パラメータ

value: 電力アラームのしきい値を指定します。設定範囲は 1～99%です。

pse *pse-id*: PSE の ID を指定します。

説明

poe utilization-threshold コマンドは PSE の電力アラームのしきい値を設定します。

undo poe utilization-threshold コマンドは PSE の電力アラームのしきい値をデフォルトに戻します。

PSE 電力の使用率がしきい値を越えたあるいは下回った場合、システムは超過あるいは下回った都度、SNMP notification メッセージを送信します。詳細はオペレーションマニュアルのセクション 11 *システム管理*”*SNMP*”を参照してください。

例

PSE 4 の電力アラームのしきい値を 90%に設定します。

<Switch> system-view

[Switch] poe utilization-threshold 90 pse 4

目次

このセクションのページは **11-x-x** です。

5 章 SNMP 5-1
5.1 SNMP 設定コマンド 5-1
5.1.1 display snmp-agent community 5-1
5.1.2 display snmp-agent group 5-3
5.1.3 display snmp-agent local-engineid 5-5
5.1.4 display snmp-agent mib-view 5-5
5.1.5 display snmp-agent statistics 5-7
5.1.6 display snmp-agent sys-info 5-10
5.1.7 display snmp-agent trap queue 5-10
5.1.8 display snmp-agent trap-list 5-11
5.1.9 display snmp-agent usm-user 5-12
5.1.10 enable snmp trap updown 5-14
5.1.11 snmp-agent 5-16
5.1.12 snmp-agent { inform | trap } source 5-16
5.1.13 snmp-agent calculate-password 5-18
5.1.14 snmp-agent community 5-19
5.1.15 snmp-agent group 5-22
5.1.16 snmp-agent local-engineid 5-26
5.1.17 snmp-agent log 5-27
5.1.18 snmp-agent mib-view 5-28
5.1.19 snmp-agent packet max-size 5-29
5.1.20 snmp-agent packet response dscp 5-30
5.1.21 snmp-agent sys-info contact 5-31
5.1.22 snmp-agent sys-info location 5-32
5.1.23 snmp-agent sys-info version 5-33
5.1.24 snmp-agent target-host 5-34
5.1.25 snmp-agent trap enable 5-36
5.1.26 snmp-agent trap if-mib link extended 5-37
5.1.27 snmp-agent trap life 5-38
5.1.28 snmp-agent trap log 5-39
5.1.29 snmp-agent trap queue-size 5-39
5.1.30 snmp-agent usm-user { v1 | v2c } 5-40
5.1.31 snmp-agent usm-user v3 5-43

5章 SNMP

SNMP エージェントはリンク状態の変更、ユーザのログイン、ログアウトのような重要なイベントを NMS に知らせるため、notification（トラップと inform）を送信します。特に指定しない限り、コマンドラインの trap キーワードは trap と inform を含みます。

5.1 SNMP設定コマンド

5.1.1 display snmp-agent community

Syntax

display snmp-agent community [**read** | **write**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

read: 読み出し専用コミュニティ情報を表示します。

write: 読み出し、書き込みコミュニティ情報を表示します。

説明

display snmp-agent community コマンドは SNMPv1 あるいは SNMPv2c のコミュニティ情報を表示します。

パラメータを指定しない場合、作成されたすべての SNMPv1 あるいは SNMPv2c のコミュニティ情報を表示します。

このコマンドは以下の方法で作成された SNMPv1、SNMPv2c コミュニティを表示します。

- **snmp-agent community** コマンドで作成されたコミュニティ
- 既存の SNMP グループに割り当てられた SNMPv1 と SNMPv2c のユーザ用に自動で作成されたコミュニティ

例

すべての SNMPv1 あるいは SNMPv2c のコミュニティ情報を表示します。

<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
```

表 5-1 コマンド出力

フィールド	説明
Community name	**snmp-agent community**コマンドで作成されたコミュニティ名あるいは**snmp-agent usm-user** { **v1** | **v2c** }コマンドで作成されたユーザ名を表示します。
Group name	SNMPグループ名です。 ● **snmp-agent community**コミュニティがコマンドで作成された場合、グループ名はコミュニティ名と同一です。 ● **snmp-agent usm-user** { **v1** | **v2c** }コミュニティがコマンドで作成された場合、ユーザがあるグループ名が表示されます。
Role name	コミュニティのユーザロールです。 コミュニティがRBACモードの**snmp-agent community**コマンドで作成された場合、ユーザロールはコミュニティ名と結合できます。
ACL	ACL番号です。 このフィールドはSNMPv1あるいはSNMPv2cコミュニティで、ACLが指定されたときのみ表示されます。ACL名フィールドと一緒に表示されません。
ACL name	ACL名です。 このフィールドはSNMPv1あるいはSNMPv2cコミュニティで、ACL名が指定されたときのみ表示されます。ACLフィールドと一緒に表示されません。

フィールド	説明
Storage-type	記憶媒体のタイプです。 • **volatile**—システムが再起動したときに設定が失われます。 • **nonVolatile**—システムが再起動しても設定は失われません。 • **permanent**—システムが再起動しても設定は失われません。変更することができますが、削除することができません。 • **readOnly**—システムが再起動しても設定は失われません。変更あるいは削除することができません。 • **other**—他の記憶媒体のタイプです。
Context name	SNMPの内容です。 • SNMPコミュニティとSNMPの内容間のマッピングが設定されている場合、SNMPの内容が表示されます。 • SNMPコミュニティとSNMPの内容間のマッピングが設定されていない場合、表示されません。

関連コマンド

- **snmp-agent community**
- **snmp-agent usm-user { v1 | v2c }**

5.1.2 display snmp-agent group

Syntax

display snmp-agent group [*group-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

group-name: SNMPv1、SNMPv2c、SNMPv3 グループ名を指定します。設定範囲は 1～32 です。大文字、小文字を区別します。指定しない場合、すべての SNMP グループの情報を表示します。

説明

display snmp-agent group コマンドは SNMP グループの情報を表示します。

例

すべての SNMP グループの情報を表示します。

<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
```

表 5-2 コマンド出力

フィールド	説明
Group name	SNMPグループ名です。
Security model	SNMPグループのセキュリティモデルです。 ● **authPriv**—プライバシーセキュリティありの認証です。 ● **authNoPriv**—プライバシーセキュリティなしの認証です。 ● **noAuthNoPriv**—認証なし、プライバシーセキュリティなしです。 SNMPv1あるいはSNMPv2cグループのセキュリティモデルはnoAuthNoPrivのみです。
Readview	SNMPグループにアクセス可能な読み込み専用のMIB viewです。
Writeview	SNMPグループにアクセス可能な書き込みのMIB viewです。
Notifyview	SNMP viewの通知MIB viewです。グループのSNMPユーザは通知MIB viewのノードの通知を送信できます。
Storage-type	記憶媒体のタイプです。**volatile**、**nonvolatile**、**permanent**、**readOnly**、**other**が含まれます。（表 5-1を参照してください。）
ACL	ACL番号です。 このフィールドはSNMPグループで、ACLが指定されたときのみ表示されます。ACL名フィールドと一緒に表示されません。
ACL name	ACL名です。 このフィールドはSNMPグループで、ACL名が指定されたときのみ表示されます。ACLフィールドと一緒に表示されません。

関連コマンド

snmp-agent group

5.1.3 display snmp-agent local-engineid

Syntax

display snmp-agent local-engineid

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display snmp-agent local-engineid コマンドはローカル SNMP エンジン ID を表示します。

各 SNMP エージェントはメッセージの送受信、メッセージの認証、暗号化、管理されたオブジェクトへのアクセス制御のサービスを提供するため 1 つの SNMP エンジンがあります。

ローカル SNMP エンジン ID は SNMP ドメインの SNMP エージェントの SNMP エンジンを固有に識別します。

例

ローカル SNMP エンジン ID を表示します。

<Switch> display snmp-agent local-engineid

```
SNMP local engine ID: 800063A2800084E52BED7900000001
```

関連コマンド

snmp-agent local-engineid

5.1.4 display snmp-agent mib-view

Syntax

display snmp-agent mib-view [**exclude** | **include** | **viewname** *view-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

exclude: MIB view から除外されたサブツリーを表示します。

include: MIB view から含まれるサブツリーを表示します。

viewname *view-name*: 指定された MIB view の情報を表示します。設定範囲は 1～32 文字です。大文字、小文字を区別します。

説明

display snmp-agent mib-view コマンドは MIB view を表示します。

パラメータを指定しない場合、すべての MIB view を表示します。

例

すべての MIB view を表示します。

<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 はデフォルトの MIB view です。出力は **snmpUsmMIB**、**snmpVacmMIB**、**snmpModules.18** の MIB オブジェクトを除いて **iso** サブツリーのすべての MIB オブジェクトがアクセス可能です。

表 5-3 コマンド出力

フィールド	説明
View name	MIB view名です。
MIB Subtree	MIB viewで扱われるMIBサブツリーです。
Subtree mask	MIBサブツリーマスクです。
Storage-type	サブツリーが記録される記憶媒体（表 5-1を参照してください）のタイプです。
View Type	MIB viewのMIBサブツリーのアクセス権です。 • **Included**—MIBサブツリーのすべてのオブジェクトがMIB viewにアクセス可能です。 • **Excluded**—MIBサブツリーのすべてのオブジェクトがMIB viewにアクセス可能できません。
View status	MIB viewの状態です。 • **active**—MIB viewが有効です。 • **inactive**— MIB viewが無効です。MIB viewのオブジェクトはアクセスできませんがnotificationを送信することができます。

関連コマンド

snmp-agent mib-view

5.1.5 display snmp-agent statistics

Syntax

display snmp-agent statistics

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display snmp-agent statistics コマンドは SNMP メッセージの統計情報を表示します。

例

SNMP メッセージの統計情報を表示します。

<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.
```

表 5-4 コマンド出力

フィールド	説明
messages delivered to the SNMP entity	SNMPエージェントが受信したメッセージ数です。
messages were for an unsupported version	SNMPエージェントのバージョンでサポートされていないメッセージ数です。

フィールド	説明
messages used an unknown SNMP community name	不明なSNMPコミュニティ名が使用されたメッセージ数です。
messages represented an illegal operation for the community supplied	コミュニティを実行する権限がないオペレーションが運ばれたメッセージ数です。
ASN.1 or BER errors in the process of decoding	復号化の間にASN.1あるいはBERエラーがあるメッセージ数です。
messages passed from the SNMP entity	SNMPエージェントによって送信されたメッセージ数です。
SNMP PDUs had badValue error-status	BadValueエラーのPDU数です。
SNMP PDUs had genErr error-status	genErrエラーのPDU数です。
SNMP PDUs had noSuchName error-status	NoSuchNameエラーのPDU数です。
SNMP PDUs had tooBig error-status	TooBigエラーのPDU数です。（最大パケットサイズが1500バイトです）
MIB objects retrieved successfully	正常に読み込まれたMIBオブジェクト数です。
MIB objects altered successfully	正常に書き込まれたMIBオブジェクト数です。
GetRequest-PDU accepted and processed	読み込み、処理されたGetRequest要求の数です。
GetNextRequest-PDU accepted and processed	読み込み、処理されたgetNext要求の数です。
GetBulkRequest-PDU accepted and processed	読み込み、処理されたgetBulk要求の数です。
GetResponse-PDU accepted and processed	読み込み、処理されたget応答の数です。
SetRequest-PDU accepted and processed	読み込み、処理されたset要求の数です。
Trap PDUs accepted and processed	読み込み、処理された通知の数です。
alternate Response Class PDUs dropped silently	廃棄された応答パケットの数です。
forwarded Confirmed Class PDUs dropped silently	廃棄された転送パケットの数です。

5.1.6 display snmp-agent sys-info

Syntax

display snmp-agent sys-info [**contact** | **location** | **version**] *

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

contact: システム連絡先を表示します。

location: 装置の所在地を表示します。

version: SNMP エージェントのバージョンを表示します。

説明

display snmp-agent sys-info コマンドは SNMP エージェントシステムの情報を表示します。

パラメータを指定しない場合、すべての SNMP エージェントシステムの情報を表示します。

例

すべての SNMP エージェントシステムの情報を表示します。

<Switch> display snmp-agent sys-info

```
The contact information of the agent:

The location information of the agent:

The SNMP version of the agent:
   SNMPv3
```

関連コマンド

snmp-agent sys-info

5.1.7 display snmp-agent trap queue

Syntax

display snmp-agent trap queue

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display snmp-agent trap queue コマンドは trap キューの基本情報を表示します。

例

trap キューの設定と使用状態を表示します。

<Switch> display snmp-agent trap queue

```
Queue size: 100
Message number: 6
```

関連コマンド

- **snmp-agent trap life**
- **snmp-agent trap queue-size**

5.1.8 display snmp-agent trap-list

Syntax

display snmp-agent trap-list

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display snmp-agent trap-list コマンドは SNMP 通知（notification）を作成できるモジュールの SNMP 通知機能の状態（**enable** あるいは **disable**）を表示します。

モジュールのサブモジュールで、サブモジュールで SNMP 通知機能が有効である場合、SNMP 通知機能が有効であることを表示します。

モジュールで SNMP 通知機能をサポートしているかどうか確認する場合、**snmp-agent trap enable ?**コマンドを使用します。

display snmp-agent trap-list コマンドの出力は **snmp-agent trap enable** コマンドの設定とモジュールの設定によって異なります。

例

モジュールの SNMP 通知機能の状態を表示します。

<Switch> display snmp-agent trap-list

```
arp notification is disabled.
configuration notification is enabled.
mac-address notification is enabled.
radius notification is disabled.
standard notification is enabled.
syslog notification is disabled.
system notification is enabled.

Enabled notifications: 4; Disabled notifications: 3
```

関連コマンド

snmp-agent trap enable

5.1.9 display snmp-agent usm-user

Syntax

display snmp-agent usm-user [**engineid** *engineid* | **group** *group-name* | **username** *user-name*] *

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

engineid *engineid*: SNMP エンジン ID の SNMPv3 ユーザ情報を表示します。SNMP エンジン ID は *engineid* で識別されます。*engineid* は大文字、小文字を区別しません。SNMPv3 ユーザが作成されているとき、システムはローカル SNMP エンティティのエンジン ID を記録します。エンジン ID が変更されるとユーザは無効になり、記録されたエンジン ID が復元されるとユーザが有効になります。

group *group-name*: 指定した SNMP グループ名の SNMPv3 ユーザ情報を表示します。グループ名は大文字、小文字を区別します。

username *user-name*: 指定した SNMPv3 ユーザの情報を表示します。ユーザ名は大文字、小文字を区別します。

説明

display snmp-agent usm-user コマンドは SNMPv3 ユーザ情報を表示します。

このコマンドは **snmp-agent usm-user v3** コマンドを使用して作成された SNMPv3 ユーザのみ表示します。**snmp-agent usm-user** { **v1** | **v2c** }コマンドを使用して作成された SNMPv1 あるいは SNMPv2c ユーザを表示する場合、**display snmp-agent community** コマンドを使用します。

例

すべての SNMPv3 ユーザ情報を表示します。

<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
```

表 5-5 コマンド出力

フィールド	説明
Username	SNMPユーザ名です。
Group name	SNMPグループ名です。
Role name	SNMPユーザロール名です。
Engine ID	SNMPユーザが作成されたとき、SNMPエージェントが使用したエンジンIDです。
Storage-type	記憶媒体のタイプです。 • **volatile** • **nonVolatile** • **permanent** • **readOnly** • **other** 記憶媒体の詳細は表 5-1を参照してください。
UserStatus	SNMPユーザの状態です。 • **active**—SNMPユーザは動作しています。 • **notInService**—SNMPユーザは正常に設定されていますが、動作していません。 • **notReady**—SNMPユーザの設定が不完全です。 • **other**—他の状態です。
ACL	ACL番号です。 このフィールドはSNMPv3ユーザで、ACLが指定されたときのみ表示されます。ACL名フィールドと一緒に表示されません。
ACL name	ACL名です。 このフィールドはSNMPv3ユーザで、ACL名が指定されたときのみ表示されます。ACLフィールドと一緒に表示されません。

関連コマンド

snmp-agent usm-user v3

5.1.10 enable snmp trap updown

Syntax

enable snmp trap updown

undo enable snmp trap updown

デフォルト

有効

View

Interface view

定義済みユーザロール

network-admin

説明

enable snmp trap updown コマンドはインタフェースのリンク状態の通知を有効にします。

undo enable snmp trap updown コマンドはインタフェースのリンク状態の通知を無効にします。

状態が変更したとき、インタフェースで linkUp/linkDown の通知を作成する場合、**snmp-agent trap enable standard** [**linkdown** | **linkup**] *コマンドを使用してグローバルに linkUp/linkDown 通知機能を有効にする必要があります。

例

GigabitEthernet 1/0/1 で linkUp/linkDown の SNMP trap を 10.1.1.1 に送信することを有効にします。コミュニティ名は **public** を使用します。

<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

関連コマンド

- **snmp-agent target-host**
- **snmp-agent trap enable**

5.1.11 snmp-agent

🕮 メモ：

- デフォルトコンフィグが設定された装置で **snmp-agent** コマンドを設定すると、**snmp-agent local-engineid** コマンドと **snmp-agent sys-info version v3** コマンドが自動的に追加されます。
- snmp の設定を変更した装置を **undo snmp-agent** コマンドによって無効した後、再度 snmp を有効にすると **undo** コマンド実行前の設定状態に戻ります。

Syntax

snmp-agent

undo snmp-agent

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

snmp-agent コマンドは SNMP エージェントを有効にします。

undo snmp-agent コマンドは SNMP エージェントを無効にします。

snmp-agent calculate-password を除く **snmp-agent** で始まるコマンドを実行するとき、SNMP エージェントは自動で有効になります。

例

SNMP エージェントを有効にします。

<Switch> system-view

[Switch] snmp-agent

5.1.12 snmp-agent { inform | trap } source

Syntax

snmp-agent { **inform** | **trap** } **source** *interface-type interface-number*

undo snmp-agent { **inform** | **trap** } **source**

デフォルト

SNMP エージェントはルートの送信インタフェースの IP アドレスを使用します。

View

System view

定義済みユーザロール

network-admin

パラメータ

inform: inform を指定します。

trap: trap を指定します。

interface-type interface-number: インタフェースのタイプと番号を指定します。

説明

snmp-agent { **inform** | **trap** } **source** コマンドは SNMP エージェントによって送信される inform あるいは trap の送信元 IP アドレスを指定します。

undo snmp-agent { **inform** | **trap** } **source** コマンドはデフォルトに戻します。

snmp-agent source コマンドは、送信インタフェースに関わらず、SNMP エージェントがすべての SNMP の inform あるいは trap の送信元 IP アドレスとして、インタフェースのプライマリ IP アドレスを使用することを有効にします。NMS は SNMP エージェントによって送信されたすべての inform あるいは trap をフィルタするため、この IP アドレスを使用します。

指定されたインタフェースが作成され、有効な IP アドレスが割り当てられていることを確認してください。インタフェースが作成されていない場合、設定は適用されません。指定したインタフェースに有効な IP アドレスが割り当てられたのち、設定が適用されます。

例

SNMP trap の送信元アドレスとして、GigabitEthernet 1/0/1 のプライマリ IP アドレスを設定します。

<Switch> system-view

[Switch] snmp-agent trap source gigabitethernet 1/0/1

SNMP inform の送信元アドレスとして、GigabitEthernet 1/0/2 のプライマリ IP アドレスを設定します。

<Switch> system-view

[Switch] snmp-agent inform source gigabitethernet 1/0/2

関連コマンド

- **snmp-agent target-host**

- **snmp-agent trap enable**

5.1.13 snmp-agent calculate-password

Syntax

snmp-agent calculate-password *plain-password* **mode** { **3desmd5** | **3dessha** | **md5** | **sha** } { **local-engineid** | **specified-engineid** *engineid* }

View

System view

定義済みユーザロール

network-admin

パラメータ

plain-password: プレーンテキストの認証あるいはプライバシーキーを指定します。設定範囲は 1～64 文字です。大文字、小文字を区別します。

mode:認証アルゴリズムと暗号化アルゴリズムを指定します。装置は、HMAC-MD5、HMAC-SHA1 認証アルゴリズムをサポートします。HMAC-MD5 は HMAC-SHA1 よりも計算が早いですが、HMAC-SHA1 は HMAC-MD5 よりもセキュリティ強度が高いです。

暗号化アルゴリズムは AES、3DES、DES の順番でセキュリティ強度が弱くなります。セキュリティ強度が強いアルゴリズムは計算が遅くなります。DES は一般的なセキュリティの要件を満たすのに十分です。

- **3desmd5**: HMAC-MD5 認証アルゴリズムと連携して使用される 3DES 認証キーのため、プライバシーキーをプレーンテキストから暗号テキストに変換します。
- **3dessha**: HMAC-SHA1 認証アルゴリズムと連携して使用される 3DES 認証キーのため、プライバシーキーをプレーンテキストから暗号テキストに変換します。
- **md5**: HMAC-SHA1 認証アルゴリズムと AES あるいは DES 暗号化アルゴリズムを使用して認証キーあるいは暗号化キーをプレーンテキストから暗号テキストに変換します。HMAC-MD5 認証アルゴリズムが使用されるとき、AES あるいは DES 暗号化アルゴリズムが使用されているかどうかにかかわらず、同一の認証キーあるいは暗号化キーを使用します。
- **sha**: HMAC-SHA1 認証アルゴリズムと AES あるいは DES 暗号化アルゴリズムを使用して認証キーあるいは暗号化キーをプレーンテキストから暗号テキストに変換します。HMAC-SHA1 認証アルゴリズムが使用されるとき、AES あるいは DES 暗号化アルゴリズムが使用されているかどうかにかかわらず、同一の認証キーあるいは暗号化キーを使用します。

local-engineid: 暗号テキストのキーを計算するためローカルエンジン ID を使用します。**snmp-agent local-engineid** コマンドでローカルエンジン ID を設定することができます。

specified-engineid *engineid*: 暗号テキストのキーを計算するためユーザ定義のエンジン ID を使用します。*engineid* は 16 進数の文字列で SNMP エンジン ID を指定します。文字列の長さは偶数で構成する必要があります。設定範囲は 10～64 です。すべて 0 あるいはすべて F の文字列は無効です。

説明

snmp-agent calculate-password コマンドは暗号テキストの認証あるいは SNMPv3 でプレーンテキストから変換されたプライバシーキーのダイジェストを計算します。

snmp-agent calculate-password コマンドを実行する前に SNMP エージェントが有効であることを確認してください。

セキュリティのため、**snmp-agent usm-user v3** コマンドを使用して SNMPv3 ユーザを作成するとき、暗号テキストの認証とプライバシーキーのダイジェストを計算するために、**snmp-agent calculate-password** コマンドを使用します。

変換されたキーは変換のため、指定されたエンジン ID でのみ有効です。

例

プレーンテキスト **authkey** から変換された暗号テキストのダイジェストを計算するため、ローカルエンジンと HMAC-SHA1 アルゴリズムを使用します。

<Switch> system-view

[Switch] snmp-agent calculate-password authkey mode sha local-engineid

```
The encrypted key is: 09659EC5A9AE91BA189E5845E1DDE0CC
```

関連コマンド

- **snmp-agent local-engineid**
- **snmp-agent usm-user v3**

5.1.14 snmp-agent 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*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

read: 指定されたコミュニティを MIB オブジェクトへの読み出し専用のアクセス権限に割り当てます。読み出し専用コミュニティは MIB 情報を問い合わせることのみ可能です。

write: 指定されたコミュニティを MIB オブジェクトへの読み出し、書き込みのアクセス権限に割り当てます。読み出し専用コミュニティは MIB 情報を設定することができます。

simple: プレーンテキストのコミュニティを設定します。セキュリティのため、コミュニティは暗号テキストで保存されます。

cipher: 暗号テキストのコミュニティを設定し、暗号テキストで保存します。

community-name: コミュニティを設定します。大文字、小文字を区別します。プレーンテキストの設定範囲は 1～32 文字です。暗号テキストの設定範囲は 33～73 文字です。バックスラッシュの後にエスケープ文字として文字列を入力します。

mib-view *view-name*: コミュニティで有効な MIB view を指定します。*view-name* は MIB view の名前を示します。設定範囲は 1～32 文字です。MIB view はアクセス可能な MIB オブジェクトの一式を示します。MIB view を指定しない場合、コミュニティはデフォルト MIB view の **ViewDefault** の MIB オブジェクトにアクセスできます。

acl: 標準 IPv4 ACL コミュニティを指定します。

ipv4-acl-number: 標準 IPv4 ACL 番号を指定します。設定範囲は 2000～2999 です。

name *ipv4-acl-name*: 標準 IPv4 ACL 名を指定します。設定範囲は 1～63 文字です。大文字、小文字を区別しません。

acl ipv6: 標準 IPv6 ACL コミュニティを指定します。

ipv6-acl-number: 標準 IPv6 ACL 番号を指定します。設定範囲は 2000～2999 です。

name *ipv6-acl-name*: 標準 IPv6 ACL 名を指定します。設定範囲は 1～63 文字です。大文字、小文字を区別しません。

説明

snmp-agent community コマンドは SNMPv1 あるいは SNMPv2c コミュニティを設定します。

undo snmp-agent community コマンドは SNMPv1 あるいは SNMPv2c コミュニティを削除します。

コマンドはユーザロールが network-admin あるいは level-15 のみ実行することができます。これらのロールがほかのユーザロールでは SNMP 機能やコマンドの使用を許可されたとしても実行することができません。

SNMP コミュニティは NMS と SNMP エージェントの一式を構成し、コミュニティによって識別します。NMS と SNMP エージェントは互いにに称するため、同じコミュニティを使用する必要があります。

通常、**public** は読み込み専用のコミュニティとして使用され、**private** は読み込み、書き込みコミュニティとして使用します。セキュリティを改善するため、SNMP コミュニティに **public** と **private** 以外の名前を割り当てます。

SNMP コミュニティで MIB オブジェクトにアクセスを制御するため、以下のモードを使用することができます。

- **VACM（View ベースアクセス制御モデル）**—VACM モードは MIB view を SNMP コミュニティに割り当てることで MIB オブジェクトへのアクセスを制御します。

VACM モードは NMS から MIB オブジェクトのアクセス権のみを必要とします。

snmp-agent community コマンドを使用して 10 個の SNMP コミュニティを作成することができます。コミュニティ名が同一で、ほかのパラメータが異なる設定を指定するため、コマンドを複数回実行する場合、最後に実行した設定が適用されます。

プレーンテキストでコミュニティを設定し、保存する場合、**simple** あるいは **cipher** を指定しないでください。

ACL は不正な NMS をフィルタするために使用します。

- ACL を指定しない、指定した ACL が存在しない、ACL にルールがない場合、すべての NMS は SNMP エージェントにアクセスすることができます。
- ACL を指定し､ACL にルールが存在する場合､ACL に許可された NMS のみが SNMP エージェントにアクセスすることができます。

ACL の詳細は、オペレーションマニュアルのセクション 8 *ACL and QoS* “*ACL*”を参照してください。

snmp-agent usm-user { v1 | v2c }コマンド、**snmp-agent group { v1 | v2c }**コマンドを使用して SNMP コミュニティを作成することができます。2 つのコマンドは SNMPv1 あるいは SNMPv2c ユーザ、ユーザが割り当てられるグループを作成します。システムは自動で SNMPv1 あるいは SNMPv2c ユーザ名を使用して SNMP コミュニティを作成します。

例

プレーンテキストで読み込み専用のコミュニティ readaccess を作成します。SNMPv1 あるいは SNMPv2c の NMS はデフォルト view の ViewDefault の MIB オブジェクトを読むため、コミュニティ readaccess を使用します。

<Switch> system-view

[Switch] snmp-agent sys-info version v1 v2c

[Switch] snmp-agent community read simple readaccess

プレーンテキストで読み込み、書き込みコミュニティ writeaccess を作成します。SNMPv1 あるいは SNMPv2c の IP アドレスが 1.1.1.1 の NMS はデフォルト view の ViewDefault の MIB オブジェクトを読み書きするため、コミュニティ writeaccess を使用します。

<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

プレーンテキストで読み込み、書き込みコミュニティ writeaccess を作成します。SNMPv1 あるいは SNMPv2c の IP アドレスが 1.1.1.2 の NMS はデフォルト view の ViewDefault の MIB オブジェクトを読み書きするため、コミュニティ writeaccess を使用します。

<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

プレーンテキストで読み込み、書き込みコミュニティ wr-sys-acc を作成します。SNMPv1 あるいは SNMPv2c の NMS はシステムサブツリー（OID 1.3.6.1.2.1.1）の MIB オブジェクトを読み書きするため、コミュニティ wr-sys-acc を使用します。

<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

関連コマンド

- **display snmp-agent community**
- **snmp-agent mib-view**

5.1.15 snmp-agent group

Syntax

SNMPv1、SNMPv2c：

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** *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 v3 *group-name* [**authentication** | **privacy**]

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

v1: SNMPv1 を指定します。

v2c: SNMPv2c を指定します。

v3: SNMPv3 を指定します。

group-name: SNMP グループ名を指定します。設定範囲は 1～32 文字です。大文字、小文字を区別します。

authentication: SNMPv3 グループでプライバシーなしのモデルを指定します。

privacy: SNMPv3 グループでプライバシーセキュリティのモデルを指定します。

read-view *view-name*: 読み込み専用の MIB view を指定します。*view-name* は MIB view の名前を示します。設定範囲は 1～32 文字です。MIB view はアクセス可能な MIB オブジェクトの一式を示します。読み込み専用の MIB view を指定しない場合、SNMP グループはデフォルト MIB view の **ViewDefault** の MIB オブジェクトに問い合わせることができます。

write-view *view-name*: 読み込み、書き込みの MIB view を指定します。*view-name* は MIB view の名前を示します。設定範囲は 1～32 文字です。読み込み、書き込みの MIB view を指定しない場合、SNMP グループは SNMP エージェントの MIB オブジェクトを設定することができません。

notify-view *view-name*: notify の MIB view を指定します。*view-name* は MIB view の名前を示します。設定範囲は 1～32 文字です。SNMP エージェントは notify view に含まれる MIB オブジェクトのため、指定されたグループのみのユーザに通知を送信します。notify の MIB view を指定しない場合、SNMP グループは指定されたグループのユーザに通知を送信しません。

acl: 標準 IPv4 ACL コミュニティを指定します。

ipv4-acl-number: 標準 IPv4 ACL 番号を指定します。設定範囲は 2000～2999 です。

name *ipv4-acl-name*: 標準 IPv4 ACL 名を指定します。設定範囲は 1～63 文字です。大文字、小文字を区別しません。

acl ipv6: 標準 IPv6 ACL コミュニティを指定します。

ipv6-acl-number: 標準 IPv6 ACL 番号を指定します。設定範囲は 2000～2999 です。

name *ipv6-acl-name*: 標準 IPv6 ACL 名を指定します。設定範囲は 1～63 文字です。大文字、小文字を区別しません。

説明

snmp-agent group コマンドは SNMP グループを作成し、アクセス権限を指定します。

undo snmp-agent group コマンドは SNMP グループを削除します。

SNMP グループのすべてのユーザはグループのセキュリティモデルとアクセス権限を共有します。

コマンドはユーザロールが network-admin あるいは level-15 のみ実行することができます。これらのロールがほかのユーザロールでは SNMP 機能やコマンドの使用を許可されたとしても実行することができません。

SNMP グループのすべてのユーザはセキュリティモデルとグループのアクセス権限を共有します。

SNMPv1 グループ、SNMPv2c グループ、SNMPv3 グループを含んで 20 個の SNMP グループを作成することができます。

グループのすべての SNMPv3 ユーザは同じセキュリティモデルを共有しますが、異なる認証とプライバシーセキュリティの設定を使用することができます。ユーザのセキュリティモデルを実装し、SNMP 通信の失敗を防ぐため、グループのセキュリティモデルの設定とユーザのセキュリティのキーの設定が、表 5-6 に従い、NMS の設定に一致していることを確認してください。

表 5-6 異なるセキュリティモデルの標準セキュリティの設定要件

セキュリティモデル	グループのセキュリティモデルのキーワード	ユーザのセキュリティのキーの設定	補足
プライバシーセキュリティあり、認証	**privacy**	認証キー、プライバシーキー	認証キーあるいはプライバシーセキュリティが設定されていない場合、SNMPの通信は失敗します。

セキュリティモデル	グループのセキュリティモデルのキーワード	ユーザのセキュリティのキーの設定	補足
プライバシーセキュリティなし、認証	**authentication**	暗号キー	認証キーが設定されていない場合、SNMP の通信は失敗します。ユーザのプライバシーセキュリティ（ある場合）は影響しません。
プライバシーセキュリティなし、認証なし	**authentication**、**privacy** のどちらもありません、	なし	認証キーとプライバシーセキュリティが設定されても影響ありません。

ユーザ、グループのため、ACL は不正な NMS をフィルタするために使用します。ユーザ、グループの両方で ACL に許可された NMS のみが SNMP エージェントにアクセスすることができます。

- ACL を指定しない、指定した ACL が存在しない、ACL にルールがない場合、すべての NMS は SNMP エージェントにアクセスすることができます。
- ACL を指定し､ACL にルールが存在する場合､ACL に許可された NMS のみが SNMP エージェントにアクセスすることができます。

ACL の詳細は、オペレーションマニュアルのセクション 8 *ACL and QoS* “*ACL*”を参照してください。

例

SNMPv3 グループ **group1** を作成します。

<Switch> system-view

[Switch] snmp-agent group v3 group1

関連コマンド

- **display snmp-agent group**
- **snmp-agent mib-view**
- **snmp-agent usm-user**

5.1.16 snmp-agent local-engineid

🕮 **メモ**:

デフォルトコンフィグが設定された装置で snmp を有効にすると、**snmp-agent local-engineid** コマンドが自動的に追加されます。

Syntax

snmp-agent local-engineid *engineid*

undo snmp-agent local-engineid

デフォルト

ローカルエンジン ID は company ID と device ID の組み合わせです。Device ID は製品によって異なります。

View

System view

定義済みユーザロール

network-admin

パラメータ

engineid: 16 進数の文字列で SNMP エンジン ID を指定します。文字列の長さは偶数で構成する必要があります。設定範囲は 10〜64 です。すべて 0 あるいはすべて F の文字列は無効です。

説明

snmp-agent local-engineid コマンドはローカル SNMP エージェントの SNMP エンジン ID を変更します。

undo snmp-agent local-engineid コマンドはデフォルトに戻します。

SNMP エンジン ID は SNMP が管理するネットワークで SNMP エンティティを固有に識別します。ローカル SNMP エンジン ID は通信の問題を防ぐため、SNMP が管理するネットワーク内で一意であることを確認してください。

SNMPv3 ユーザが設定されている場合、必要に応じてローカル SNMP エンジン ID を変更してください。変更すると設定した SNMPv3 ユーザ名と暗号化したキーを無効にすることができます。

ネットワーク計画にもとづいて、デフォルトのエンジン ID、あるいは覚えやすいエンジン ID を設定することができます。たとえば、ビル A の 1 階の装置 1 のエンジン ID は 000Af0010001、装置 2 のエンジン ID は 000Af0010002 です。

例

ローカルエンジン ID を 123456789A に変更します。

<Switch> system-view

[Switch] snmp-agent local-engineid 123456789A

関連コマンド

- **display snmp-agent local-engineid**
- **snmp-agent usm-user**

5.1.17 snmp-agent log

Syntax

snmp-agent log { **all** | **authfail** | **get-operation** | **set-operation** }

undo snmp-agent log { **all** | **authfail** | **get-operation** | **set-operation** }

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

パラメータ

all: SNMP 認証失敗、Get オペレーション、Set オペレーションのロギングを有効にします。

authfail: SNMP 認証の失敗のロギングを有効にします。

get-operation: SNMP Get オペレーションのロギングを有効にします。

set-operation: SNMP Set オペレーションのロギングを有効にします。

説明

snmp-agent log コマンドは SNMP オペレーションのロギングを有効にします。

undo snmp-agent log コマンドは SNMP オペレーションのロギングを無効にします。

NMS のふるまいを検査するため、SNMP エージェントで実行された SNMP オペレーションを記録することができます。SNMP エージェントはログデータを information center に送信します。必要に応じて宛先にデータを出力するように Information Center を設定することができます。

例

SNMP Get オペレーションのロギングを有効にします。

<Switch> system-view

[Switch] snmp-agent log get-operation

SNMP Set オペレーションのロギングを有効にします。

<Switch> system-view

[Switch] snmp-agent log set-operation

SNMP 認証失敗のロギングを有効にします。

<Switch> system-view

[Switch] snmp-agent log authfail

5.1.18 snmp-agent mib-view

Syntax

snmp-agent mib-view { **excluded** | **included** } *view-name oid-tree* [**mask** *mask-value*]

undo snmp-agent mib-view *view-name*

デフォルト

SNMP エージェントが有効なとき、システムは **ViewDefault** view を作成します。デフォルト MIB view では **iso** サブツリーのすべての MIB オブジェクトは **snmpUsmMIB**、**snmpVacmMIB**、**snmpModules.18** サブツリーを除いてアクセス可能です。

View

System view

定義済みユーザロール

network-admin

パラメータ

excluded: 指定した MIB サブツリーのすべてのノードへのアクセスを拒否します。

included: 指定した MIB サブツリーのすべてのノードへのアクセスを許可します。
view-name: view 名を指定します。設定範囲は 1～32 文字です。

oid-tree: ルートノードの OID（たとえば、**1.3.6.1.2.1.1**）あるいはオブジェクト名（たとえば、**system**）によって MIB サブツリーを指定します。設定範囲は 1～255 文字です。大文字、小文字を区別します。OID は MIB ツリーのオブジェクトを固有に識別するドットで区切られた 10 進数の数字です。

mask *mask-value*: MIB サブツリーのマスクを指定します。16 進数です。マスク長は 1～32 の偶数にする必要があります。

説明

snmp-agent mib-view コマンドは MIB view を作成あるいはアップデートします。

undo snmp-agent mib-view コマンドは MIB view を削除します。

MIB view は、アクセス制限のある MIB オブジェクトの集合（あるいは MIB オブジェクト階層）を示し、view 名によって識別されます。MIB view に含まれる MIB オブジェクトはアクセス可能ですが、MIB view から除外されている MIB オブジェクトはアクセスできません。

各 *view-name oid-tree* は view のレコードを示します。異なる MIB サブツリーのマスクで複数回、同一のレコードを指定する場合、最後に行った設定が適用されます。

デフォルト MIB view を削除する場合には注意してください。デフォルト view を使用する NMS から装置の MIB オブジェクトにアクセスできなくなります。

例

mibtest view に mib-2（OID 1.3.6.1.2.1）サブツリーを含め、この view から **system** サブツリーを除外します。

<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

コミュニティ **public** の SNMPv1 の NMS は **mib-2** サブツリーのオブジェクトに問い合わせすることができますが、**system** サブツリーの他のオブジェクト（たとえば、**sysDescr** あるいは **sysObjectID** ノード）は問い合わせすることができません。

関連コマンド

- **display snmp-agent mib-view**
- **snmp-agent group**

5.1.19 snmp-agent packet max-size

Syntax

snmp-agent packet max-size *byte-count*

undo snmp-agent packet max-size

デフォルト

1500 バイト

View

System view

定義済みユーザロール

network-admin

パラメータ

byte-count: SNMP エージェントが送受信できる SNMP パケットの最大サイズを指定します。設定範囲は 484～17940 バイトです。

説明

snmp-agent packet max-size コマンドは SNMP エージェントが送受信できる SNMP パケットの最大サイズを設定します。

undo snmp-agent packet max-size コマンドはデフォルトに戻します。

NMS へのパス上の装置がパケットのフラグメンテーションをサポートしていない場合、大きいサイズのパケットが廃棄されないようにするため、SNMP パケットサイズを制限します。通常のネットワークではデフォルトの設定で十分です。

例

SNMP パケットの最大サイズを 1024 バイトに設定します。

<Switch> system-view

[Switch] snmp-agent packet max-size 1024

5.1.20 snmp-agent packet response dscp

Syntax

snmp-agent packet response dscp *dscp-value*

undo snmp-agent packet response dscp

デフォルト

0

View

System view

定義済みユーザロール

network-admin

パラメータ

dscp-value: SNMP レスポンスパケットの DSCP 値を指定します。設定範囲は 0～63 です。DSCP 値が大きいほど、優先順位が高くなります。

説明

DSCP 値は、IP パケットの ToS フィールドにカプセル化されます。パケットの優先順位レベルを指定し、パケットの送信優先順位に影響します。

例

SNMP レスポンスパケットの DSCP 値を 40 に設定します。

<Switch> system-view

[Switch] snmp-agent packet response dscp 40

5.1.21 snmp-agent sys-info contact

Syntax

snmp-agent sys-info contact *sys-contact*

undo snmp-agent sys-info contact

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

sys-contact: システム連絡先を指定します。設定範囲は 1～255 文字です。

説明

snmp-agent sys-info contact コマンドはシステム連絡先を設定します。

undo snmp-agent sys-info contact コマンドはデフォルトに戻します。

システム管理の連絡先と管理者を設定します。

例

システム連絡先を **Dial System Operator # 27345** に指定します。

<Switch> system-view

[Switch] snmp-agent sys-info contact Dial System Operator # 27345

関連コマンド

display snmp-agent sys-info

5.1.22 snmp-agent sys-info location

Syntax

snmp-agent sys-info location *sys-location*

undo snmp-agent sys-info location

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

sys-location: システム所在地を指定します。設定範囲は 1～255 文字です。

説明

snmp-agent sys-info location コマンドはシステム所在地を設定します。

undo snmp-agent sys-info location コマンドはデフォルトに戻します。

システム管理の装置と管理者の所在地を設定します。

例

システム所在地を **Room524-row1-3** に設定します。

<Switch> system-view

[Switch] snmp-agent sys-info location Room524-row1-3

関連コマンド

display snmp-agent sys-info

5.1.23 snmp-agent sys-info version

🕮 **メモ**:

SNMP 機能を有効にすると、自動的に **snmp-agent sys-info version v3** が設定されます。SNMPv3 が必要ない場合、**undo snmp-agent sys-info version v3** コマンドを実行してください。

Syntax

snmp-agent sys-info version { **all** | { **v1** | **v2c** | **v3** } * }

undo snmp-agent sys-info version { **all** | { **v1** | **v2c** | **v3** } * }

デフォルト

SNMPv3

View

System view

定義済みユーザロール

network-admin

パラメータ

all: SNMPv1、SNMPv2c、SNMPv3 を指定します。

v1: SNMPv1 を指定します。

v2c: SNMPv2c を指定します。

v3: SNMPv3 を指定します。

説明

snmp-agent sys-info version コマンドは SNMP のバージョンを有効にします。

undo snmp-agent sys-info version コマンドは SNMP のバージョンを無効にします。

NMS が SNMP エージェントと正常に通信するため、SNMP エージェントは NMS と同じ SNMP のバージョンを設定します。

例

SNMPv3 を有効にします。

<Switch> system-view

[Switch] snmp-agent sys-info version v3

関連コマンド

display snmp-agent sys-info

5.1.24 snmp-agent target-host

Syntax

snmp-agent target-host inform address udp-domain { *ipv4-address* | **ipv6** *ipv6-address* } [**udp-port** *port-number*] **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*] **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*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

inform: inform として通知を送信します。

trap: trap として通知を送信します。

address: SNMP 通知の宛先アドレスを指定します。

udp-domain: トランスポートプロトコルとして UDP を指定します。

ipv4-address: SNMP 通知の宛先として、ターゲットホストの IPv4 アドレスあるいはホスト名を指定します。ホスト名の設定範囲は 1～253 文字です。大文字、小文字を区別しません。英字、数字、ハイフン（-）、アンダーライン（_）、ドット（.）を含むことができます。ホスト名を指定する場合、ターゲットホストの IPv4 アドレスは、取得することができます。

ipv6 *ipv6-address*: SNMP 通知の宛先として、ターゲットホストの IPv6 アドレスあるいはホスト名を指定します。ホスト名の設定範囲は 1～253 文字です。大文字、小文字を区別しません。英字、数字、ハイフン（-）、アンダーライン（_）、ドット（.）を含むことができます。ホスト名を指定する場合、ターゲットホストの IPv6 アドレスは、取得することができます。

udp-port *port-number*: SNMP 通知の UDP ポートを指定します。指定しない場合、UDP ポート 162 が使用されます。

params securityname *security-string*: 認証パラメータを指定します。*security-string* は SNMPv1 コミュニティ、SNMPv2c コミュニティ、あるいは SNMPv3 ユーザ名を指定します。設定範囲は 1～32 文字です。

v1: SNMPv1 を指定します。

v2c: SNMPv2c を指定します。

v3: SNMPv3 を指定します。

- **authentication**: プライバシーセキュリティなしで認証するようにセキュリティモデルを指定します。SNMPv3 ユーザを作成したとき認証キーを指定する必要があります。
- **privacy**: プライバシーセキュリティありで認証するようにセキュリティモデルを指定します。SNMPv3 ユーザを作成したとき認証キーとプライバシーキーを指定する必要があります。

説明

snmp-agent target-host コマンドは SNMP 通知（inform あるいは trap）をホストに送信するため、SNMP エージェントを設定します。

undo snmp-agent target-host コマンドは SNMP 通知のターゲットホストを削除します。

複数の SNMP 通知のターゲットホストを指定することができます。

SNMP エージェントは SNMP 通知のため、ターゲットホストの UDP ポートと同一のポートを使用する必要があります。通常、MIB ブラウザのような NMS は SNMP 通知のために、SNMP プロトコルで定義された UDP ポート 162 を使用します。

v1、**v2c**、**v3** を指定しない場合、SNMPv1 が使用されます。ホストが通知を受信できるように、SNMP エージェントは、ターゲットホストの SNMP のバージョンと同一のバージョンを使用することを確認してください。

authentication あるいは **privacy** の両方を指定しない場合、セキュリティモデルはプライバシーセキュリティなし、認証なしです。

例

ユーザ **public** の 10.1.1.1 に SNMPv3 の trap を送信するため、SNMP エージェントを設定します。

<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

関連コマンド

- **snmp-agent { inform | trap } source**
- **snmp-agent trap enable**
- **snmp-agent trap life**

5.1.25 snmp-agent trap enable

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**]

デフォルト

SNMP configuration 通知、standard 通知、system 通知は有効です。他の SNMP 通知はモジュールによって変わります。

View

System view

定義済みユーザロール

network-admin

パラメータ

configuration: configuration 通知を指定します。configuration 通知が有効である場合、システムはカレントコンフィグレーションとスタートアップコンフィグレーションを 10 分毎に変更点を確認し、最新の変更の通知を作成します。

protocol: SNMP 通知が有効なモジュールを指定します。パラメータの値を取得する場合、**snmp-agent trap enable ?**コマンドを使用します。このパラメータの詳細は各モジュールのコマンドマニュアルを参照してください。

standard: standard 通知を指定します。

表 5-7 Standard SNMP 通知

キーワード	定義
authentication	NMSがSNMPエージェントへの認証に失敗したとき、認証失敗通知を送信します。
coldstart	装置が再起動したときに通知を送信します。
linkdown	ポートのリンクがダウンしたときに通知を送信します。
linkup	ポートのリンクがアップしたときに通知を送信します。
warmstart	SNMPエージェントが再起動したときに通知を送信します。

system: システム時間が変更された、システムが再起動した、あるいはメインのシステムソフトウェアイメージが有効でないときに system 通知を指定します。

説明

snmp-agent trap enable コマンドはグローバルで SNMP 通知を有効にします。

undo snmp-agent trap enable コマンドはグローバルで SNMP 通知を無効にします。

重大なプロトコルのイベントを NMS に通知するため、プロトコルの SNMP 通知を有効にしてください。SNMP 通知を正常に送信するため、必要な Notification のパラメータを設定してください。

パラメータを指定しない場合、**snmp-agent trap enable** コマンドあるいは **undo** コマンドは装置でサポートされるすべての SNMP 通知を有効あるいは無効にします。

例

SNMP 認証の失敗の Notification を送信するように SNMP エージェントを有効にします。

<Switch> system-view

[Switch] snmp-agent trap enable standard authentication

関連コマンド

snmp-agent target-host

5.1.26 snmp-agent trap if-mib link extended

Syntax

snmp-agent trap if-mib link extended

undo snmp-agent trap if-mib link extended

デフォルト

SNMP エージェントは標準 linkUp/linkDown 通知を送信します。

View

System view

定義済みユーザロール

network-admin

説明

snmp-agent trap if-mib link extended コマンドは拡張 linkUp/linkDown 通知を送信するように SNMP エージェントを設定します。

undo snmp-agent trap if-mib link extended コマンドはデフォルトに戻します。

拡張 linkUp/linkDown 通知は、早急に故障個所を識別するため、標準 linkUp/linkDown 通知にインタフェースの説明とインタフェースのタイプを追加します。

このコマンドを使用するとき、NMS が拡張 linkUp/linkDown 通知をサポートしていることを確認してください。

例

拡張 linkUp/linkDown 通知を送信するように SNMP エージェントを設定します。

<Switch> system-view

[Switch] snmp-agent trap if-mib link extended

5.1.27 snmp-agent trap life

Syntax

snmp-agent trap life *seconds*

undo snmp-agent trap life

デフォルト

120 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

seconds: ライフタイムを指定します。設定範囲は 1～2592000 秒です。

説明

snmp-agent trap life コマンドは SNMP 通知キューの通知のライフタイムを設定します。

undo snmp-agent trap life コマンドはデフォルトの通知のライフタイムに戻します。

衝突が発生すると、SNMP エージェントはキューに通知をバッファします。通知のライフタイムはキューに保持しておく期間を設定します。ライフタイムが終了したとき notification は削除されます。

例

SNMP 通知のライフタイムを 60 秒に設定します。

<Switch> system-view

[Switch] snmp-agent trap life 60

関連コマンド

- **snmp-agent target-host**

- **snmp-agent trap enable**
- **snmp-agent trap queue-size**

5.1.28 snmp-agent trap log

Syntax

snmp-agent trap log

undo snmp-agent trap log

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

snmp-agent trap log コマンドは SNMP 通知のロギングを有効にします。

undo snmp-agent trap log コマンドは SNMP 通知のロギングを無効にします。

通知のトラッキングを行うため、SNMP エージェントによって送信された SNMP 通知を記録するため、SNMP 通知のロギングを使用します。SNMP エージェントは Information Center にログを送信します。必要に応じて宛先にログを出力するように Information Center を設定することができます。

例

SNMP 通知のロギングを有効にします。

<Switch> system-view

[Switch] snmp-agent trap log

5.1.29 snmp-agent trap queue-size

Syntax

snmp-agent trap queue-size *size*

undo snmp-agent trap queue-size

デフォルト

100

View

System view

定義済みユーザロール

network-admin

パラメータ

size: SNMP 通知のキューが保持できる通知の最大数を指定します。設定範囲は 1～1000 です。

説明

snmp-agent trap queue-size コマンドは SNMP 通知のキューのサイズを設定します。

undo snmp-agent trap queue-size コマンドはデフォルトのキューのサイズに戻します。

衝突が発生したとき、SNMP エージェントはキューに通知をバッファします。SNMP 通知のキューのサイズは SNMP 通知のキューが保持できる通知の最大数を設定します。キューのサイズが上限に到達したとき、新しい通知のために、古い通知が廃棄されます。

例

SNMP 通知のキューのサイズを 200 に設定します。

<Switch> system-view

[Switch] snmp-agent trap queue-size 200

関連コマンド

- **snmp-agent target-host**
- **snmp-agent trap enable**
- **snmp-agent trap life**

5.1.30 snmp-agent usm-user { v1 | v2c }

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*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

v1: SNMPv1 を指定します。

v2c: SNMPv2c を指定します。

user-name: SNMP ユーザ名を指定します。設定範囲は 1～32 文字です。大文字、小文字を区別します。

group-name: SNMPv1 あるいは SNMPv2c のグループ名を指定します。設定範囲は 1～32 文字です。大文字、小文字を区別します。グループは、すでに作成されたものでも指定できます。グループが作成されていない場合、グループを作成した後、適用されます。

acl: 標準 IPv4 ACL を指定します。

ipv4-acl-number: 標準 IPv4 ACL 番号を指定します。設定範囲は 2000～2999 です。

name *ipv4-acl-name*: 標準 IPv4 ACL 名を指定します。設定範囲は 1～63 文字です。大文字、小文字を区別しません。

acl ipv6: 標準 IPv6 ACL を指定します。

ipv6-acl-number: 標準 IPv6 ACL 番号を指定します。設定範囲は 2000～2999 です。

name *ipv6-acl-name*: 標準 IPv6 ACL 名を指定します。設定範囲は 1～63 文字です。大文字、小文字を区別しません。

説明

snmp-agent usm-user { **v1** | **v2c** }コマンドは SNMPv1 あるいは SNMPv2c グループにユーザを追加します。

undo snmp-agent usm-user { **v1** | **v2c** }コマンドは SNMPv1 あるいは SNMPv2c グループからユーザを削除します。

コマンドはユーザロールが network-admin あるいは level-15 のみ実行することができます。これらのロールがほかのユーザロールでは SNMP 機能やコマンドの使用を許可されたとしても実行することができません。

SNMPv1 あるいは SNMPv2c では NMS、SNMP エージェントはコミュニティ名を使用して互いに認証します。SNMPv3 ではユーザ名を使用して互いに認証します。

以下のどちらかの方法を使用して SNMPv1 あるいは SNMPv2c コミュニティを作成することができます。

- **snmp-agent community** コマンドを実行します。
- SNMPv1 あるいは SNMPv2c ユーザ、ユーザに割り当てられるグループを作成するため、**snmp-agent usm-user { v1 | v2c }**コマンド、**snmp-agent group { v1 | v2c }** コマンドを実行します。システムは SNMPv1 あるいは SNMPv2c のユーザ名を使用して自動で SNMP コミュニティを作成します。

ユーザ、グループのために ACL は不正な NMS をフィルタするために使用します。ユーザ、グループの両方で ACL に許可された NMS のみが SNMP エージェントにアクセスすることができます。

- ACL を指定しない、指定した ACL が存在しない、ACL にルールがない場合、すべての NMS は SNMP エージェントにアクセスすることができます。
- ACL を指定し、ACL にルールが存在する場合、ACL に許可された NMS のみが SNMP エージェントにアクセスすることができます。

ACL の詳細は、オペレーションマニュアルのセクション 8 *ACL and QoS* “*ACL*”を参照してください。

例

NMS が SNMPv2c を使用するため、SNMPv2c グループ **readCom** にユーザ **userv2c** を追加します。読み込み専用のコミュニティ **userv2c** を使用して装置にアクセスします。

<Switch> system-view

[Switch] snmp-agent sys-info version v2c

[Switch] snmp-agent group v2c readCom

[Switch] snmp-agent usm-user v2c userv2c readCom

IP アドレス 1.1.1.1 の NMS が SNMPv2c を使用するため、SNMPv2c グループ **readCom** にユーザ **userv2c** を追加します。読み込み専用のコミュニティ **userv2c** を使用して装置にアクセスします。

<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

IP アドレス 1.1.1.2 の NMS が SNMPv2c を使用するため、SNMPv2c グループ **readCom** にユーザ **userv2c** を追加します。読み込み専用のコミュニティ **userv2c** を使用して装置にアクセスします。

[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

関連コマンド

- **display snmp-agent community**
- **snmp-agent community**
- **snmp-agent group**

5.1.31 snmp-agent usm-user v3

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* }

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

user-name: SNMPv3 ユーザ名を指定します。設定範囲は 1～32 文字です。大文字、小文字を区別します。

group-name: SNMPv3 のグループ名を指定します。設定範囲は 1～32 文字です。大文字、小文字を区別します。グループが作成されていない場合、ユーザはグループが作成されたのち適用されます。

cipher: 認証キーと暗号化キーを暗号テキストとして指定します。キーは暗号テキストで保存されます。

simple: 認証キーと暗号化キーをプレーンテキストとして指定します。

authentication-mode: 認証アルゴリズムを指定します。指定しない場合、認証を行いません。

- **md5**: HMAC-MD5 認証アルゴリズムを指定します。
- **sha**: HMAC-SHA1 認証アルゴリズムを指定します。

auth-password: 認証キーを指定します。大文字、小文字を区別します。

- プレーンテキストの設定範囲は 1～64 文字です。数字、大文字、小文字、記号を含む必要があります。
- キーの暗号テキストは **snmp-agent calculate-password** コマンドで計算されます。

privacy-mode: 暗号アルゴリズムを指定します。指定しない場合、暗号を行いません。

- **3des**: 168 ビットのキーを使用して 3DES アルゴリズムを指定します。
- **aes128**: 128 ビットのキーを使用して AES アルゴリズムを指定します。
- **des56:** 56 ビットのキーを使用して DES アルゴリズムを指定します。

priv-password: 暗号キーを指定します。大文字、小文字を区別します。

- プレーンテキストの設定範囲は 1～64 文字です。数字、大文字、小文字、記号を含む必要があります。
- キーの暗号テキストは **snmp-agent calculate-password** コマンドで計算されます。

acl: 標準 IPv4 ACL を指定します。

ipv4-acl-number: 標準 IPv4 ACL 番号を指定します。設定範囲は 2000～2999 です。

name *ipv4-acl-name*: 標準 IPv4 ACL 名を指定します。設定範囲は 1～63 文字です。大文字、小文字を区別しません。

acl ipv6: 標準 IPv6 ACL を指定します。

ipv6-acl-number: 標準 IPv6 ACL 番号を指定します。設定範囲は 2000～2999 です。

name *ipv6-acl-name*: 標準 IPv6 ACL 名を指定します。設定範囲は 1～63 文字です。大文字、小文字を区別しません。

local: ローカル SNMP エンジンを指定します。デフォルトで SNMPv3 ユーザはローカル SNMP エンジンに関連づけられています。

engineid *engineid-string*: 16 進数の文字列で SNMP エンジン ID を指定します。文字列の長さは偶数で構成する必要があります。設定範囲は 10～64 です。すべて 0 あるいはすべて F の文字列は無効です。ローカルエンジンの ID を変更した後、既存の SNMPv3 ユーザと暗号化されたキーは無効になります。無効なユーザ名を削除する場合、**undo snmp-agent usm-user v3** コマンドでユーザ名にエンジン ID を指定してください。

再度設定を行う必要があります。

説明

snmp-agent usm-user v3 コマンドは SNMPv3 ユーザを作成します。

undo snmp-agent usm-user v3 コマンドは SNMPv3 グループからユーザを削除します。

コマンドはユーザロールが network-admin あるいは level-15 のみ実行することができます。これらのロールがほかのユーザロールでは SNMP 機能やコマンドの使用を許可されたとしても実行することができません。

SNMPv3 ユーザで MIB オブジェクトにアクセスを制御するため、以下のモードを使用することができます。

- **VACM（View ベースアクセス制御モデル）**—VACM モードはグループに SNMPv3 ユーザを割り当てる前に SNMPv3 グループを作成する必要があります。そうでない場合、グループが作成されたのち、ユーザが適用されません。SNMP グループは複

数のユーザを含むことができます。SNMP グループはユーザのグループの MIB view とセキュリティモデルを指定します。各ユーザの認証と暗号化アルゴリズムは作成されたときに指定されます。

異なる SNMPv3 ユーザを作成するため **snmp-agent usm-user v3** コマンドを複数設定することができます。ユーザ名が同一である場合、最後に行った設定が適用されます。

NMS でエージェントにアクセスする場合、以下のことが必要です。

ユーザ、グループのために ACL は不正な NMS をフィルタするために使用します。ユーザ、グループの両方で ACL に許可された NMS のみが SNMP エージェントにアクセスすることができます。

- ACL を指定しない、指定した ACL が存在しない、ACL にルールがない場合、すべての NMS は SNMP エージェントにアクセスすることができます。
- ACL を指定し、ACL にルールが存在する場合、ACL に許可された NMS のみが SNMP エージェントにアクセスすることができます。

ACL の詳細は、オペレーションマニュアルのセクション 8 *ACL and QoS* “*ACL*”を参照してください。

例

SNMPv3 グループ **testGroup** にユーザ **testUser** を追加します。グループでプライバシーセキュリティモデルなしで認証を有効にします。ユーザの認証アルゴリズムを HMAC-SHA11、プレーンテキストで認証キーを **123456TESTplat&!**に設定します。

<Switch> system-view

[Switch] snmp-agent group v3 testGroup authentication

[Switch] snmp-agent usm-user v3 testUser testGroup simple authentication-mode sha 123456TESTplat&!

デフォルト view が **ViewDefault** の MIB オブジェクトに NMS がアクセスするため、SNMP エージェントの設定と同様に以下の NMS の設定を行います。

- SNMPv3 ユーザ名
- SNMP プロトコルバージョン
- 認証アルゴリズムとキー

SNMPv3 グループ **testGroup** にユーザ **testUser** を追加します。グループで認証とプライバシーセキュリティモデルを有効にします。ユーザの認証アルゴリズムを HMAC-SHA1、プライバシーアルゴリズムを AES、プレーンテキストで認証キーを **123456TESTauth&!**に設定します。プレーンテキストでユーザのプライバシーキーを **123456TESTencr&!**に設定します。

<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&!

デフォルト view が **ViewDefault** の MIB オブジェクトに NMS がアクセスするため、SNMP エージェントの設定と同様に以下の NMS の設定を行います。

- SNMPv3 ユーザ名
- SNMP プロトコルバージョン
- 認証アルゴリズム
- プライバシーアルゴリズム
- プレーンテキストの認証とプライバシーキー

関連コマンド

- **display snmp-agent usm-user**
- **snmp-agent calculate-password**
- **snmp-agent group**

目次

このセクションのページは **11-x-x** です。

6 章 RMON 6-1
6.1 RMON 設定コマンド 6-1
6.1.1 display rmon alarm 6-1
6.1.2 display rmon event 6-3
6.1.3 display rmon eventlog 6-4
6.1.4 display rmon history 6-6
6.1.5 display rmon prialarm 6-9
6.1.6 display rmon statistics 6-11
6.1.7 rmon alarm 6-14
6.1.8 rmon event 6-17
6.1.9 rmon history 6-18
6.1.10 rmon prialarm 6-20
6.1.11 rmon statistics 6-22

6章 RMON

6.1 RMON設定コマンド

6.1.1 display rmon alarm

Syntax

display rmon alarm [*entry-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

entry-number: RMON アラームエントリのインデックスを指定します。設定範囲は 1～65535 です。指定しない場合、RMON アラームテーブルのすべてのエントリを表示します。

説明

display rmon alarm コマンドは RMON アラームテーブルのエントリを表示します。

例

RMON アラームテーブルのすべてのエントリを表示します。

<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
```

表 6-1 コマンド出力

フィールド	説明
AlarmEntry *entry-number* owned by *owner* is status.	アラームエントリのオーナと状態です。 ● *entry-number*—アラームエントリのインデックスです。 ● *owner*—エントリオーナです。 ● *status*—エントリ状態です。 • **VALID**—エントリが有効です。 • **UNDERCREATION**—エントリが無効です。 *status*フィールドはCLIで設定できません。CLIから作成されたすべてのアラームエントリはデフォルトで有効です。 **display rmon alarm**コマンドは無効のエントリを表示することができますが、**display current-configuration**コマンドと**display this**コマンドは設定を表示しません。
Sample type	サンプルタイプです。 ● **absolute**—RMONはサンプリング間隔の両端で増加方向のしきい値と減少方向のしきい値を比較します。 ● **delta**—RMONは現在の値から前に取得したサンプル値を引き、増加方向と減少方向のしきい値の差異を比較します。
Sampled variable	モニタされる変数です。
Sampling interval	サンプルされるデータの間隔（単位は秒です）と増加方向かなくいのしきい値と減少方向のしきい値を比較します。
Rising threshold	アラームの増加方向のしきい値です。
associated with event	アラームに関連したイベントインデックスです。
Falling threshold	アラームの減少方向のしきい値です。
Alarm sent upon entry startup	エントリが有効になったとき、作成されるアラームです。 ● **risingAlarm**—エントリが有効になったのち、最初のサンプルが増加方向のしきい値以上になった場合、増加方向のアラームを作成します。 ● **fallingAlarm**—エントリが有効になったのち、最初のサンプルが増加方向のしきい値以下になった場合、減少方向のアラームを作成します。 ● **risingOrFallingAlarm**—エントリが有効になったのち、最初のサンプルが増加方向のしきい値あるいは減少方向のしきい値と交差したとき、増加方向のアラームあるいは減少方向のアラームを作成します。 デフォルトは**risingOrFallingAlarm**です。

フィールド	説明
Latest value	最後に取得したサンプル値です。

関連コマンド

rmon alarm

6.1.2 display rmon event

Syntax

display rmon event [*entry-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

entry-number: イベントエントリのインデックスを指定します。設定範囲は 1～65535 です。指定しない場合、すべてのイベントエントリを表示します。

説明

display rmon event コマンドは RMON イベントエントリを表示します。

イベントエントリは、以下の情報が含まれます。

- イベントインデックス
- イベントオーナ
- イベント説明
- イベントによって発生するアクション（たとえば、イベントをロギングします、あるいは SNMP 通知を送信します）
- イベントが発生した最後の時間（システムが起動してからの経過時間です。単位は秒です）

例

すべてのイベントエントリを表示します。

<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.
```

表 6-2 コマンド出力

フィールド	説明
EventEntry *entry-number* owned by *owner* is *status*.	イベントエントリのオーナと状態です。 ● *entry-number*—イベントエントリのインデックスです。 ● *owner*—エントリオーナです。 ● *status*—エントリ状態です。 • **VALID**—エントリが有効です。 • **UNDERCREATION**—エントリが無効です。 *status*フィールドはCLIで設定できません。CLIから作成されたすべてのイベントエントリはデフォルトで有効です。 **display rmon event**コマンドは無効のエントリを表示することができますが、**display current-configuration**コマンドと**display this**コマンドは設定を表示しません。
Description	イベント説明です。
Community	RMONイベントのSNMPコミュニティ名です。
Take the action action when triggered	イベントが発生したときのアクションです。 ● **none**—アクションを行いません。 ● **log**—イベントをロギングします。 ● **trap**—SNMP通知を送信します。 ● **log-trap**—イベントをロギングし、SNMP通知を送信します。
last triggered at time uptime	イベントが発生したときの最後の時間です。システムが起動してからの経過時間として表示されます。

関連コマンド

rmon event

6.1.3 display rmon eventlog

Syntax

display rmon eventlog [*entry-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

entry-number: イベントエントリのインデックスを指定します。設定範囲は 1～65535 です。指定しない場合、すべてのイベントエントリを表示します。

説明

display rmon eventlog コマンドはイベントログのエントリを表示します。

イベントのログのアクションが指定されている場合、イベントが発生する毎に、イベントログテーブルにレコードを追加します。各レコードはログエントリインデックス、イベントがログされた時間（システムが起動してからの経過時間）、イベント説明を含みます。

システムはイベントに 10 個のレコードを追加することができます。レコードが 10 になったとき、古いレコードを最新のレコードに置き換えます。

例

イベントエントリ 99 の RMON ログを表示します。

<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.
```

この例では、イベントログテーブルはイベント 99 で 4 つのレコードがあることを示します。

- イベント 99 がアラームエントリ 77 によって発生したとき 2 つのレコードが作成されました。
- イベント 99 がアラームエントリ 777 によって発生したとき 2 つのレコードが作成されました。

表 6-3 コマンド出力

フィールド	説明

EventEntry *entry-number* owned by *owner* is *status*.	イベントログエントリのオーナと状態です。
	• *entry-number*—イベントログエントリのインデックスです。ログエントリが作成されたイベントエントリのインデックスと同一です。
	• *owner*—エントリオーナです。
	• *status*—エントリ状態です。
	  • **VALID**—エントリが有効です。（デフォルトです）
	  • **UNDERCREATION**—エントリが無効です。
	*status*フィールドはCLIで設定できません。CLIから作成されたすべてのイベントログエントリはデフォルトで有効です。**display rmon eventlog**コマンドは無効のエントリを表示することができますが、**display current-configuration**コマンドと**display this**コマンドは設定を表示しません。

LogEntry *entry-number* created at *created-time* uptime.	イベントレコードが作成された時間です。 • **entry-number**—イベントレコードインデックスです。logEventIndex.logIndexとして示されます。これはイベントのすべてのレコードのなかでレコードを一意に識別します。 • **created-time**—イベントエントリが作成された時間です。
Description	レコードの説明です。

関連コマンド

rmon event

6.1.4 display rmon history

Syntax

display rmon history [*interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface-type interface-number: インタフェースのタイプと番号を指定します。インタフェースを指定しない場合、RMON 履歴管理エントリがあるすべてのインタフェースの履歴サンプルを表示します。

説明

display rmon history コマンドは Ethernet インタフェースの RMON 履歴管理エントリと Ethernet 履歴のサンプルの統計情報を表示します。

RMON は Ethernet インタフェースの Ethernet 履歴のサンプルを記録するため、etherHistoryTable オブジェクトを使用します。

Ethernet インタフェースの履歴サンプルを収集するため、最初にインタフェースで履歴管理エントリを作成する必要があります。

表示できる履歴サンプルの数とサンプリング間隔を設定する場合、**rmon history** コマンドを使用します。

例

GigabitEthernet 1/0/1 の RMON 履歴管理エントリと履歴のサンプルの情報を表示します。

<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
```

表 6-4 コマンド出力

フィールド	説明
HistoryControlEntry *entry-number* owned by *owner* is *status*.	ヒストリ制御エントリのオーナと状態です。 ● *entry-number*—ヒストリ制御エントリのインデックスです。 ● *owner*—エントリオーナです。 ● *status*—エントリ状態です。 • **VALID**—エントリが有効です。 • **UNDERCREATION**—エントリが無効です。 *status*フィールドはCLIで設定できません。CLIから作成されたすべてのヒストリ制御エントリはデフォルトで有効です。The **display rmon history**コマンドは無効のエントリを表示することができますが、**display current-configuration**コマンドと**display this**コマンドは設定を表示しません。
Sampled Interface	サンプルされるインタフェースです。
Sampling interval	サンプルされるデータの間隔です。単位は秒です。
buckets max	履歴管理エントリで保存できるサンプルの最大数です。 **rmon history**コマンドで設定した、予期したバケットサイズが有効な履歴テーブルサイズを超過した場合、RMONはバケットサイズをできるだけ、予期したバケットサイズに近づけます。 バケットサイズが一杯になったとき、RMONは新しいサンプルを古いサンプルに上書きします。
Sampling record	履歴さんプリインデックスです。
dropevents	サンプリング間隔中にパケットが廃棄されたイベントの総数です。 🕮 **メモ：** 統計情報は、廃棄が発生した回数です。廃棄したパケットの総数になるわけではありません。
octets	サンプリング間隔中に受信したオクテット数です。
packets	サンプリング間隔中に受信したパケットの総数（不良パケットを含みます）です。
broadcast packets	サンプリング間隔中に受信したブロードキャストパケットの総数です。
multicast packets	サンプリング間隔中に受信したマルチキャストパケットの総数です。

フィールド	説明
CRC alignment errors	サンプリング間隔中に受信したCRCエラーパケットの数です。
undersize packets	サンプリング間隔中に受信した過小サイズのエラーパケットの数です。 過小サイズエラーパケットはパケット長が64オクテット未満のパケットです。（フレームビットを除き、FCSオクテットを含みます）
oversize packets	サンプリング間隔中に受信した過大サイズのエラーパケットの数です。 過大サイズエラーパケットはパケット長が1518オクテットより長いパケットです。（フレームビットを除き、FCSオクテットを含みます）
fragments	サンプリング間隔中に受信した過小サイズのCRCエラーパケットの数です。
jabbers	サンプリング間隔中に受信した過大サイズのCRCエラーパケットの数です。
collisions	サンプリング間隔中に受信したコリジョンパケットの数です。
utilization	サンプリング間隔中の帯域幅の使用率です。(単位は% です)

関連コマンド

rmon history

6.1.5 display rmon prialarm

Syntax

display rmon prialarm [*entry-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

entry-number: アラームエントリのインデックスを指定します。設定範囲は 1～65535 です。指定しない場合、すべてのプライベートアラームエントリを表示します。

説明

display rmon prialarm コマンドはプライベート RMON アラームテーブルのエントリを表示します。

例

すべてのプライベートアラームエントリを表示します。

<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
```

表 6-5 コマンド出力

フィールド	説明
PrialarmEntry *entry-number* owned by *owner* is *status*.	プライベートアラームエントリのオーナと状態です。 ● *entry-number*—プライベートアラームエントリのインデックスです。 ● *owner*—エントリオーナです。 ● *status*—エントリ状態です。 • **VALID**—エントリが有効です。 • **UNDERCREATION**—エントリが無効です。 *status*フィールドはCLIで設定できません。CLIから作成されたすべてのプライベートアラームエントリはデフォルトで有効です。 **display rmon prialarm**コマンドは無効のエントリを表示することができますが、**display current-configuration**コマンドと**display this**コマンドは設定を表示しません。
Sample type	サンプルタイプです。 ● **absolute**—RMONはサンプリング間隔の両端で増加方向のしきい値と減少方向のしきい値を比較します。 ● **delta**—RMONは現在の値から以前に取得したサンプル値を引き、増加方向と減少方向のしきい値の差異を比較します。

フィールド	説明
Variable formula	変数の式です。
Description	アラームエントリの説明です。
Sampling interval	サンプルされるデータの間隔です。単位は秒です。
Rising threshold	アラームの増加方向のしきい値です。
Falling threshold	アラームの減少方向のしきい値です。
associated with event	アラームに関連したイベントインデックスです。
Alarm sent upon entry startup	エントリが有効になったとき、作成されるアラームです。 ● **risingAlarm**—エントリが有効になったのち、最初のサンプルが増加方向のしきい値以上になった場合、増加方向のアラームを作成します。 ● **fallingAlarm**—エントリが有効になったのち、最初のサンプルが増加方向のしきい値以下になった場合、減少方向のアラームを作成します。 ● **risingOrFallingAlarm**—エントリが有効になったのち、最初のサンプルが増加方向のしきい値あるいは減少方向のしきい値と交差したとき、増加方向のアラームあるいは減少方向のアラームを作成します。 デフォルトは**risingOrFallingAlarm**です。
Entry lifetime	エントリの有効期限です。 ● 有効期限がforeverに設定されている場合、エントリは削除されません。 ● 有効期限に時間が設定されている場合、時間が終了したときエントリが削除されます。
Latest value	最後に取得したサンプル値です。

関連コマンド

rmon prialarm

6.1.6 display rmon statistics

Syntax

display rmon statistics [*interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface-type interface-number: インタフェースのタイプと番号を指定します。インタフェースを指定しない場合、すべてのインタフェースの RMON の統計情報を表示します。

説明

display rmon statistics コマンドは RMON の統計情報を表示します。

このコマンドは、統計情報エントリが作成された時間からコマンドが実行された時間までの期間のインタフェース統計情報を表示します。装置が再起動するとその統計情報は削除されます。

例

GigabitEthernet 1/0/1 の RMON の統計情報を表示します。

<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
```

表 6-6 コマンド出力

フィールド	説明
EtherStatsEntry *entry-number* owned by *owner* is *status*.	統計情報エントリのオーナと状態です。 ● *entry-number*—統計情報エントリのインデックスです。 *owner*—エントリオーナです。 ● *status*—エントリ状態です。 • **VALID**—エントリが有効です。 • **UNDERCREATION**—エントリが無効です。 *status*フィールドはCLIで設定できません。CLIから作成されたすべての統計情報エントリはデフォルトで有効です。 **display rmon statistics**コマンドは無効のエントリを表示することができますが、**display current-configuration**コマンドと**display this**コマンドは設定を表示しません。
Interface	統計情報が収集されたインタフェースです。
etherStatsOctets	インタフェースで受信したオクテットの総数です。
etherStatsPkts	インタフェースで受信したパケットの総数です。
etherStatsBroadcastPkts	インタフェースで受信したブロードキャストパケットの総数です。
etherStatsMulticastPkts	インタフェースで受信したマルチキャストパケットの総数です。
etherStatsUndersizePkts	インタフェースで受信した過小サイズのエラーパケットの総数です。
etherStatsOversizePkts	インタフェースで受信した過大サイズのエラーパケットの総数です。
etherStatsFragments	インタフェースで受信したCRCエラーパケットの総数です。
etherStatsJabbers	インタフェースで受信した過大サイズのCRCエラーパケットの総数です。
etherStatsCRCAlignErrors	インタフェースで受信したCRCエラーパケットの総数です。
etherStatsCollisions	インタフェースで受信したコリジョンパケットの総数です。
etherStatsDropEvents	廃棄されたパケットのイベント総数です。 🕮 **メモ：** 統計情報は、廃棄が発生した回数です。廃棄したパケットの総数になるわけではありません。

フィールド	説明
Incoming packets by size:	パケット長毎の入力パケットです。 ● **64**—64バイト長のパケット数です。 ● **65-127**—65～127バイト長のパケット数です。 ● **128-255**—128～255バイト長のパケット数です。 ● **256-511**—256～511バイト長のパケット数です。 ● **512-1023**—512～1023バイト長のパケット数です。 ● **1024-1518**—1024～1518バイト長のパケット数です。

関連コマンド

rmon statistics

6.1.7 rmon alarm

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*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

entry-number: アラームエントリのインデックスを指定します。設定範囲は 1～65535 です。

alarm-variable: アラーム変数を指定します。設定範囲は 1～255 です。変数は ASN.1 INTEGER（INTEGER、NTEGER32、Unsigned32、Counter32、Counter64、Gauge、TimeTicks）のみを使用できます。アラーム変数は表 6-7 の 1 つを使用します。

表 6-7 アラーム変数

フォーマット	例
ドットで区切られたOID形式： エントリ.整数,インスタンス	1.3.6.1.2.1.2.1.10.1
オブジェクト名.インスタンス	etherStatsOctets.1 etherStatsPkts.1 etherStatsBroadcastPkts.1 ifInOctets.1 ifInUcastPkts.1 ifInNUcastPkts.1

sampling-interval: サンプリング間隔を指定します。設定範囲は 5～65535 秒です。

absolute: 絶対値のサンプリングを指定します。RMON はサンプリング間隔の両端で増加方向のしきい値と減少方向のしきい値を比較します。

delta: 相対値のサンプリングを指定します。RMON は現在の値から前に取得したサンプル値を引き、増加方向と減少方向のしきい値の差異を比較します。

startup-alarm: アラームエントリが有効なときに作成されるアラームを指定します。アラームを指定しない場合、RMON は最初のサンプルに依存して増加方向のアラームあるいは減少方向のアラームを作成します。

rising: エントリが有効になったのち、最初にサンプルが増加方向のしきい値以上になった場合に、増加方向のアラームを作成します。

falling: エントリが有効になったのち、最初にサンプルが減少方向のしきい値以下になった場合に、減少方向のアラームを作成します。

rising-falling: 最初のサンプルが増加方向のしきい値と交差した場合、増加方向のアラームを作成します。あるいは最初のサンプルが減少方向のしきい値と交差した場合、減少方向のアラームを作成します。

rising-threshold *threshold-value1 event-entry1*: 増加方向のしきい値を指定します。*threshold-value1* の設定範囲は–2147483648 ～ +2147483647 です。*event-entry1* は増加方向のしきい値が交差したとき発生するイベントのインデックスを示します。*event-entry1* の設定範囲は 0～65535 です。0 が指定された場合、イベントでアラームが発生しません。

falling-threshold *threshold-value2 event-entry2*: 減少方向のしきい値を指定します。*threshold-value2* の設定範囲は–2147483648 ～ +2147483647 です。*event-entry2* は減少方向のしきい値が交差したとき発生するイベントのインデックスを示します。*event-entry2* の設定範囲は 0～65535 です。0 が指定された場合、イベントでアラームが発生しません。

owner *text*: エントリオーナを指定します。設定範囲は 1～127 文字です。大文字、小文字を区別します。

説明

rmon alarm コマンドは RMON アラームテーブルのエントリを作成します。

undo rmon alarm コマンドは RMON アラームテーブルからエントリを削除します。

RMON アラームテーブルに最大 60 のエントリを作成することができます。

アラームエントリは固有のアラーム変数、サンプリング間隔、サンプリングタイプ、増加方向のしきい値あるいは減少方向のしきい値がある必要があります。エントリのすべてのパラメータが既存のエントリと同一である場合、アラームエントリを作成することができません。

アラーム状況に関連したイベントを発生させるため、**rmon event** コマンドでイベントを作成する必要があります。

RMON は指定されたサンプリング間隔でモニタ対象のアラーム変数をサンプリングします。予期されたしきい値とサンプリングされた値と比較し、以下の 1 つの処理を行います。

- サンプリングした値が増加方向のしきい値以上である場合、増加方向のアラームに関連したイベントを発生します。
- サンプリングした値が減少方向のしきい値以下である場合、減少方向のアラームに関連したイベントを発生します。

例

GigabitEthernet 1/0/1 でアラームテーブルにエントリ 1 を作成します。サンプリングタイプを absolute （絶対値）にし、オブジェクト ID 1.3.6.1.2.1.16.1.1.1.4.1 を 10 秒間隔でサンプリングします。サンプリングした値が上昇しきい値 5000 以上になった場合、増加方向のアラームイベントをロギングします。サンプリングした値が 5 以下である場合、アクションは発生しません。

<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

この例では、1.3.6.1.2.1.16.1.1.1.4.1 を etherStatsOctets に置き換えることができます。ここで 1 はインタフェースのエントリインデックスの統計情報です。**rmon statistics 5** コマンドを実行した場合、1.3.6.1.2.1.16.1.1.1.4.5 を置き換えるために etherStatsOctets を使用します。

関連コマンド

- **display rmon alarm**

- **rmon event**

6.1.8 rmon event

Syntax

rmon event *entry-number* [**description** *string*] { **log** | **log-trap** *security-string* | **none** | **trap** *security-string* } [**owner** *text*]

undo rmon event *entry-number*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

entry-number: アラームエントリのインデックスを指定します。設定範囲は 1～65535 です。

description *string*: イベントの説明を設定します。設定範囲は 1～127 文字です。大文字、小文字を区別します。

log: イベントが発生したとき、ログを取得します。

log-trap: イベントが発生したとき、ログを取得し、SNMP 通知を送信します。

security-string: SNMP コミュニティを指定します。設定範囲は 1～127 文字です。大文字、小文字を区別します。SNMP の設定に依存します。このパラメータは現在のソフトウェアバージョンでサポートしていません。

none: イベントが発生したとき、アクションを行いません。

trap: イベントが発生したとき、SNMP 通知を送信します。

owner *text*: エントリオーナを指定します。設定範囲は 1～127 文字です。大文字、小文字を区別します。

🕮 **メモ：**

security-string の SNMP コミュニティの設定は、コマンドで設定することができますが適用されません。システムは RMON の SNMP 通知を送信するとき、SNMP の設定を使用します。SNMP 通知の詳細は、オペレーションマニュアルのセクション 11 *システム管理*" *SNMP*" を参照してください。

説明

rmon event コマンドは RMON イベントテーブルのエントリを作成します。

undo rmon event コマンドは RMON イベントテーブルからエントリを削除します。

最大 60 のイベントエントリを作成することができます。

アラーム状況が発生したとき、アクションを指定するため、イベントエントリを標準あるいはプライベートアラームエントリに関連づけることができます。設定に依存して、イベントのログを取得し、SNMP 通知を送信することができます。

複数のアラームエントリに 1 つのイベントを関連づけることができます。

例

RMON イベントエントリを作成しますのイベント 10、エントリオーナ user1 を指定します。

<Switch> system-view

[Switch] rmon event 10 log owner user1

関連コマンド

- **display rmon event**
- **rmon alarm**
- **rmon prialarm**

6.1.9 rmon history

Syntax

rmon history *entry-number* **buckets** *number* **interval** *sampling-interval* [**owner** *text*]

undo rmon history *entry-number*

デフォルト

設定なし

View

Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

entry-number: 履歴管理エントリのインデックスを指定します。設定範囲は 1～65535 です。

buckets *number*: エントリのために記録されるサンプルの予期する最大数を指定します。設定範囲は 1～65535 です。RMON は各履歴管理エントリで 50 のサンプルを記録することができます。予期したバケットサイズが有効な履歴テーブルサイズを超過した場合、RMON はバケットサイズをできるだけ、予期したバケットサイズに近づけます。しかし 50 を超過することはできません。たとえば、予期したバケットサイズを 55 に設定し、有効なバケットサイズが 30 である場合、履歴管理エントリのバケットサイズは 30 となります。

interval *sampling-interval*: サンプリング間隔を指定します。設定範囲は 5～3600 秒です。

owner *text*: エントリオーナを指定します。設定範囲は 1～127 文字です。大文字、小文字を区別します。

説明

rmon history コマンドは RMON 履歴管理テーブルのエントリを作成します。

undo rmon history コマンドは RMON 履歴管理テーブルからエントリを削除します。

レイヤ 2 Ethernet インタフェースあるいはレイヤ 3 Ethernet インタフェースでのみ RMON 履歴管理エントリを作成することができます。

システムで最大 100 の履歴管理エントリを作成することができます。

Ethernet インタフェースで履歴管理エントリがある場合、RMON はインタフェースで定期的にパケットの統計情報をサンプリングし、履歴テーブルにサンプルを記録します。履歴管理エントリのバケットサイズが最大になったとき、RMON は古いサンプルを新しいサンプルに上書きします。

1 つのインタフェースで複数の履歴管理エントリを設定することができますが、エントリ数とサンプリング間隔を変更する必要があります。

例

GigabitEthernet 1/0/1 で RMON 履歴管理テーブルのエントリ 1 を作成します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] rmon history 1 buckets 10 interval 5 owner user1

関連コマンド

display rmon history

6.1.10 rmon prialarm

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*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

entry-number: アラームエントリのインデックスを指定します。設定範囲は 1～65535 です。

prialarm-formula: プライベートアラーム変数を指定します。設定範囲は 1～255 文字です。変数の式はドット（.）始まる OID で示されます。たとえば、(.1.3.6.1.2.1.2.1.10.1）*8 です。この変数は、加減乗除の四則演算を行うことができます。演算の結果は長整数になります。エラーを防ぐため、演算の各段階の結果が、以下の値になるようにしてください。

- 式の変数の値が整数
- 設定範囲各計算のステップが long 整数

prialarm-des: エントリの説明を設定します。設定範囲は 1～127 文字です。大文字、小文字を区別します。

sampling-interval: サンプリング間隔を指定します。設定範囲は 10～65535 秒です。

absolute: 絶対値のサンプリングを指定します。RMON はサンプリング間隔の両端で増加方向のしきい値と減少方向のしきい値を比較します。

delta: 相対値のサンプリングを指定します。RMON は現在の値から前に取得したサンプル値を引き、増加方向と減少方向のしきい値の差異を比較します。

startup-alarm: アラームエントリが有効なときに作成されるアラームを指定します。アラームを指定しない場合、RMON は以下を行います。

- 最初のサンプルが増加方向のしきい値を交差したとき、増加方向のアラームを作成します。

- 最初のサンプルが減少方向のしきい値を交差したとき、減少方向のアラームを作成します。

rising: エントリが有効になったのち、最初にサンプルが増加方向のしきい値以上になった場合に、増加方向のアラームを作成します。

falling: エントリが有効になったのち、最初にサンプルが減少方向のしきい値以下になった場合に、減少方向のアラームを作成します。

rising-falling: 最初のサンプルが増加方向のしきい値と交差した場合、増加方向のアラームを作成します。あるいは最初のサンプルが減少方向のしきい値と交差した場合、減少方向のアラームを作成します。

rising-threshold *threshold-value1 event-entry1*: 増加方向のしきい値を指定します。*threshold-value1* の設定範囲は–2147483648 ～ +2147483647 です。*event-entry1* は増加方向のしきい値が交差したとき発生するイベントのインデックスを示します。*event-entry1* の設定範囲は 0～65535 です。0 が指定された場合、イベントでアラームが発生しません。

falling-threshold *threshold-value2 event-entry2*: 減少方向のしきい値を指定します。*threshold-value2* の設定範囲は–2147483648 ～ +2147483647 です。*event-entry2* は減少方向のしきい値が交差したとき発生するイベントのインデックスを示します。*event-entry2* の設定範囲は 0～65535 です。0 が指定された場合、イベントでアラームが発生しません。

forever: 無期限のエントリを指定します。RMON は手動で削除するまで無期限のプライベートアラームエントリを保持します。

cycle *cycle-period*: エントリの有効期限を指定します。設定範囲は 0～4294967 秒です。RMON は有効期限が終了したとき、エントリを削除します。

owner *text*: エントリオーナを指定します。設定範囲は 1～127 文字です。大文字、小文字を区別します。

説明

rmon prialarm コマンドはプライベートアラームテーブルのエントリを作成します。

undo rmon prialarm コマンドはプライベートアラームテーブルからエントリを削除します。

最大 50 のプライベートアラームエントリを作成することができます。

アラームエントリは固有のアラーム変数、サンプリング間隔、サンプリングタイプ、増加方向のしきい値あるいは減少方向のしきい値がある必要があります。エントリのすべてのパラメータが既存のエントリと同一である場合、アラームエントリを作成することができません。

アラーム状況に関連したイベントを発生させるため、**rmon event** コマンドでイベントを作成する必要があります。

RMON エージェントは変数をサンプリングし、プライベートアラームエントリをもとにしてアラームのアクションを行います。

1) プライベートアラームの式で指定された変数を定期的にサンプリングします。

2) 式でサンプリングした値を処理します。
3) 計算結果と予期されたしきい値を比較し、以下のアクションの 1 つを行います。
   - □ 結果が増加方向のしきい値以上である場合、増加方向のアラームに関連したイベントを発生します。
   - □ 結果が減少方向のしきい値以下である場合、減少方向のアラームに関連したイベントを発生します。

例

GigabitEthernet 1/0/1 で入力パケットの総数と入力ブロードキャストの割合をモニタするため、無期限のプライベートアラームエントリを追加します。割合が 80%を超過したとき、増加方向のアラームイベントのログを取得し、割合が 5%以下になったとき、アクションを行いません。式は（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）です。ここで 1.3.6.1.2.1.16.1.1.1.6.1 はオブジェクトインスタンス etherStatsBroadcastPkts.1 の OID です。1.3.6.1.2.1.16.1.1.1.5.1 はオブジェクトインスタンス etherStatsPkts.1 の OID です。

<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

変数の OID の最後の数はインタフェースのエントリインデックスの統計情報と同一にする必要があります。たとえば、**rmon statistics 5** コマンドを実行するとき、それぞれ 1.3.6.1.2.1.16.1.1.1.6.1 、 1.3.6.1.2.1.16.1.1.1.5.1 を 1.3.6.1.2.1.16.1.1.1.6.5 、1.3.6.1.2.1.16.1.1.1.5.5 に置き換えます。

関連コマンド

- **display rmon prialarm**
- **rmon event**

6.1.11 rmon statistics

Syntax

rmon statistics *entry-number* [**owner** *text*]

undo rmon statistics *entry-number*

デフォルト

設定なし

View

Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

entry-number: アラームエントリのインデックスを指定します。設定範囲は 1～65535 です。

owner *text*: エントリオーナを指定します。設定範囲は 1～127 文字です。大文字、小文字を区別します。

説明

rmon statistics コマンドは RMON 統計情報テーブルのエントリを作成します。

undo rmon statistics コマンドは RMON 統計情報テーブルからエントリを削除します。

各 RMON 統計情報テーブルエントリは、インタフェースで収集したトラフィックを現在の時間まで累積した統計情報の合計です。統計情報はコリジョン、過大サイズの CRC エラーパケットの数、過大サイズのパケット数、過小サイズのパケット数、ブロードキャストパケット数、マルチキャストパケット数、受信したバイト数、受信したパケット数を含みます。統計情報は、再起動で削除されます。

RMON 統計情報のテーブルを表示する場合、**display rmon statistics** コマンドを使用します。

各インタフェースで 1 つの統計情報のエントリを作成することができます。

例

GigabitEthernet 1/0/1 でインデックス 20、オーナ **user1** の RMON 統計情報エントリを作成します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] rmon statistics 20 owner user1

関連コマンド

display rmon statistics

目次

このセクションのページは **11-x-x** です。

7 章 NETCONF 7-1
7.1.1 netconf log 7-1
7.1.2 netconf soap enable 7-3
7.1.3 netconf ssh server enable 7-4
7.1.4 xml 7-4

7章 NETCONF

7.1.1 netconf log

Syntax

netconf log source { **all** | { **agent** | **soap** | **web** } * } { **protocol-operation** { **all** | { **action** | **config** | **get** | **session** | **set** | **syntax** | **others** } * } | **row-operation** | **verbose** }

undo netconf log source { **all** | { **agent** | **soap** | **web** } * } { **protocol-operation** { **all** | { **action** | **config** | **get** | **session** | **set** | **syntax** | **others** } * } | **row-operation** | **verbose** }

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

パラメータ

source: プロトコルを使用するクライアントを表す NETCONF オペレーションソースを指定します。

- **all**: すべてのプロトコルを使用する NETCONF クライアントを指定します。
- **agent**: Telnet、SSH、コンソール、または SSH 経由の NETCONF を使用するクライアントを指定します。
- **soap**: SOAP over HTTP または SOAP over HTTPS を使用するクライアントを指定します。
- **web**: Web を使用するクライアントを指定します。

protocol-operation: 特定のタイプの NETCONF オペレーションに対するリクエストとリプライを記録します。

- **all**: NETCONF テストのすべてのタイプを指定します。
- **action**: <action>テストを指定します。
- **config:** <CLI>、<save>、<load>、<rollback>、<lock>、<unlock>、および<save-point>テストなど、設定に関連した NETCONF テストを指定します。
- **get:** <get>、<get-config>、<get-bulk>、<get-bulk-config>、および<get-sessions>の各テストを含む、データ取得関連の NETCONF テストを指定します。

- **session**: <kill-session>および<close-session>テスト、hello メッセージによる機能交換など、セッション関連の NETCONF テストを指定します。
- **set**: すべての<edit-config>テストを指定します。
- **syntax**: XML およびスキーマエラーを含む要求を指定します。
- **others**: **action**、**config**、**get**、**set**、**session**、および **syntax** で指定されたテスト以外の NETCONF テストを指定します。

row-operation: <action>および<edit-config>テストの行テストをログに記録します。

verbose: NETCONF テストのタイプに対する要求と応答の詳細情報を記録します。これには、フォーマットが正しい要求のパケットの内容や、失敗した<edit-config>テストに関するエラー情報が含まれます。

説明

netconf log コマンドは、NETCONF ロギングを有効にします。

undo netconf log コマンドは、指定した NETCONF オペレーションソースおよび NETCONF オペレーションの設定を削除します。

protocol-operation を指定した場合、装置は一致したテストとその結果をそれぞれログに記録します。たとえば、VLAN3 から 5 を作成するために NETCONF オペレーションを実行すると、装置は以下のログメッセージを出力します。

```
%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.
```

row-operation を指定した場合、装置は<action>または<edit-config>テストの各行テストをログに記録します。たとえば、NETCONF テストを実行して VLAN 3～5 を作成すると、装置は次のログメッセージを出力します。

```
%Mar 31 17:50:02:608 2017 NEC XMLSOAP/6/EDIT-CONFIG: User (test, 192.168.100.20,
session ID 1), message ID=100, operation=create VLAN/VLANs (ID=3),
result=Succeeded. No attributes.
%Mar 31 17:50:02:609 2017 NEC XMLSOAP/6/EDIT-CONFIG: User (test, 192.168.100.20,
session ID 1), message ID=100, operation=create VLAN/VLANs (ID=4),
result=Succeeded. No attributes.
%Mar 31 17:50:02:611 2017 NEC XMLSOAP/6/EDIT-CONFIG: User (test, 192.168.100.20,
session ID 1), message ID=100, operation=create VLAN/VLANs (ID=5),
result=Succeeded. No attributes.
```

NETCONF が作成されたログを information center に正しく送信するには、information center も設定する必要があります。information center の設定の詳細については、オペレーションマニュアルのセクション 11 *システム管理*を参照してください。

例

エージェントクライアントから送信された NETCONF の編集設定情報を記録するように装置を設定します。

<Switch> system-view

[Switch] netconf log source agent protocol-operation set

7.1.2 netconf soap enable

Syntax

netconf soap { **http** | **https** } **enable**

undo netconf soap { **http** | **https** } **enable**

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

パラメータ

http: HTTP 上の SOAP で NETCONF を指定します。

https: HTTPS 上の SOAP で NETCONF を指定します。

説明

netconf soap enable コマンドは、SOAP 上で NETCONF を有効にします。

undo netconf soap enable コマンドは、SOAP 上で NETCONF を無効にします。

このコマンドを使用すると、装置は HTTP あるいは HTTPS パケットの SOAP でカプセル化されている NETCONF メッセージを解決できます。

例

HTTP 上の SOAP で NETCONF を有効にします。

<Switch> system-view

[Switch] netconf soap http enable

7.1.3 netconf ssh server enable

Syntax

netconf ssh server enable

undo netconf ssh server enable

デフォルト

無効

View

システムビュー

定義済みユーザロール

network-admin

説明

netconf ssh server enable コマンドは、SSH 経由で NETCONF を有効にします。

undo netconf ssh server enable コマンドは、SSH 経由で NETCONF を無効にします。

この機能により、SSH クライアントを使って NETCONF を SSH サブシステムとして呼び出すことができます。その後、xml コマンドを使用せずに XML メッセージを直接使用して NETCONF テストを実行できます。

このコマンドを実行する前に、装置の **scheme** としてユーザの認証モードを設定します。その後、NETCONF-over-SSH 対応のユーザ端末は、SSH を介した NETCONF を介して装置にアクセスできます。

機能セット **urn**：**ietf**：**params**：**netconf**：**base**：**1.0** のみが利用可能です。それは装置とユーザ端末の両方によってサポートされています。

例

SSH で NETCONF を有効にします。

<Switch> system-view

[Switch] netconf ssh server enable

7.1.4 xml

Syntax

xml

View

User view

定義済みユーザロール

network-admin

network-operator

説明

xml コマンドは、XML ビューに移行します。

XML ビューでは、NETCONF メッセージを使用して装置を設定するか、装置からデータを取得します。実行できる NETCONF テストは、表 7-1 に示すように、ユーザロールによって異なります。

表 7-1 事前定義されたユーザ役割で使用可能な NETCONF テスト

ユーザの役割	NETCONF オペレーション
network-admin	すべてのNETCONFオペレーションです。
network-operator	• Get • Get-bulk • Get-bulk-config • Get-config • Get-sessions • Close-session

XML ビューで NETCONF メッセージのフォーマットが正しいことを確認するには、NETCONF メッセージを手動で入力しないでください。メッセージをコピーして貼り付けます。

装置が NETCONF オペレーションを実行している間は、NETCONF メッセージの貼り付けや **Enter** キーの押下などの他のオペレーションを実行しないでください。

装置が NETCONF メッセージを識別するためには、各 NETCONF メッセージの最後にエンドマーク **]]>]]>**を追加する必要があります。

XML ビューに入ると、装置は自動的に NETCONF 機能をクライアントに配信します。それに応じて、サポートされている NETCONF 機能を装置に通知するようにクライアントを設定する必要があります。機能交換の後、クライアントを使用して装置を設定できます。

NETCONF メッセージは、装置の NETCONF XML API リファレンスの XML 形式の要件と意味および構文の要件に準拠している必要があります。サードパーティ製のソフトウェアを使用して NETCONF メッセージを作成し、設定を確実に成功させます。

XML ビューを終了するには、**quit** コマンドの代わりに NETCONF メッセージを使用してください。

ユーザ行またはユーザ行クラスのビューで **escape-key** コマンドを使用してショートカットキー（デフォルトでは **Ctrl + C**）を設定している場合は、NETCONF メッセージにショートカットキーの文字列を含めないでください。NETCONF メッセージにショートカットキーの文字列が含まれている場合、XML ビューの関連設定が影響を受ける可能性があります。たとえば、ユーザラインビューでは、**escape-key a** コマンドを使用して「a」をショートカットキーとして設定しました。 NETCONF メッセージに文字 "a"が含まれていると、メッセージ内の最後の "a"以降の内容のみを処理できます

例

XML ビューに移行します。

<Switch> xml

```
<?xml version="1.0" encoding="UTF-8"?><hello
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"><capabilities><capability>urn
:ietf:params:netconf:base:1.1</capability><capability>urn:ietf:params:netconf
:writable-running</capability><capability>urn:ietf:params:netconf:capability:
notification:1.0</capability><capability>urn:ietf:params:netconf:capability:v
alidate:1.1</capability><capability>urn:ietf:params:netconf:capability:interl
eave:1.0</capability><capability>urn:nec:params:netconf:capability:nec-netcon
f-ext:1.0</capability></capabilities><session-id>1</session-id></hello>]]>]]>
```

クライアントでサポートされている NETCONF 機能ついて装置に通知してください。

```
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <capabilities>
    <capability>
          urn:ietf:params:netconf:base:1.0
    </capability>
  </capabilities>
</hello>]]>]]>
```

クライアントでサポートされている NETCONF 機能を装置に通知します。

```
hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <capabilities>
    <capability>
          urn:ietf:params:netconf:base:1.0
    </capability>
  </capabilities>
</hello>]]>]]>
```

XML ビューを終了します。

```
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
```

```
  <close-session/>
  </close-session>
</rpc>]]>]]>
```

<Switch>

目次

このセクションのページは **11-x-x** です。

8章 プロセスモニタリングとメンテナンス 8-1
8.1 プロセスモニタリングとメンテナンス設定コマンド 8-1
8.1.1 display exception context 8-1
8.1.2 display exception filepath 8-6
8.1.3 display kernel deadloop 8-7
8.1.4 display kernel exception 8-11
8.1.5 display kernel reboot 8-14
8.1.6 exception filepath 8-18
8.1.7 process core 8-19
8.1.8 reset exception context 8-20
8.1.9 reset kernel deadloop 8-20
8.1.10 reset kernel exception 8-21
8.1.11 reset kernel reboot 8-22

8章 プロセスモニタリングとメンテナンス

8.1 プロセスモニタリングとメンテナンス設定コマンド

8.1.1 display exception context

Syntax

display exception context [**count** *value*] [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

パラメータ

count *value*: コンテキスト情報のエントリを指定します。設定範囲は 1～20 です。デフォルトは 1 です。

slot *slot-number*: IRF スタックメンバ装置のメンバ ID を指定します。指定しない場合、IRF スタックのマスタ装置が指定されます。

説明

display exception context コマンドはプロセス例外に関するコンテキスト情報を表示します。

システムは、各コアファイルのコンテキスト情報エントリを作成します。コンテキスト情報エントリは、プロセス ID、クラッシュ時間、コアファイルのディレクトリ、スタック情報、レジスタ情報が含まれます。

例

x86 ベースの 32 ビット端末のプロセス例外に関するコンテキスト情報を表示します。

<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
```

x86 ベースの 64 ビット端末のプロセス例外に関するコンテキスト情報を表示します。

<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
```

Power PC ベースの 32 ビット端末のプロセス例外に関するコンテキスト情報を表示します。

<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
```

Power PC ベースの 64 ビット端末のプロセス例外に関するコンテキスト情報を表示します。

<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
```

MIPS ベースの 32 ビット端末のプロセス例外に関するコンテキスト情報を表示します。

<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   t3:0xffffff8
   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
```

MIPS ベースの 64 ビット端末のプロセス例外に関するコンテキスト情報を表示します。

<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:0x0000000000400ff3       lo:0xdf3b645a1cac08c9
       hi:0x000000000000007f      bad:0x000000555589ba84
    cause:0x0000000000800020       pc:0x0000005555a3bcb4
```

表 8-1 コマンド出力

フィールド	説明
Crashed PID	クラッシュプロセスのIDです。

フィールド	説明
Crash signal	クラッシュを引き起こした信号です。 ● **SIGABRT**—中断です。 ● **SIGBUS**—バスエラーです。 ● **SIGFPE**—間違った四則演算です。 ● **SIGILL**—不正なハードウェア指令です。 ● **SIGQUIT**—コントロール端末によってquit信号が送信されました。 ● **SIGSEGV**—不正なメモリアクセスです。 ● **SIGSYS**—不正なシステムコールです。 ● **SIGTRAP**—トラップメッセージです。 ● **SIGXCPU**—CPU使用率の制限が超過しました。 ● **SIGXFSZ**—ファイルサイズの制限が超過しました。 ● **SIGUNKNOW**—不明な理由です。
Crash time	コアファイルが作成された時間です。
Core file path	コアファイルが保存されているディレクトリです。
Backtrace stopped	すべてのスタック情報が表示されています。

関連コマンド

reset exception context

8.1.2 display exception filepath

Syntax

display exception filepath [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

パラメータ

slot *slot-number*: IRF スタックメンバ装置のメンバ ID を指定します。指定しない場合、IRF スタックのマスタ装置が指定されます。

説明

display exception filepath コマンドはコアファイルのディレクトリを表示します。

例

コアファイルのディレクトリを表示します。

<Switch> display exception filepath slot 1

```
The exception filepath on slot 1 is flash:.
```

8.1.3 display kernel deadloop

Syntax

display kernel deadloop *show-number* [*offset*] [**verbose**] [**slot** *slot-number* [**cpu** *cpu-number*]]

View

すべての view

定義済みユーザロール

network-admin

パラメータ

show-number: 表示するデッドループの数を指定します。設定範囲は 1～20 です。

offset: 開始デッドループと最新デッドループの間のオフセットを指定します。設定範囲は 0～19 です。デフォルトは 0 です。

verbose: 詳細情報を表示します。指定しない場合、概要情報を表示します。

slot s*lot-number*: IRF スタックメンバ装置を ID で指定します。指定しない場合、マスタ装置のカーネルスレッドデッドループ情報を表示します。

cpu *cpu-number*: CPU を番号で指定します。

説明

display kernel deadloop コマンドはカーネルスレッドのデッドループ情報を表示します。

例

最新のカーネルスレッドデッドループに関する概要情報を表示します。

<Switch> display kernel deadloop 1

```
----------------- Deadloop record 1 -----------------
Description         : BUG: soft lockup - CPU#0 stuck for 61! [comsh: 16306]
Recorded at         : 2013-05-01  11:16:00.823018
```

```
Occurred at         : 2013-05-01  11:16:00.823018
Instruction address  : 0x4004158c
Thread              : comsh (TID: 16306)
Context             : thread context
Slot               : 1
Cpu                : 0
VCPU ID             : 0
Kernel module info   : module name (mrpnc) module address (0xe332a000)
```

最新のカーネルスレッドデッドループに関する詳細情報を表示します。

<Switch> display kernel deadloop 1 verbose

```
----------------- Deadloop record 1 -----------------
Description         : BUG: soft lockup - CPU#0 stuck for 61! [comsh: 16306]
Recorded at         : 2013-05-01  11:16:00.823018
Occurred at         : 2013-05-01  11:16:00.823018
Instruction address  : 0x4004158c
Thread              : comsh (TID: 16306)
Context             : thread context
Slot               : 1
Cpu                : 0
VCPU ID             : 0
Kernel module info   : module name (mrpnc) module address (0xe332a000)

Last 5 thread switches : migration/0 (11:16:00.823018)-->
                         swapper (11:16:00.833018)-->
                         kthreadd (11:16:00.833518)-->
                         swapper (11:16:00.833550)-->
                         disk (11:16:00.833560)

Register content:
Reg:      r0, Val = 0x00000000 ; Reg:      r1, Val = 0xe2be5ea0 ;
Reg:      r2, Val = 0x00000000 ; Reg:      r3, Val = 0x77777777 ;
Reg:      r4, Val = 0x00000000 ; Reg:      r5, Val = 0x00001492 ;
Reg:      r6, Val = 0x00000000 ; Reg:      r7, Val = 0x0000ffff ;
Reg:      r8, Val = 0x77777777 ; Reg:      r9, Val = 0x00000000 ;
Reg:     r10, Val = 0x00000001 ; Reg:     r11, Val = 0x0000002c ;
Reg:     r12, Val = 0x057d9484 ; Reg:     r13, Val = 0x00000000 ;
Reg:     r14, Val = 0x00000000 ; Reg:     r15, Val = 0x02000000 ;
Reg:     r16, Val = 0xe2be5f00 ; Reg:     r17, Val = 0x00000000 ;
Reg:     r18, Val = 0x00000000 ; Reg:     r19, Val = 0x00000000 ;
Reg:     r20, Val = 0x024c10f8 ; Reg:     r21, Val = 0x057d9244 ;
Reg:     r22, Val = 0x00002000 ; Reg:     r23, Val = 0x0000002c ;
Reg:     r24, Val = 0x00000002 ; Reg:     r25, Val = 0x24000024 ;
```

```
Reg:      r26, Val = 0x00000000 ; Reg:      r27, Val = 0x057d9484 ;
Reg:      r28, Val = 0x0000002c ; Reg:      r29, Val = 0x00000000 ;
Reg:      r30, Val = 0x0000002c ; Reg:      r31, Val = 0x00000000 ;
Reg:       cr, Val = 0x84000028 ; Reg:      nip, Val = 0x057d9550 ;
Reg:      xer, Val = 0x00000000 ; Reg:       lr, Val = 0x0186eff0 ;
Reg:      ctr, Val = 0x682f7344 ; Reg:      msr, Val = 0x00784b5c ;
Reg:     trap, Val = 0x0000b030 ; Reg:      dar, Val = 0x77777777 ;
Reg:    dsisr, Val = 0x40000000 ; Reg:   result, Val = 0x00020300 ;

Dump stack (total 1024 bytes, 16 bytes/line):
0xe2be5ea0: 02 be 5e c0 24 00 00 24 00 00 00 00 05 7d 94 84
0xe2be5eb0: 00 00 00 04 00 00 00 00 00 00 00 28 05 8d 34 c4
0xe2be5ec0: 02 be 60 a0 01 86 ef f0 00 00 00 00 00 00 00 00
0xe2be5ed0: 02 04 05 b4 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5ee0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5ef0: 95 47 73 35 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5f00: a0 e1 64 21 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5f10: 00 00 00 00 00 00 00 00 00 00 00 00 01 e9 00 00
0xe2be5f20: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5f30: 00 00 00 00 00 00 00 00 02 be 66 c0 02 be 66 d0
0xe2be5f40: 02 be 61 e0 00 00 00 02 00 00 00 00 02 44 b3 a4
0xe2be5f50: 02 be 5f 90 00 00 00 08 02 be 5f e0 00 00 00 08
0xe2be5f60: 02 be 5f 80 00 ac 1b 14 00 00 00 00 00 00 00 00
0xe2be5f70: 05 b4 5f 90 02 be 5f e0 00 00 00 30 02 be 5f e0
0xe2be5f80: 02 be 5f c0 00 ac 1b f4 00 00 00 00 02 45 00 00
0xe2be5f90: 00 03 00 00 00 00 00 00 02 be 5f e0 00 00 00 30
0xe2be5fa0: 02 be 5f c0 00 ac 1b 14 61 f1 2e ae 02 45 00 00
0xe2be5fb0: 02 44 b3 74 02 be 5f d0 00 00 00 30 02 be 5f e0
0xe2be5fc0: 02 be 60 60 01 74 ff f8 00 00 00 00 00 00 08 00
0xe2be5fd0: 02 be 5f f0 00 e8 93 7e 02 be 5f f8 02 be 5f fc
0xe2be5fe0: 00 00 00 00 00 00 00 00 00 00 00 00 02 be 60 18
0xe2be5ff0: 02 be 60 10 00 e9 65 98 00 00 00 58 00 00 2a 4f
0xe2be6000: 02 be 60 10 00 00 00 00 00 00 00 00 02 be 60 68
0xe2be6010: 02 be 60 40 00 e8 c6 a0 00 00 11 17 00 00 00 00
0xe2be6020: 02 be 60 40 00 00 00 00 00 00 00 00 02 be 60 98
0xe2be6030: 02 27 00 00 00 00 00 00 00 00 00 00 02 be 60 68
0xe2be6040: 02 be 60 60 00 00 00 01 00 00 b0 30 02 be 60 98
0xe2be6050: 00 00 00 04 02 21 00 00 00 00 00 00 01 e9 00 00
0xe2be6060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be6070: 00 00 00 00 00 00 00 00 02 be 66 c0 02 be 66 d0
0xe2be6080: 02 be 61 e0 00 00 00 02 00 00 00 00 02 be 61 70
0xe2be6090: 00 00 00 00 02 21 00 00 05 8d 34 c4 05 7d 92 44
```

```
Call trace:
Function Address = 0x8012a4b4
Function Address = 0x8017989c
Function Address = 0x80179b30
Function Address = 0x80127438
Function Address = 0x8012d734
Function Address = 0x80100a00
Function Address = 0xe0071004
Function Address = 0x8016ce0c
Function Address = 0x801223a0

Instruction dump:
41a2fe9c 812300ec 800200ec 7f890000 409efe8c 80010014 540b07b9 40a2fe80
4bfffe6c 80780290 7f64db78 4804ea35 <807f002c> 38800000 38a00080 3863000c
```

表 8-2 コマンド出力

フィールド	説明
Description	CPU番号、スレッド実行時間、スレッド名、スレッド番号など、カーネルスレッドデッドループの説明です。
Recorded at	カーネルスレッドデッドループが記録された時間 (マイクロ秒単位の精度)です。
Occurred at	カーネルスレッドのデッドループが発生した時刻 (マイクロ秒精度)です。
Instruction address	カーネルスレッドデッドループの命令アドレスです。
Thread	カーネルスレッドデッドループの名前と番号です。
Context	カーネルスレッドデッドループのコンテキストです。
Cpu	カーネルスレッドが実行されたCPUの番号です。
VCPU ID	カーネルスレッドが実行されたCPUの番号です。
Kernel module info	カーネルスレッドデッドループが検出されたときにロードされたカーネルモジュールに関する情報です。次の情報が含まれます。 ● **Module name**—カーネルモジュール名です。 ● **Module address**—モジュールのメモリアドレスです。
Last 5 thread switches	カーネルスレッドのデッドループが検出される前に、最後の5つのカーネルスレッドがCPUに切り替えられます。これには、カーネルスレッド名と、マイクロ秒単位の精度でのカーネルスレッドの切り替え時間が含まれます。

フィールド	説明
Register content	登録情報です。 ● **Reg**—レジスタの名前です。 ● **Val**—レジスタに保存された値です。
Dump stack	スタック情報です。
Call trace	各レベルで呼び出された関数の命令アドレスを示す関数呼び出しスタック情報です。
Instruction dump	カーネルスレッドデッドループが検出されたときの命令コードです。**ffffffff**は不正な命令コードを示します。
No information to display	カーネルスレッドのデッドループ情報がありません。

関連コマンド

reset kernel deadloop

8.1.4 display kernel exception

Syntax

display kernel exception *show-number* [*offset*] [**verbose**] [**slot** *slot-number* [**cpu** *cpu-number*]]

View

すべての view

定義済みユーザロール

network-admin

パラメータ

show-number: 表示するカーネル例外の数を指定します。設定範囲は 1～20 です。

offset: 開始例外と最新例外の間のオフセットを指定します。設定範囲は 0～19 です。デフォルトは 0 です。

verbose: 詳細情報を表示します。指定しない場合、コマンドは概要情報を表示します。

slot *slot-number*: IRF スタックメンバ装置を ID で指定します。指定しない場合、マスタ装置のカーネルスレッド例外情報を表示します。

cpu *cpu-number*: CPU を番号で指定します。

説明

display kernel exception コマンドはカーネルスレッド例外情報を表示します。

実行中のカーネルスレッドに例外が発生すると、システムは自動的に例外情報を記録します。

例

最新のカーネルスレッド例外に関する概要情報を表示します。

<Switch> display kernel exception 1

```
----------------- Exception record 1 -----------------
Description         : Oops[#0]
Recorded at         : 2013-05-01  11:16:00.823018
Occurred at         : 2013-05-01  11:16:00.823018
Instruction address  : 0x4004158c
Thread              : comsh (TID: 16306)
Context             : thread context
Slot               : 1
Cpu                : 0
VCPU ID             : 0
Kernel module info   : module name (mrpnc) module address (0xe332a000)
                     module name (disk) module address (0xe00bd000)
```

最新のカーネルスレッド例外に関する詳細情報を表示します。

<Switch> display kernel exception 1 verbose

```
----------------- Exception record 1 -----------------
Description         : Oops[#0]
Recorded at         : 2013-05-01  11:16:00.823018
Occurred at         : 2013-05-01  11:16:00.823018
Instruction address  : 0x4004158c
Thread              : comsh (TID: 16306)
Context             : thread context
Slot               : 1
Cpu                : 0
VCPU ID             : 0
Kernel module info   : module name (mrpnc) module address (0xe332a000)
                     module name (12500) module address (0xe00bd000)

Last 5 thread switches : migration/0 (11:16:00.823018)-->
                       swapper (11:16:00.833018)-->
                       kthreadd (11:16:00.833518)-->
                       swapper (11:16:00.833550)-->
                       disk (11:16:00.833560)

Register content:
Reg:      r0, Val = 0x00000000 ; Reg:      r1, Val = 0xe2be5ea0 ;
Reg:      r2, Val = 0x00000000 ; Reg:      r3, Val = 0x77777777 ;
```

```
Reg:      r4, Val = 0x00000000 ; Reg:      r5, Val = 0x00001492 ;
Reg:      r6, Val = 0x00000000 ; Reg:      r7, Val = 0x0000ffff ;
Reg:      r8, Val = 0x77777777 ; Reg:      r9, Val = 0x00000000 ;
Reg:     r10, Val = 0x00000001 ; Reg:     r11, Val = 0x0000002c ;
Reg:     r12, Val = 0x057d9484 ; Reg:     r13, Val = 0x00000000 ;
Reg:     r14, Val = 0x00000000 ; Reg:     r15, Val = 0x02000000 ;
Reg:     r16, Val = 0xe2be5f00 ; Reg:     r17, Val = 0x00000000 ;
Reg:     r18, Val = 0x00000000 ; Reg:     r19, Val = 0x00000000 ;
Reg:     r20, Val = 0x024c10f8 ; Reg:     r21, Val = 0x057d9244 ;
Reg:     r22, Val = 0x00002000 ; Reg:     r23, Val = 0x0000002c ;
Reg:     r24, Val = 0x00000002 ; Reg:     r25, Val = 0x24000024 ;
Reg:     r26, Val = 0x00000000 ; Reg:     r27, Val = 0x057d9484 ;
Reg:     r28, Val = 0x0000002c ; Reg:     r29, Val = 0x00000000 ;
Reg:     r30, Val = 0x0000002c ; Reg:     r31, Val = 0x00000000 ;
Reg:      cr, Val = 0x84000028 ; Reg:     nip, Val = 0x057d9550 ;
Reg:     xer, Val = 0x00000000 ; Reg:      lr, Val = 0x0186eff0 ;
Reg:     ctr, Val = 0x682f7344 ; Reg:     msr, Val = 0x00784b5c ;
Reg:    trap, Val = 0x0000b030 ; Reg:     dar, Val = 0x77777777 ;
Reg:   dsisr, Val = 0x40000000 ; Reg:  result, Val = 0x00020300 ;

Dump stack (total 1024 bytes, 16 bytes/line):
0xe2be5ea0: 02 be 5e c0 24 00 00 24 00 00 00 00 05 7d 94 84
0xe2be5eb0: 00 00 00 04 00 00 00 00 00 00 00 28 05 8d 34 c4
0xe2be5ec0: 02 be 60 a0 01 86 ef f0 00 00 00 00 00 00 00 00
0xe2be5ed0: 02 04 05 b4 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5ee0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5ef0: 95 47 73 35 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5f00: a0 e1 64 21 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5f10: 00 00 00 00 00 00 00 00 00 00 00 00 01 e9 00 00
0xe2be5f20: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5f30: 00 00 00 00 00 00 00 00 02 be 66 c0 02 be 66 d0
0xe2be5f40: 02 be 61 e0 00 00 00 02 00 00 00 00 02 44 b3 a4
0xe2be5f50: 02 be 5f 90 00 00 00 08 02 be 5f e0 00 00 00 08
0xe2be5f60: 02 be 5f 80 00 ac 1b 14 00 00 00 00 00 00 00 00
0xe2be5f70: 05 b4 5f 90 02 be 5f e0 00 00 00 30 02 be 5f e0
0xe2be5f80: 02 be 5f c0 00 ac 1b f4 00 00 00 00 02 45 00 00
0xe2be5f90: 00 03 00 00 00 00 00 00 02 be 5f e0 00 00 00 30
0xe2be5fa0: 02 be 5f c0 00 ac 1b 14 61 f1 2e ae 02 45 00 00
0xe2be5fb0: 02 44 b3 74 02 be 5f d0 00 00 00 30 02 be 5f e0
0xe2be5fc0: 02 be 60 60 01 74 ff f8 00 00 00 00 00 00 08 00
0xe2be5fd0: 02 be 5f f0 00 e8 93 7e 02 be 5f f8 02 be 5f fc
0xe2be5fe0: 00 00 00 00 00 00 00 00 00 00 00 00 02 be 60 18
0xe2be5ff0: 02 be 60 10 00 e9 65 98 00 00 00 58 00 00 2a 4f
```

```
0xe2be6000: 02 be 60 10 00 00 00 00 00 00 00 02 be 60 68
0xe2be6010: 02 be 60 40 00 e8 c6 a0 00 00 11 17 00 00 00 00
0xe2be6020: 02 be 60 40 00 00 00 00 00 00 00 02 be 60 98
0xe2be6030: 02 27 00 00 00 00 00 00 00 00 00 02 be 60 68
0xe2be6040: 02 be 60 60 00 00 00 01 00 00 b0 30 02 be 60 98
0xe2be6050: 00 00 00 04 02 21 00 00 00 00 00 00 01 e9 00 00
0xe2be6060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be6070: 00 00 00 00 00 00 00 00 02 be 66 c0 02 be 66 d0
0xe2be6080: 02 be 61 e0 00 00 00 02 00 00 00 00 02 be 61 70
0xe2be6090: 00 00 00 00 02 21 00 00 05 8d 34 c4 05 7d 92 44

Call trace:
Function Address = 0x8012a4b4
Function Address = 0x8017989c
Function Address = 0x80179b30
Function Address = 0x80127438
Function Address = 0x8012d734
Function Address = 0x80100a00
Function Address = 0xe0071004
Function Address = 0x8016ce0c
Function Address = 0x801223a0

Instruction dump:
41a2fe9c 812300ec 800200ec 7f890000 409efe8c 80010014 540b07b9 40a2fe80
4bfffe6c 80780290 7f64db78 4804ea35 <807f002c> 38800000 38a00080 3863000c
```

コマンド出力の詳細については、表 8-2 を参照してください。

関連コマンド

reset kernel exception

8.1.5 display kernel reboot

Syntax

display kernel reboot *show-number* [*offset*] [**verbose**] [**slot** *slot-number* [**cpu** *cpu-number*]]

View

すべての view

定義済みユーザロール

network-admin

パラメータ

show-number:　表示するリブートの数を指定します。設定範囲は 1～20 です。

offset: 開始リブートと最新のリブートの間のオフセットを指定します。設定範囲は 0～19 です。デフォルトは 0 です。

verbose: 詳細情報を表示します。指定しない場合、コマンドは概要情報を表示します。

slot *slot-number*: IRF スタックメンバ装置を ID で指定します。指定しない場合、マスタ装置の再起動情報を表示します。メンバ装置の再起動情報は、マスタ装置のメモリに記録されます。マスタ装置の電源がオフになっている場合、再起動情報は失われます。

cpu *cpu-number*: CPU を番号で指定します。

説明

display kernel reboot コマンドはメンバ装置の再起動情報を表示します。

例

最新のリブートに関する概要情報を表示します。

<Switch> display kernel reboot 1

```
----------------- Reboot record 1 -----------------
Recorded at         : 2013-05-01  11:16:00.823018
Occurred at         : 2013-05-01  11:16:00.823018
Reason             : 0x31
Thread             : comsh (TID: 16306)
Context            : thread context
Slot               : 1
Target Slot         : 0
Cpu                : 0
VCPU ID            : 0
Kernel module info   : module name (mrpnc) module address (0xe332a000)
                       module name (12500) module address (0xe00bd000)
```

最新のリブートに関する詳細情報を表示します。

<Switch> display kernel reboot 1 verbose

```
----------------- Reboot record 1 -----------------
Recorded at         : 2013-05-01  11:16:00.823018
Occurred at         : 2013-05-01  11:16:00.823018
Reason             : 0x31
Thread             : comsh (TID: 16306)
Context            : thread context
Slot               : 1
Target Slot         : 0
Cpu                : 0
VCPU ID            : 0
```

```
Kernel module info   : module name (mrpnc) module address (0xe332a000)
                       module name (12500) module address (0xe00bd000)

Last 5 thread switches : migration/0 (11:16:00.823018)-->
                         swapper (11:16:00.833018)-->
                         kthreadd (11:16:00.833518)-->
                         swapper (11:16:00.833550)-->
                         disk (11:16:00.833560)

Dump stack (total 1024 bytes, 16 bytes/line):
0xe2be5ea0: 02 be 5e c0 24 00 00 24 00 00 00 00 05 7d 94 84
0xe2be5eb0: 00 00 00 04 00 00 00 00 00 00 00 28 05 8d 34 c4
0xe2be5ec0: 02 be 60 a0 01 86 ef f0 00 00 00 00 00 00 00 00
0xe2be5ed0: 02 04 05 b4 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5ee0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5ef0: 95 47 73 35 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5f00: a0 e1 64 21 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5f10: 00 00 00 00 00 00 00 00 00 00 00 00 01 e9 00 00
0xe2be5f20: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5f30: 00 00 00 00 00 00 00 00 02 be 66 c0 02 be 66 d0
0xe2be5f40: 02 be 61 e0 00 00 00 02 00 00 00 00 02 44 b3 a4
0xe2be5f50: 02 be 5f 90 00 00 00 08 02 be 5f e0 00 00 00 08
0xe2be5f60: 02 be 5f 80 00 ac 1b 14 00 00 00 00 00 00 00 00
0xe2be5f70: 05 b4 5f 90 02 be 5f e0 00 00 00 30 02 be 5f e0
0xe2be5f80: 02 be 5f c0 00 ac 1b f4 00 00 00 00 02 45 00 00
0xe2be5f90: 00 03 00 00 00 00 00 00 02 be 5f e0 00 00 00 30
0xe2be5fa0: 02 be 5f c0 00 ac 1b 14 61 f1 2e ae 02 45 00 00
0xe2be5fb0: 02 44 b3 74 02 be 5f d0 00 00 00 30 02 be 5f e0
0xe2be5fc0: 02 be 60 60 01 74 ff f8 00 00 00 00 00 00 08 00
0xe2be5fd0: 02 be 5f f0 00 e8 93 7e 02 be 5f f8 02 be 5f fc
0xe2be5fe0: 00 00 00 00 00 00 00 00 00 00 00 00 02 be 60 18
0xe2be5ff0: 02 be 60 10 00 e9 65 98 00 00 00 58 00 00 2a 4f
0xe2be6000: 02 be 60 10 00 00 00 00 00 00 00 00 02 be 60 68
0xe2be6010: 02 be 60 40 00 e8 c6 a0 00 00 11 17 00 00 00 00
0xe2be6020: 02 be 60 40 00 00 00 00 00 00 00 00 02 be 60 98
0xe2be6030: 02 27 00 00 00 00 00 00 00 00 00 00 02 be 60 68
0xe2be6040: 02 be 60 60 00 00 00 01 00 00 b0 30 02 be 60 98
0xe2be6050: 00 00 00 04 02 21 00 00 00 00 00 00 01 e9 00 00
0xe2be6060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be6070: 00 00 00 00 00 00 00 00 02 be 66 c0 02 be 66 d0
0xe2be6080: 02 be 61 e0 00 00 00 02 00 00 00 00 02 be 61 70
0xe2be6090: 00 00 00 00 02 21 00 00 05 8d 34 c4 05 7d 92 44
```

```
Call trace:
Function Address = 0x8012a4b4
Function Address = 0x8017989c
Function Address = 0x80179b30
Function Address = 0x80127438
Function Address = 0x8012d734
Function Address = 0x80100a00
Function Address = 0xe0071004
Function Address = 0x8016ce0c
Function Address = 0x801223a0
```

表 8-3 コマンド出力

フィールド	説明
Recorded at	再起動が記録された時刻です。単位はマイクロ秒です。
Occurred at	リブートが発生した時刻です。単位はマイクロ秒です。
Reason	再起動の理由です。
Thread	リブートが発生したときに実行されていたカーネルスレッドの名前と番号です。
Context	再起動が発生したコンテキストです。
Slot	再起動をトリガしたスロットの番号です。
Target Slot	再起動したスロットの番号です。
Cpu	再起動をトリガしたCPUの番号です。
VCPU ID	リブートをトリガしたCPUコアの数です。
Kernel module info	再起動時にロードされたカーネルモジュールに関する情報(カーネルモジュール名やメモリアドレスなど)です。
Last 5 thread switches	リブート前にCPUで発生した最後の5つのカーネルスレッドスイッチ (カーネルスレッド名とカーネルスレッドの切り替え時点を含む、マイクロ秒単位の精度)です。
Dump stack	再起動が発生したときに実行されていたスレッドのスタック情報です。
Call trace	関数呼び出しスタック情報です。
No information to display	再起動情報が存在しません。

関連コマンド

reset kernel reboot

8.1.6 exception filepath

Syntax

exception filepath *directory*

undo exception filepath *directory*

デフォルト

コアファイルのファイルは flash:/に保存されます。

View

User view

定義済みユーザロール

network-admin

パラメータ

directory: コアファイルを保存するディレクトリを指定します。

説明

exception filepath コマンドはコアファイルを保存するディレクトリを設定します。

undo exception filepath コマンドは指定されたディレクトリを削除します。

ディレクトリはマスタ装置のフラッシュのルートディレクトリのみ可能です。

システムは指定したディレクトリのコアディレクトリにコアファイルを保存します。コアディレクトリが存在しない場合、保存する前にコアディレクトリを作成します。

ディレクトリが指定されていない、あるいは指定されたディレクトリがアクセス不能である場合、プロセス例外のコアファイルを記録することができません。

例

コアファイルを保存するディレクトリを flash:/に指定します。

<Switch> exception filepath flash:/

関連コマンド

- **display exception filepath**
- **process core**

8.1.7 process core

Syntax

process core { **maxcore** *value* | **off** } { **job** *job-id* | **name** *process-name* } [**slot** *slot-number*]

View

User view

デフォルト

プロセスは最初の例外のコアファイルを作成し、続く例外のコアファイルを作成しません。

定義済みユーザロール

network-admin

パラメータ

off: コアファイルの作成を無効にします。

maxcore *value*: コアファイルの作成を有効にし、コアファイルの最大数を設定します。設定範囲は 1～10 です。

name *process-name*: プロセス名を指定します。設定範囲は 1～15 文字です。大文字、小文字を区別しません。

job *job-id*: job ID でプロセスを指定します。設定範囲は 1～2147483647 です。プロセスを再起動しても、job ID は変わりません。

slot *slot-number*: IRF スタックメンバ装置のメンバ ID を指定します。指定しない場合、IRF スタックのマスタ装置が指定されます。

説明

process core コマンドは例外のコアファイルを作成するプロセスを有効あるいは無効にし、コアファイルの最大数を設定します。

process core コマンドはプロセスのすべてのインスタンスに適用します。

コマンドは、コアファイルが最大数になるまで、指定されたプロセスがクラッシュするたびに、コアファイルを作成することを有効にします。コアファイルは例外情報を記録します。

コアファイルがシステム記憶リソースを消費するため、例外情報のレビューする必要がないプロセスはコアファイルの生成を無効にすることができます。

例

プロセス **routed** のコアファイルの作成を無効にします。

<Switch> process core off name routed

プロセス **routed** のコアファイルの作成を有効にし、コアファイルの最大数を 5 に設定します。

<Switch> process core maxcore 5 name routed

関連コマンド

- **display exception context**
- **exception filepath**

8.1.8 reset exception context

Syntax

reset exception context [**slot** *slot-number*]

View

User view

定義済みユーザロール

network-admin

パラメータ

slot *slot-number*: IRF スタックメンバ装置のメンバ ID を指定します。指定しない場合、IRF スタックのマスタ装置が指定されます。

説明

reset exception context コマンドはプロセス例外のコンテキスト情報を削除します。

例

プロセス例外のコンテキスト情報を削除します。

<Switch> reset exception context

関連コマンド

display exception context

8.1.9 reset kernel deadloop

Syntax

reset kernel deadloop [**slot** *slot-number* [**cpu** *cpu-number*]]

View

User view

定義済みユーザロール

network-admin

パラメータ

slot *slot-number*: IRF スタックメンバ装置のメンバ ID を指定します。指定しない場合、IRF スタックのマスタ装置のカーネルスレッドデッドループ情報を削除します。

cpu *cpu-number*: CPU を番号で指定します。

説明

reset kernel deadloop コマンドはカーネルスレッドのデッドループ情報を削除します。

例

カーネルスレッドのデッドループ情報を削除します。

<Switch> reset kernel deadloop

関連コマンド

display kernel deadloop

8.1.10 reset kernel exception

Syntax

reset kernel exception [**slot** *slot-number* [**cpu** *cpu-number*]]

View

User view

定義済みユーザロール

network-admin

パラメータ

slot *slot-number*: IRF スタックメンバ装置のメンバ ID を指定します。指定しない場合、IRF スタックのマスタ装置のカーネルスレッドの例外情報を削除します。

cpu *cpu-number*: CPU を番号で指定します。

説明

reset kernel exception コマンドはカーネルスレッドの例外情報を削除します。

例

カーネルスレッドの例外情報を削除します。

<Switch> reset kernel exception

関連コマンド

display kernel exception

8.1.11 reset kernel reboot

Syntax

reset kernel reboot [**slot** *slot-number* [**cpu** *cpu-number*]]

View

User view

定義済みユーザロール

network-admin

パラメータ

slot *slot-number*: IRF スタックメンバ装置のメンバ ID を指定します。指定しない場合、IRF スタックのマスタ装置のカーネルスレッドの再起動情報を削除します。

cpu *cpu-number*: CPU を番号で指定します。

説明

reset kernel reboot コマンドはカーネルスレッドの再起動情報を削除します。

例

カーネルスレッドの再起動情報を削除します。

<Switch> reset kernel reboot

関連コマンド

display kernel reboot

目次

このセクションのページは **11-x-x** です。

9 章 ポートミラーリング 9-1
9.1 ポートミラーリング設定コマンド 9-1
9.1.1 display mirroring-group 9-1
9.1.2 mirroring-group 9-2
9.1.3 mirroring-group mirroring-port (interface view) 9-3
9.1.4 mirroring-group mirroring-port (system view) 9-4
9.1.5 mirroring-group monitor-egress 9-6
9.1.6 mirroring-group monitor-port (interface view) 9-8
9.1.7 mirroring-group monitor-port (system view) 9-9
9.1.8 mirroring-group reflector-port 9-10
9.1.9 mirroring-group remote-probe vlan 9-12

9章 ポートミラーリング

9.1 ポートミラーリング設定コマンド

9.1.1 display mirroring-group

Syntax

display mirroring-group { *group-id* | **all** | **local** | **remote-destination** | **remote-source** }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

group-id: ミラーリンググループの番号を指定します。設定範囲は 1～4 です。

all: すべてのミラーリンググループの情報を表示します。

local: ローカルミラーリンググループの情報を表示します。

remote-destination: リモート宛先グループの情報を表示します。

remote-source: リモート送信元グループの情報を表示します。

説明

display mirroring-group コマンドはミラーリンググループの情報を表示します。

ミラーリンググループの情報は、ミラーリンググループのタイプ、状態、内容が含まれます。ミラーリンググループの番号の順番で表示されます。

例

すべてのミラーリンググループの情報を表示します。

<Switch> display mirroring-group all

```
Mirroring group 1:
    Type: Local
    Status: Active
    Mirroring port:
        GigabitEthernet1/0/1  Inbound
    Monitor port: GigabitEthernet1/0/2
```

表 9-1 コマンド出力

フィールド	説明
Mirroring group	ミラーリンググループの番号です。
Type	ミラーリンググループのタイプです。 ● **Local**－ローカルです。 ● **Remote source**－リモート送信元です。 ● **Remote destination**－リモート宛先です。
Status	ミラーリンググループの状態です。 ● **Active**—アクティブです。 ● **Incomplete**—ミラーリンググループが完全に設定されておらず、適用されません。
Mirroring port	送信元ポートです。
Monitor port	宛先ポートです。

9.1.2 mirroring-group

Syntax

mirroring-group *group-id* { **local** | **remote-destination** | **remote-source** }

undo mirroring-group { *group-id* | **all** | **local** | **remote-destination** | **remote-source** }

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

group-id: ミラーリンググループの番号を指定します。設定範囲は 1～4 です。

local: ローカルミラーリンググループを指定します。

remote-destination: リモート宛先グループを指定します。

remote-source: リモート送信元グループを指定します。

all: すべてのミラーリンググループを指定します。

説明

mirroring-group コマンドはミラーリンググループを作成します。

undo mirroring-group コマンドはミラーリンググループを削除します。

例

ローカルミラーリンググループ 1 を作成します。

<Switch> system-view

[Switch] mirroring-group 1 local

9.1.3 mirroring-group mirroring-port (interface view)

Syntax

mirroring-group *group-id* **mirroring-port** { **both** | **inbound** | **outbound** }

undo mirroring-group *group-id* **mirroring-port**

デフォルト

設定なし

View

Interface view

定義済みユーザロール

network-admin

パラメータ

group-id: ミラーリンググループの番号を指定します。設定範囲は 1～4 です。ミラーリンググループは作成されている必要があります。

both: 指定されたポートで受信パケットと送信パケットの両方をミラーします。

inbound: 指定されたポートで受信パケットをミラーします。

outbound: 指定されたポートで送信パケットをミラーします。

説明

mirroring-group mirroring-port コマンドはミラーリンググループの送信元ポートを設定します。

undo mirroring-group mirroring-port コマンドはミラーリンググループから送信元ポートを削除します。

送信元ポートはローカルミラーリンググループあるいはリモート送信元グループの送信元ポートのみを設定することができます。

アグリゲートインタフェースはモニタポートとして設定することができません。

ミラーリンググループの送信元ポートをミラーリンググループのリモートプローブ VLAN に割り当てないでください。

ポートは以下のミラーリンググループのため、片方向の送信元ポートとして設定することができます。

- inbound トラフィックミラーリング
- outbound トラフィックミラーリング

双方向の送信元ポートは 1 つのミラーリンググループのみ割り当てることができます。

装置は 1 つの outbound トラフィックミラーリングあるいは双方向ミラーリングのみをサポートします。

送信元ポートとしてポートが設定されている場合、ポートはリフレクタポート、出力ポート、モニタポートとして使用することができません。

例

GigabitEthernet 1/0/1 の双方向のトラフィックをモニタするため、ローカルミラーリンググループ 1 を作成します。

<Switch> system-view

[Switch] mirroring-group 1 local

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] mirroring-group 1 mirroring-port both

GigabitEthernet 1/0/2 の双方向のトラフィックをモニタするため、リモート送信元グループ 2 を作成します。

<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

関連コマンド

mirroring-group

9.1.4 mirroring-group mirroring-port (system view)

Syntax

mirroring-group *group-id* **mirroring-port** *interface-list* { **both** | **inbound** | **outbound** }

undo mirroring-group *group-id* **mirroring-port** *interface-list*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

group-id: ミラーリンググループの番号を指定します。設定範囲は 1～4 です。ミラーリンググループは作成されている必要があります。

interface-list: 送信元インタフェースを指定します。半角スペースで区切り、8 までインタフェースを指定するか、インタフェースの範囲を指定します。インタフェースを指定する形式は *interface-type interface-number1* **to** *interface-type interface-number2* です。インタフェースのタイプは同一にする必要があります。*interface-number2* は *interface-number1* 以上の値にしてください。

both: 指定されたポートで受信されたパケットと送信されたポートの両方をミラーします。

inbound: 指定されたポートで受信されたパケットのみをミラーします。

outbound: 指定されたポートで送信されたポートのみをミラーします。

説明

mirroring-group mirroring-port コマンドはミラーリンググループの送信元ポートを設定します。

undo mirroring-group mirroring-port コマンドはミラーリンググループから送信元ポートを削除します。

送信元ポートはローカルミラーリンググループあるいはリモート送信元グループの送信元ポートのみを設定することができます。

アグリゲートインタフェースはモニタポートとして設定することができません。

ミラーリンググループの送信元ポートをミラーリンググループのリモートプローブ VLAN に割り当てないでください。

ポートは以下のミラーリンググループのため、片方向の送信元ポートとして設定することができます。

- inbound トラフィックミラーリング
- outbound トラフィックミラーリング

双方向の送信元ポートは 1 つのミラーリンググループのみ割り当てることができます。

装置は 1 つの outbound トラフィックミラーリングあるいは双方向ミラーリングのみをサポートします。

送信元ポートとしてポートが設定されている場合、ポートはリフレクタポート、出力ポート、モニタポートとして使用することができません。

例

GigabitEthernet 1/0/1 の双方向のトラフィックをモニタするため、ローカルミラーリンググループ 1 を作成します。

<Switch> system-view

[Switch] mirroring-group 1 local

[Switch] mirroring-group 1 mirroring-port gigabitethernet 1/0/1 both

GigabitEthernet 1/0/2 の双方向のトラフィックをモニタするため、リモート送信元グループ 2 を作成します。

<Switch> system-view

[Switch] mirroring-group 2 remote-source

[Switch] mirroring-group 2 mirroring-port gigabitethernet 1/0/2 both

関連コマンド

mirroring-group

9.1.5 mirroring-group monitor-egress

Syntax

system view :

mirroring-group *group-id* **monitor-egress** *interface-type interface-number*

undo mirroring-group *group-id* **monitor-egress** *interface-type interface-number*

interface view :

mirroring-group *group-id* **monitor-egress**

undo mirroring-group *group-id* **monitor-egress**

デフォルト

設定なし

View

System view

Interface view

定義済みユーザロール

network-admin

パラメータ

group-id: ミラーリンググループの番号を指定します。設定範囲は 1～4 です。ミラーリンググループは作成されている必要があります。

interface-type interface-number: 送信ポートとして設定されたポートのタイプと番号を指定します。

説明

mirroring-group monitor-egressコマンドはリモート送信元グループの送信ポートを設定します。

undo mirroring-group monitor-egressコマンドはリモート送信元グループから送信ポートを削除します。

リモート送信元グループの送信ポートのみ設定することができますが、ローカルミラーリンググループあるいはリモート宛先グループを設定することはできません。

ミラーリンググループの送信ポートをミラーリンググループのリモート送信元 VLAN に割り当てないでください。

ポートミラーリングを正常に動作させるため、送信ポートで以下の機能を無効にしてください。

- スパニングツリー
- 802.1X
- IGMP snooping
- スタティック ARP
- MAC アドレス学習

既存のミラーリンググループのメンバポートを送信ポートに設定しないでください。

既存のアグリゲートインタフェースのメンバポートを送信ポートに設定しないでください。

例

リモート送信元グループ 1 を作成し、system view で送信ポートとして GigabitEthernet 1/0/1 を設定します。

<Switch> system-view

[Switch] mirroring-group 1 remote-source

[Switch] mirroring-group 1 monitor-egress gigabitethernet 1/0/1

リモート送信元グループ 2 を作成し、interface view で送信ポートとして GigabitEthernet 1/0/2 を設定します。

<Switch> system-view

[Switch] mirroring-group 2 remote-source

[Switch] interface gigabitethernet 1/0/2

[Switch-GigabitEthernet1/0/2] mirroring-group 2 monitor-egress

関連コマンド

mirroring-group

9.1.6 mirroring-group monitor-port (interface view)

Syntax

mirroring-group *group-id* **monitor-port**

undo mirroring-group *group-id* **monitor-port**

デフォルト

設定なし

View

Interface view

定義済みユーザロール

network-admin

パラメータ

group-id: ミラーリンググループの番号を指定します。設定範囲は 1～4 です。ミラーリンググループは作成されている必要があります。

説明

mirroring-group monitor-port コマンドはミラーリンググループのモニタポートを設定します。

undo mirroring-group monitor-port コマンドはミラーリンググループのモニタポートを削除します。

ローカルミラーリンググループあるいはリモート宛先グループのモニタポートを設定することができますが、リモート送信元グループのモニタポートを設定することはできません。

モニタポートでスパニングツリーを有効にすることはできません。

モニタポートとして設定されたアグリゲートインタフェースでは、送信元ポートとしてメンバポートを設定しないでください。

ポートミラーリングで使用するポートはモニタポート専用ポートとして使用してください。データをモニタリングする装置は、混在したトラフィックでなく、ミラーされたトラフィックのみを受信するように、ポートミラーリングのモニタポートのみを使用してください。

既存のミラーリンググループのポートをモニタポートに設定しないでください。

例

ローカルミラーリンググループ 1 を作成し、モニタポートとして GigabitEthernet 1/0/1 を設定します。

<Switch> system-view

[Switch] mirroring-group 1 local

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] mirroring-group 1 monitor-port

リモート宛先グループ 2 を作成し、モニタポートとして GigabitEthernet 1/0/2 を設定します。

<Switch> system-view

[Switch] mirroring-group 2 remote-destination

[Switch] interface gigabitethernet 1/0/2

[Switch-GigabitEthernet1/0/2] mirroring-group 2 monitor-port

関連コマンド

mirroring-group

9.1.7 mirroring-group monitor-port (system view)

Syntax

mirroring-group *group-id* **monitor-port** *interface-type interface-number*

undo mirroring-group *group-id* **monitor-port** *interface-type interface-number*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

group-id: ミラーリンググループの番号を指定します。設定範囲は 1～4 です。ミラーリンググループは作成されている必要があります。

interface-type interface-number: モニタポートとして設定されたポートのタイプと番号を指定します。

説明

mirroring-group monitor-port コマンドはミラーリンググループのモニタポートを設定します。

undo mirroring-group monitor-port コマンドはミラーリンググループからモニタポートを削除します。

ローカルミラーリンググループあるいはリモート宛先グループのモニタポートを設定することができますが、リモート送信元グループのモニタポートを設定することはできません。

ミラーリンググループのモニタポートでスパニングツリーを有効にすることはできません。

ミラーリンググループのモニタポートとして設定されたアグリゲートインタフェースでは、送信元ポートとしてメンバポートを設定しないでください。

ポートミラーリングで使用するポートはモニタポート専用ポートとして使用してください。データをモニタリングする装置は、混在したトラフィックでなく、ミラーされたトラフィックのみを受信するように、ポートミラーリングのモニタポートのみを使用してください。

既存のミラーリンググループのポートをモニタポートに設定しないでください。

例

ローカルミラーリンググループ 1 を作成し、モニタポートとして GigabitEthernet 1/0/1 を設定します。

<Switch> system-view

[Switch] mirroring-group 1 local

[Switch] mirroring-group 1 monitor-port gigabitethernet 1/0/1

リモート宛先グループ 2 を作成し、モニタポートとして GigabitEthernet 1/0/2 を設定します。

<Switch> system-view

[Switch] mirroring-group 2 remote-destination

[Switch] mirroring-group 2 monitor-port gigabitethernet 1/0/2

関連コマンド

mirroring-group

9.1.8 mirroring-group reflector-port

Syntax

system view :

mirroring-group *group-id* **reflector-port** *interface-type interface-number*

undo mirroring-group *group-id* **reflector-port** *interface-type interface-number*

interface view :

mirroring-group *group-id* **reflector-port**

undo mirroring-group *group-id* **reflector-port**

デフォルト

設定なし

View

System view

Interface view

定義済みユーザロール

network-admin

パラメータ

group-id: ミラーリンググループの番号を指定します。設定範囲は 1～4 です。ミラーリンググループは作成されている必要があります。

interface-type interface-number: リフレクタポートとして設定されたポートのタイプと番号を指定します。

説明

mirroring-group reflector-port コマンドはリモート送信元グループのリフレクタポートを設定します。

undo mirroring-group reflector-port コマンドはリモート送信元グループのリフレクタポートを削除します。

リモート送信元グループのリフレクタポートを設定することができますが、ローカルミラーリンググループあるいはリモート宛先グループのリフレクタポートを設定することはできません。

リフレクタポートとして設定されたポートは装置で使用されていないポートを選択してください。リフレクタポートにネットワークケーブルを接続しないでください。

ポートをリフレクタポートに設定したとき、ポートの既存の設定は削除されます。リフレクタポートとして設定されると、リフレクタポートで他の機能を設定することはできません。

IRF スタックポートが 1 つの物理インタフェースのみ割り当てられている場合、リフレクタポートとして物理インタフェースを設定しないでください。そうでない場合、IRF スタックユニットが分裂する可能性があります。

リフレクタポートのデュプレックスモード、MDI、通信速度の設定を変更することはできません。

リフレクタポートとしてアグリゲートインタフェースのメンバポートを設定することはできます。

例

リモート送信元グループ 1 を作成し、system view でリフレクタポートとして GigabitEthernet 1/0/1 を設定します。

<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
```

リモート送信元グループ 2 を作成し、interface view でリフレクタポートとして GigabitEthernet 1/0/2 を設定します。

<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
```

関連コマンド

mirroring-group

9.1.9 mirroring-group remote-probe vlan

Syntax

mirroring-group *group-id* **remote-probe vlan** *vlan-id*

undo mirroring-group *group-id* **remote-probe vlan** *vlan-id*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

group-id: ミラーリンググループの番号を指定します。設定範囲は 1～4 です。ミラーリンググループは作成されている必要があります。

vlan-id: VLAN の ID を指定します。

説明

mirroring-group remote-probe vlan コマンドはミラーリンググループのリモートプローブ VLAN を設定します。

undo mirroring-group remote-probe vlan コマンドはミラーリンググループからリモートプローブ VLAN を削除します。

リモート送信元グループあるいはリモート宛先グループのリモートプローブ VLAN を設定することができますが、ローカルミラーリンググループのリモートプローブ VLAN を設定することはできません。

リモートプローブ VLAN として VLAN を設定したとき、ポートミラーリングのリモートプローブ VLAN は専用の VLAN として使用してください。

送信元装置と宛先装置のリモートミラーリンググループは同じリモートプローブ VLAN を使用してください。

既存のスタティック VLAN のみがリモートプローブ VLAN として設定することができます。リモートプローブ VLAN として設定された VLAN は 1 つのミラーリンググループでのみ使用できます。

リモートプローブ VLAN として設定された VLAN を削除する場合、最初にリモートプローブ VLAN の設定を削除してください。

例

リモート送信元グループ 1 を作成し、リモートプローブ VLAN として VLAN 10 を設定します。

<Switch> system-view

[Switch] mirroring-group 1 remote-source

[Switch] mirroring-group 1 remote-probe vlan 10

リモート宛先グループ 2 を作成し、リモートプローブ VLAN として VLAN 20 を設定します。

<Switch> system-view

[Switch] mirroring-group 2 remote-destination

[Switch] mirroring-group 2 remote-probe vlan 20

関連コマンド

mirroring-group

目次

このセクションのページは **11-x-x** です。

10 章 トラフィックミラーリング 10-1
10.1 トラフィックミラーリング設定コマンド.....10-1
10.1.1 mirror-to interface 10-1

10章 トラフィックミラーリング

10.1 トラフィックミラーリング設定コマンド

10.1.1 mirror-to interface

Syntax

mirror-to interface *interface-type interface-number*

undo mirror-to interface *interface-type interface-number*

デフォルト

設定なし

View

Traffic behavior view

定義済みユーザロール

network-admin

パラメータ

interface-type interface-number: インタフェースのタイプと番号を指定します。

説明

mirror-to interface コマンドはインタフェースでトラフィック動作のミラーリング宛先を指定します。

undo mirror-to interface コマンドは設定を削除します。

トラフィック動作で複数のインタフェースにトラフィックミラーリングのアクションを設定することができます。

ミラーリングアクションを含むトラフィック動作に最大 4 つの設定を行うことができます。5 つ以上のトラフィック動作を設定した場合、最初の 4 つのトラフィック動作が適用されます。

トラフィック動作において、1 つのインタフェースのみトラフィックを監視することができます。複数回コマンドを実行した場合、最後に行った設定が適用されます。

例

トラフィック動作 1 を作成し、トラフィック動作の GigabitEthernet 1/0/1 にトラフィックミラーリングのアクションを設定します。

<Switch> system-view

[Switch] traffic behavior 1

[Switch-behavior-1] mirror-to interface gigabitethernet 1/0/1

目次

このセクションのページは **11-x-x** です。

11 章 sFlow 11-1
11.1 sFlow 設定コマンド 11-1
11.1.1 display sflow 11-1
11.1.2 sflow agent 11-3
11.1.3 sflow collector 11-4
11.1.4 sflow counter collector 11-5
11.1.5 sflow counter interval 11-6
11.1.6 sflow flow collector 11-7
11.1.7 sflow flow max-header 11-7
11.1.8 sflow sampling-mode 11-8
11.1.9 sflow sampling-rate 11-9
11.1.10 sflow source 11-10

11章 sFlow

11.1 sFlow設定コマンド

11.1.1 display sflow

Syntax

display sflow

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display sflow コマンドは sFlow の設定と動作の情報を表示します。

例

sFlow の設定と動作の情報を表示します。

<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
```

表 11-1 コマンド出力

フィールド	説明
sFlow datagram version	sFlowバージョンです。装置はバージョン5のsFlowパケットのみ送信することができます。

フィールド	説明
Global information	グローバルのsFlowの情報です。
Agent IP	sFlowエージェントのIPアドレスです。 ● **CLI**—手動で設定されたIPアドレスです。 ● **Auto**—自動で設定されたIPアドレスです。
Source address	sFlowパケットの送信元IPアドレスです。
Collector information	sFlowコレクタの情報です。
ID	sFlowコレクタのIDです。
IP	sFlowコレクタのIPアドレスです。
Port	sFlowコレクタのポートです。
Aging	sFlowコレクタの残りのライフタイムです。**N/A**と表示されている場合、sFlowコレクタはエージアウトしません。
Size	sFlowパケットのsFlowデータ部の最大長です。
VPN-instance	sFlowコレクタが所属しているVPNインスタンス名です。 このフィールドは現在のソフトウェアバージョンでサポートしていません。
Description	sFlowコレクタの説明です。
Port information	sFlowが設定されたインタフェースの情報です。
Interface	sFlowが設定されたインタフェースです。
CID	カウンタサンプリングのパケットを受信するsFlowコレクタのIDです。sFlowコレクタのIDが指定されていない場合、**0**と表示されます。
Interval(s)	カウンタサンプリングの間隔です。単位は秒です。
FID	フローサンプリングのパケットを受信するsFlowコレクタのIDです。sFlowコレクタのIDが指定されていない場合、**0**と表示されます。
MaxHLen	サンプリングパケットでコピーされるバイトの最大数です。（パケットヘッダから開始します）
Rate	フローサンプリングを使用してインタフェースがパケットをサンプリングするパケット数です。
Mode	フローサンプリングモードです。

フィールド	説明
Status	ポートのsFlowの状態です。 ● **Suspended**—ポートがダウンしているため、sFlow機能が中断しています。 ● **Active**—ポートがアップしているため、sFlow機能がアクティブです。

11.1.2 sflow agent

Syntax

sflow agent { **ip** *ipv4-address* | **ipv6** *ipv6-address* }

undo sflow agent { **ip** | **ipv6** }

デフォルト

sFlow エージェントの IP アドレスは設定されていません。装置は定期的に sFlow エージェントの IP アドレスがあるかどうかを確認します。ない場合、装置は自動で sFlow エージェントの IPv4 アドレスを選択します。選択された IPv4 アドレスは設定ファイルに保存されません。

View

System view

定義済みユーザロール

network-admin

パラメータ

ip *ipv4-address*: sFlow エージェントの IPv4 アドレスを設定します。

ipv6 *ipv6-address*: sFlow エージェントの IPv6 アドレスを設定します。

説明

sflow agent コマンドは sFlow エージェントの IP アドレスを設定します。

undo sflow agent コマンドはデフォルトに戻します。

sFlow エージェントの IP アドレスを手動で設定することを推奨します。

sflow agent コマンドを複数回行った場合、最後に行った設定が適用されます。

例

sFlow エージェントの IP アドレスを 10.10.10.1 に設定します。

<Switch> system-view

[Switch] sflow agent ip 10.10.10.1

11.1.3 sflow collector

Syntax

sflow collector *collector-id* { **ip** *ipv4-address* | **ipv6** *ipv6-address* } [**port** *port-number*] [**datagram-size** *size*] [**time-out** *seconds*] [**description** *string*]

undo sflow collector *collector-id*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

collector-id: sFlow コレクタの ID を指定します。設定範囲は 1～10 です。

ip *ipv4-address*: sFlow コレクタの IPv4 アドレスを指定します。

ipv6 *ipv6-address*: sFlow コレクタの IPv6 アドレスを指定します。

port *port-number*: sFlow コレクタの UDP ポート番号を指定します。設定範囲は 1～65535 です。デフォルトは 6343 です。

datagram-size *size*: sFlow パケットの sFlow データ部の最大長を指定します。設定範囲は 200～3000 バイトです。デフォルトは 1400 バイトです。

time-out *seconds*: sFlow コレクタのエージングタイマを指定します。設定範囲は 1～2147483647 秒です。エージングタイマが終了したとき、sFlow コレクタは削除されます。デフォルトで sFlow コレクタはエージアウトしません。

description *string*: sFlow コレクタの説明を指定します。設定範囲は 1～127 文字です。大文字、小文字を区別します。デフォルトは CLI Collector.です。

説明

sflow collector コマンドは sFlow コレクタのパラメータを設定します。

undo sflow collector コマンドは sFlow コレクタを削除します。

例

sFlow コレクタ 2 のパラメータを以下のように設定します。

- IP アドレス—3.3.3.1
- ポート番号—デフォルト
- 説明—netserver

- エージングタイマ—1200 秒
- sFlow パケットの sFlow データ部の最大長—1000 バイト

<Switch> system-view

[Switch] sflow collector 2 ip 3.3.3.1 description netserver time-out 1200 datagram-size 1000

11.1.4 sflow counter collector

Syntax

sflow counter collector *collector-id*

undo sflow counter collector

デフォルト

設定なし

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

collector-id: sFlow コレクタの ID を指定します。設定範囲は 1～10 です。

説明

sflow counter collector コマンドはカウンタサンプリングの sFlow コレクタを指定します。

undo sflow counter collector コマンドはデフォルトに戻します。

例

GigabitEthernet 1/0/1 でカウンタサンプリングの sFlow コレクタ 2 を指定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] sflow counter collector 2

11.1.5 sflow counter interval

注意:

sflow counter interval が 120 秒より短い場合、設定通りに動作しません。120 秒以上を設定してください。

Syntax

sflow counter interval *interval*

undo sflow counter interval

デフォルト

無効

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

interval: カウンタサンプリングの間隔を指定します。設定範囲は 2～86400 秒です。

説明

sflow counter interval コマンドはカウンタサンプリングを有効にし、カウンタサンプリングの間隔を設定します。

undo sflow counter interval コマンドはデフォルトに戻します。

例

GigabitEthernet 1/0/1 でカウンタサンプリングを有効にし、カウンタサンプリングの間隔を 120 秒に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] sflow counter interval 120

11.1.6 sflow flow collector

Syntax

sflow flow collector *collector-id*

undo sflow flow collector

デフォルト

設定なし

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

collector-id: sFlow コレクタの ID を指定します。設定範囲は 1～10 です。

説明

sflow counter collector コマンドはカウンタサンプリングの sFlow コレクタを指定します。

undo sflow counter collector コマンドはデフォルトに戻します。

例

GigabitEthernet 1/0/1 でカウンタサンプリングの sFlow コレクタ 2 を指定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] sflow flow collector 2

11.1.7 sflow flow max-header

Syntax

sflow flow max-header *length*

undo sflow flow max-header

デフォルト

128 バイト

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

length: コピーできるパケットの最大バイト長を指定します。設定範囲は 18～512 バイトです。デフォルトで使用することを推奨します。

説明

sflow flow max-header コマンドはフローサンプリングでコピーできるパケットの最大バイト長を設定します。（パケットヘッダから開始します。）

undo sflow flow max-header コマンドはデフォルトに戻します。

例

GigabitEthernet 1/0/1 でコピーできるパケットの最大バイト長を 60 バイトに設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] sflow flow max-header 60

11.1.8 sflow sampling-mode

Syntax

sflow sampling-mode random

undo sflow sampling-mode

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

random: ランダムサンプリングモードを指定します。たとえば、**sflow sampling-rate** コマンドでパケットサンプリング間隔が 4000 に設定されている場合、装置は以下のようにランダムにパケットをサンプリングします。

- 装置は、最初の 4000 から 1 個のパケットをサンプリングします。
- 装置は、次の 4000 パケットから複数のパケットをサンプリングします。
- 装置は、3 番目の 4000 パケットからサンプリングしません。

装置は平均で 4000 パケット毎に 1 個のパケットをサンプリングします。

説明

sflow sampling-mode コマンドはサンプリングモードを指定します。

undo sflow sampling-mode コマンドはデフォルトに戻します。

例

GigabitEthernet 1/0/1 でサンプリングモードを random に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] sflow sampling-mode random

関連コマンド

sflow sampling-rate

11.1.9 sflow sampling-rate

Syntax

sflow sampling-rate *rate*

undo sflow sampling-rate

デフォルト

無効

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

rate: インタフェースでパケットをサンプリングするパケットの数を指定します。設定範囲は 1000～500000 です。サンプリングするパケット数は 8192 以上の 2^n に設定することを推奨します。たとえば 32768 です。

説明

sflow sampling-rate コマンドはフローサンプリングを有効にし、インタフェースでパケットをサンプリングするパケットの数を指定します。

undo sflow sampling-rate コマンドはデフォルトに戻します。

例

フローサンプリングを有効にし、GigabitEthernet 1/0/1 でパケットをサンプリングするパケットの数を 32768 に設定します。(32768 パケットごとに 1 パケットをサンプリングします。)

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] sflow sampling-rate 32768

関連コマンド

sflow sampling-mode

11.1.10 sflow source

Syntax

sflow source { **ip** *ipv4-address* | **ipv6** *ipv6-address* } *

undo sflow source { **ip** | **ipv6** } *

デフォルト

sFlow パケットの送信元 IP アドレスはルーティングによって決定します。

View

System view

定義済みユーザロール

network-admin

パラメータ

ip *ipv4-address*: sFlow パケットの送信元 IPv4 アドレスを指定します。

ipv6 *ipv6-address*: sFlow パケットの送信元 IPv6 アドレスを指定します。

説明

sflow source コマンドは sFlow パケットの送信元 IP アドレスを指定します。

undo sflow source コマンドはデフォルトに戻します。

例

sFlow パケットの送信元 IPv4 アドレスを 10.0.0.1 に設定します。

<Switch> system-view

[Switch] sflow source ip 10.0.0.1

目次

このセクションのページは **11-x-x** です。

12 章 Information Center 12-1
12.1 Information Center 設定コマンド 12-1
12.1.1 diagnostic-logfile save 12-1
12.1.2 display diagnostic-logfile summary 12-2
12.1.3 display info-center 12-2
12.1.4 display logbuffer 12-3
12.1.5 display logbuffer summary 12-5
12.1.6 display logfile summary 12-6
12.1.7 enable log updown 12-7
12.1.8 info-center diagnostic-logfile directory 12-8
12.1.9 info-center diagnostic-logfile enable 12-9
12.1.10 info-center diagnostic-logfile frequency 12-9
12.1.11 info-center diagnostic-logfile quota 12-10
12.1.12 info-center enable 12-11
12.1.13 info-center logbuffer 12-12
12.1.14 info-center logbuffer size 12-12
12.1.15 info-center logfile directory 12-13
12.1.16 info-center logfile enable 12-14
12.1.17 info-center logfile frequency 12-15
12.1.18 info-center logfile size-quota 12-16
12.1.19 info-center logging suppress module 12-17
12.1.20 info-center loghost 12-18
12.1.21 info-center loghost source 12-19
12.1.22 info-center source 12-20
12.1.23 info-center synchronous 12-22
12.1.24 info-center syslog min-age 12-23
12.1.25 info-center timestamp 12-24
12.1.26 info-center timestamp loghost 12-25
12.1.27 logfile save 12-26
12.1.28 reset logbuffer 12-27
12.1.29 snmp-agent trap enable syslog 12-27
12.1.30 terminal debugging 12-28
12.1.31 terminal logging level 12-29
12.1.32 terminal monitor 12-30

12章 Information Center

12.1 Information Center設定コマンド

12.1.1 diagnostic-logfile save

Syntax

diagnostic-logfile save

View

すべての view

定義済みユーザロール

network-admin

説明

diagnostic-logfile save コマンドは診断ログファイルバッファから診断ログファイルに診断ログを手動で保存します

info-center diagnostic-logfile directory コマンドを使用して、診断ログファイルを保存するディレクトリを指定できます。

バッファされた診断ログを診断ログファイルに保存した後、診断ログファイルのバッファが削除されます。

診断ログファイルバッファが空の場合、このコマンドは、診断ログファイルにログが保存されていないにもかかわらず、成功メッセージイベントを表示します。

例

診断ログファイルバッファから診断ログファイルに診断ログを手動で保存します。

<Switch> diagnostic-logfile save

```
The contents in the diagnostic log file buffer have been saved to the file
flash:/diagfile/diagfile.log.
```

関連コマンド

- **info-center diagnostic-logfile enable**
- **info-center diagnostic-logfile directory**

12.1.2 display diagnostic-logfile summary

Syntax

display diagnostic-logfile summary

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display diagnostic-logfile summary コマンドは診断ログファイルの設定を表示します。

例

診断ログファイル設定を表示します。

<Switch> display diagnostic-logfile summary

```
Diagnostic log file: Enabled.
Diagnostic log file size quota: 10 MB
Diagnostic log file directory: flash:/diagfile
Writing frequency: 24 hour 0 min 0 sec
```

表 12-1 コマンド出力

フィールド	説明
Diagnostic log file	診断ログファイルの状態です。 • **Enabled**—診断ログを診断ログファイルに出力できます。 • **Disabled**—診断ログを診断ログファイルに出力できません。
Diagnostic log file size quota	診断ログファイルの最大サイズです。単位はMBです。
Log file directory	診断ログファイルが保存されるディレクトリです。
Writing frequency	診断ログをバッファから診断ログファイルに保存する間隔です。

12.1.3 display info-center

Syntax

display info-center

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display info-center コマンドは Information Center の情報を表示します。

例

Information Center の情報を表示します。

<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
```

12.1.4 display logbuffer

Syntax

display logbuffer [**reverse**] [**level** *severity* | **size** *buffersize* | **slot** *slot-number*] *

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

reverse: 最新のログエントリを年代順で上から表示します。指定しない場合、もっとも古いログエントリを上から表示します。

level *severity*: severity レベルを指定します。設定範囲は 0～7 です。指定しない場合、すべてのレベルのログ情報を表示します。

表 12-2 ログレベル

Severity	レベル	説明	コマンドに対応するキーワード
0	Emergency	システムが使用できません。たとえば、システムの許可が終了しました。	emergency
1	Alert	即急に対応が必要です。たとえば、インタフェースのトラフィックが上限を超えました。	alert
2	Critical	深刻な状態です。たとえば、装置の温度が上限を超えました、電源モジュールが故障しました、FAN トレイが故障しました。	critical
3	Error	エラー状態です。たとえば、リンク状態が変更しました。	error
4	Warning	警告状態です。たとえば、インタフェースが切断されました、あるいはメモリリソースが上限まで使われました。	warning
5	Notification	通常通りですが、注意状態です。たとえば、装置にログインしました、あるいは装置が再起動しました。	notification
6	Informational	情報メッセージです。たとえば、コマンドあるいは**ping**コマンドが実行されました。	informational
7	Debugging	デバッグメッセージです。	debugging

size *buffersize*: 表示される最新のログメッセージの数を指定します。設定範囲は 1～1024 です。指定しない場合、すべてのログ情報を表示します。

slot *slot-number*: IRF スタックメンバの ID を指定します。

説明

display logbuffer コマンドはログバッファの状態とログバッファのログ情報を表示します。

例

ログバッファの状態とログ情報を表示します。

<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 --
...
```

表 12-3 コマンド出力

フィールド	説明
Log buffer	● **Enabled**—ログバッファにログを出力できます。 ● **Disabled**—ログバッファにログを出力できません。
Max buffer size	装置でサポートしている最大バッファサイズです。
Actual buffer size	**info-center logbuffer size**コマンドで設定された最大バッファサイズです。
Dropped messages	廃棄されたメッセージ数です。
Overwritten messages	上書きされたメッセージ数です。
Current messages	現在のメッセージ数です。

関連コマンド

- **info-center logbuffer**
- **reset logbuffer**

12.1.5 display logbuffer summary

Syntax

display logbuffer summary [**level** *severity* | **slot** *slot-number*] *

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

level *severity*: severity レベルを指定します。設定範囲は 0～7 です。指定しない場合、すべてのレベルのログ情報を表示します。ログレベルの詳細は表 12-2 を参照してください。

slot *slot-number*: IRF スタックメンバの ID を指定します。指定しない場合、すべてのメンバ装置の情報を表示します。

説明

display logbuffer summary コマンドはログバッファの概要を表示します。

例

ログバッファの概要を表示します。

<Switch> display logbuffer summary

```
Slot EMERG ALERT  CRIT ERROR  WARN NOTIF  INFO DEBUG
   1     0     0     0     7     0    34    38     0
```

表 12-4 コマンド出力

フィールド	説明
EMERG	emergency を示します。詳細は表 12-2を参照してください。
ALERT	alertを示します。詳細は表 12-2を参照してください。
CRIT	criticalを示します。詳細は表 12-2を参照してください。
ERROR	errorを示します。詳細は表 12-2を参照してください。
WARN	warningを示します。詳細は表 12-2を参照してください。
NOTIF	notificationを示します。詳細は表 12-2を参照してください。
INFO	informationalを示します。詳細は表 12-2を参照してください。
DEBUG	debugを示します。詳細は表 12-2を参照してください。

12.1.6 display logfile summary

Syntax

display logfile summary

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display logfile summary コマンドはログファイルの設定を表示します。

例

ログファイルの設定を表示します。

<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
```

表 12-5 コマンド出力

フィールド	説明
Log file	• **Enabled**—ログをファイルに出力できます。 • **Disabled**—ログをファイルに出力できません。
Log file size quota	ログファイルで予約された最大記憶容量です。単位はMBです。
Log file directory	ログファイルのディレクトリです。
Writing frequency	ログファイルを書き込む間隔です。

12.1.7 enable log updown

Syntax

enable log updown

undo enable log updown

デフォルト

有効

View

Interface view

定義済みユーザロール

network-admin

説明

enable log updown コマンドはインタフェースの状態が変化したとき、インタフェースでリンクアップあるいはリンクダウンのログを作成することを有効にします。

undo enable log updown コマンドはインタフェースの状態が変化したとき、インタフェースでリンクアップあるいはリンクダウンのログを作成することを無効にします。

例

GigabitEthernet1/0/1 でリンクアップあるいはリンクダウンのログを作成することを無効にします。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] undo enable log updown

12.1.8 info-center diagnostic-logfile directory

Syntax

info-center diagnostic-logfile directory *dir-name*

デフォルト

診断ログファイルのディレクトリは **flash:/diagfile** です。

View

System view

定義済みユーザロール

network-admin

パラメータ

dir-name: ディレクトリを指定します。設定範囲は 1～64 文字です。

説明

info-center diagnostic-logfile directory コマンドは診断ログファイルを保存するディレクトリを設定します。

指定したディレクトリが作成されている必要があります。

このコマンドは、IRF の再起動またはマスタ/下位スイッチオーバーには耐えられません。

例

診断ログファイルディレクトリを **flash:/test** に設定します。

<Switch> mkdir test

```
Creating directory flash:/test... Done.
```

<Switch> system-view

[Switch] info-center diagnostic-logfile directory flash:/test

12.1.9 info-center diagnostic-logfile enable

Syntax

info-center diagnostic-logfile enable

undo info-center diagnostic-logfile enable

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

info-center diagnostic-logfile enable コマンドは診断ログファイルへの診断ログの保存を有効にします。

undo info-center diagnostic-logfile enable コマンドは診断ログファイルへの診断ログの保存を無効にします。

このコマンドを使用すると、一元管理のために診断ログを診断ログファイルに保存できます。診断ログを表示して、装置の動作を監視し、問題のトラブルシューティングを行うことができます。

例

診断ログファイルへの診断ログの保存を有効にします。

<Switch> system-view

[Switch] info-center diagnostic-logfile enable

12.1.10 info-center diagnostic-logfile frequency

Syntax

info-center diagnostic-logfile frequency *freq-sec*

undo info-center diagnostic-logfile frequency

デフォルト

診断ログファイルの保存間隔は 86400 秒です。

View

System view

定義済みユーザロール

network-admin

パラメータ

freq-sec: 診断ログファイルの保存間隔を秒単位で指定します。設定範囲は 10～86400 です。

説明

info-center diagnostic-logfile frequency コマンドは診断ログファイルバッファから診断ログファイルに診断ログを保存する間隔を設定します。

undo info-center diagnostic-logfile frequency コマンドはデフォルトに戻します。

診断ログファイルバッファに診断ログが出力され、指定した間隔でバッファされたログが診断ログファイルに保存されます。

例

診断ログファイルの保存間隔を 600 秒に設定します。

<Switch> system-view

[Switch] info-center diagnostic-logfile frequency 600

関連コマンド

info-center diagnostic-logfile enable

12.1.11 info-center diagnostic-logfile quota

Syntax

info-center diagnostic-logfile quota *size*

undo info-center diagnostic-logfile quota

デフォルト

診断ログファイルの最大サイズは 10MB です。

View

System view

定義済みユーザロール

network-admin

パラメータ

size: 診断ログファイルの最大サイズを MB 単位で指定します。設定範囲は 1～10 です。

説明

info-center diagnostic-logfile quota コマンドは診断ログファイルの最大サイズを設定します。

undo info-center diagnostic-logfile quota コマンドはデフォルトに戻します。

例

診断ログファイルの最大サイズを 6 MB に設定します。

<Switch> system-view

[Switch] info-center diagnostic-logfile quota 6

12.1.12 info-center enable

Syntax

info-center enable

undo info-center enable

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

info-center enable コマンドは Information Center を有効にします。

undo info-center enable コマンドは Information Center を無効にします。

例

Information Center を有効にします。

<Switch> system-view

[Switch] info-center enable

```
Information center is enabled.
```

12.1.13 info-center logbuffer

Syntax

info-center logbuffer

undo info-center logbuffer

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

info-center logbuffer コマンドはログバッファにログの出力を有効にします。

undo info-center logbuffer コマンドはログバッファにログの出力を無効にします。

例

ログバッファにログ情報を出力するように設定します。

<Switch> system-view

[Switch] info-center logbuffer

関連コマンド

- **display logbuffer**
- **info-center enable**

12.1.14 info-center logbuffer size

Syntax

info-center logbuffer size *buffersize*

undo info-center logbuffer size

デフォルト

512

View

System view

定義済みユーザロール

network-admin

パラメータ

buffersize: ログバッファに記憶できるログの最大数を指定します。設定範囲は 0〜1024 です。デフォルトは 512 です。

説明

info-center logbuffer size コマンドはログバッファに記憶できるログの最大数を設定します。

undo info-center logbuffer size コマンドはデフォルトに戻します。

例

ログバッファに記憶できるログの最大数を 50 に設定します。

<Switch> system-view

[Switch] info-center logbuffer size 50

ログのバッファサイズをデフォルトに戻します。

<Switch> system-view

[Switch] undo info-center logbuffer size

関連コマンド

- **display logbuffer**
- **info-center enable**

12.1.15 info-center logfile directory

Syntax

info-center logfile directory *dir-name*

デフォルト

flash:/logfile

View

System view

定義済みユーザロール

network-admin

パラメータ

dir-name: ディレクトリ名を指定します。設定範囲は 1～64 文字です。

説明

info-center logfile directory コマンドはログファイルが保存されるディレクトリを設定します。

指定されたディレクトリは作成されている必要があります。

ログファイルの拡張子は“.log”です。ファイルを記録するためにデフォルトディレクトリに十分な容量がない場合、ログファイルに新しいディレクトリを指定することができます。

このコマンドの設定は、IRF スタックの再起動あるいはマスタ/メンバの切り替えで削除されます。

例

ディレクトリ名 test をフラッシュのルートディレクトリの下に作成します。

<Switch> mkdir test

```
Creating directory flash:/test... Done.
```

<Switch> system-view

[Switch] info-center logfile directory flash:/test

関連コマンド

info-center logfile enable

12.1.16 info-center logfile enable

Syntax

info-center logfile enable

undo info-center logfile enable

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

info-center logfile enable コマンドはログファイル機能を有効にします。

undo info-center logfile enable コマンドはログファイル機能を無効にします。

例

ログファイルにログを出力することを有効にします。

<Switch> system-view

[Switch] info-center logfile enable

12.1.17 info-center logfile frequency

Syntax

info-center logfile frequency *freq-sec*

undo info-center logfile frequency

デフォルト

86400 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

freq-sec: ログファイルにシステムがログを保存する間隔を指定します。設定範囲は 1～86400 秒です。

説明

info-center logfile frequency コマンドはログバッファからログファイルにログを保存する間隔を設定します。

undo info-center logfile frequency コマンドはデフォルトに戻します。

このコマンドを実行することで、指定した間隔でログファイルに、ログファイルのバッファのログを自動で保存します。

フラッシュメモリの書き込み回数へ影響しますので、必要な場合を除き、デフォルト値のままとしてください。

例

ログファイルにログを保存する間隔を 60000 秒に設定します。

<Switch> system-view

[Switch] info-center logfile frequency 60000

関連コマンド

info-center logfile enable

12.1.18 info-center logfile size-quota

Syntax

info-center logfile size-quota *size*

undo info-center logfile size-quota

デフォルト

10 MB

View

System view

定義済みユーザロール

network-admin

パラメータ

size: ログファイルの最大サイズを指定します。設定範囲は 1～10MB です。

説明

info-center logfile size-quota コマンドはログファイルの最大サイズを設定します。

undo info-center logfile size-quota コマンドはデフォルトに戻します。

ログファイルは容量の上限があります。容量が上限に到達したとき、もっとも古いメッセージを削除し、ログファイルに新しいメッセージを書き込みます。

書き込み先の空き容量に合わせて設定してください。

例

ログファイルの最大サイズを 6MB に設定します。

<Switch> system-view

[Switch] info-center logfile size-quota 6

関連コマンド

info-center logfile enable

12.1.19 info-center logging suppress module

Syntax

info-center logging suppress module *module-name* **mnemonic** { **all** | *mnemonic-value* }

undo info-center logging suppress module *module-name* **mnemonic** { **all** | *mnemonic-value* }

デフォルト

装置は、モジュールからのログ出力を抑制しません。

View

System view

定義済みユーザロール

network-admin

パラメータ

module-name: ログソースモジュール名を指定します。設定範囲は 1～8 文字です。大文字、小文字を区別しません。使用可能なログソースモジュールのリストを表示するには、**info-center logging suppress module ?** コマンドを使用します。

mnemonic { **all** | *mnemonic-value* }: ログ抑制用の mnemonic フィルタを設定します。

- **all**: モジュールのすべてのログの出力を抑制します。
- *mnemonic-value*: 指定した mnemonic を持つログの出力を抑制します。設定範囲は 1～32 文字です。大文字小文字を区別しません。これはログメッセージの mnemonic フィールドに含まれる完全な値でなければなりません。部分的な mnemonic が指定されている場合、ログ抑制は失敗します。

説明

info-center logging suppress module コマンドはモジュールのログ抑制ルールを設定します。

undo info-center logging suppress module コマンドはログ抑制ルールを削除します。

ログ抑制ルールを構成して、関係のないログを除外できます。ログ抑制ルールは、モジュールのすべてのログまたは特定の **mnemonic** を持つログのみの出力を抑制します。

例

シェルモジュールの **shell_login** mnemonic を使用してログの出力を抑制するログ抑制ルールを設定します。

<Switch> system-view

[Switch] info-center logging suppress module shell mnemonic shell_login

関連コマンド

info-center source

12.1.20 info-center loghost

Syntax

info-center loghost { *hostname* | *ipv4-address* | **ipv6** *ipv6-address* } [**port** *port-number*] [**facility** *local-number*]

undo info-center loghost { *hostname* | *ipv4-address* | **ipv6** *ipv6-address* }

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

hostname: ログホスト名を指定します。設定範囲は 1～253 文字です。大文字、小文字を区別しません。英字、数字、ハイフン（-）、アンダーライン（_）、ドット（.）を含むことができます。

ipv4-address: ログホストの IPv4 アドレスを指定します。

ipv6 *ipv6-address*: ログホストの IPv6 アドレスを指定します。

port *port-number*: ログホストのポート番号を指定します。設定範囲は 1～65535 です。デフォルトは 514 です。設定された値はログホストで設定された値と同じにする必要があります。そうでない場合、ログホストはシステム情報を受信できません。

facility *local-number*: ログホストのロギング facility を指定します。設定範囲は local0～local7 です。デフォルトは local7 です。ロギング facility は異なるロギングの送信元、query、ログのフィルタリングを識別するために使用します。

説明

info-center loghost コマンドはログホストを指定し、出力パラメータを設定します。

undo info-center loghost コマンドはデフォルトに戻します。

info-center enable コマンドで有効にしたのち、**info-center loghost** コマンドは適用されます。

装置は最大 4 のログホストをサポートします。

例

ログホスト 1.1.1.1 にログを出力します。

<Switch> system-view

[Switch] info-center loghost 1.1.1.1

12.1.21 info-center loghost source

Syntax

info-center loghost source *interface-type interface-number*

undo info-center loghost source

デフォルト

出力ログの送信元 IP アドレスは、ルートの送信インタフェースに一致するプライマリ IP アドレスです。

View

System view

定義済みユーザロール

network-admin

パラメータ

interface-type interface-number: ログの送信インタフェースのタイプと番号を指定します。

説明

info-center loghost source コマンドは出力ログの送信元 IP アドレスを指定します。

undo info-center loghost source コマンドはデフォルトに戻します。

ログを出力するため物理インタフェースが使用されても、システムはログ情報の送信元 IP アドレスとして指定された送信インタフェースのプライマリ IP アドレスを使います。

info-center enable コマンドで有効にしたのち、**info-center loghost source** コマンドは適用されます。

例

出力ログの送信元 IP アドレスとしてループバック 0 の IP アドレスを指定します。

<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

12.1.22 info-center source

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** }

デフォルト

表 12-6 にデフォルトのログ出力ルールを示します。

表 12-6 デフォルト出力ルール

宛先	送信元モジュール	共通ログ	セキュリティログ	Diagnostic ログ	Hidden ログ
コンソール	サポートされるすべてのモジュールです。	debugging	無効	無効	無効
モニタ端末	サポートされるすべてのモジュールです。	debugging	無効	無効	無効
ログホスト	サポートされるすべてのモジュールです。	informational	無効	無効	informational
ログバッファ	サポートされるすべてのモジュールです。	informational	無効	無効	informational
ログファイル	サポートされるすべてのモジュールです。	informational	無効	無効	informational
セキュリティログファイル	サポートされるすべてのモジュール、フィルタすることはできません。	無効	debugging、フィルタすることはできません。	無効	無効
Diagnosticログファイル	サポートされるすべてのモジュール、フィルタすることはできません。	無効	無効	debugging、フィルタすることはできません。	無効

View

System view

定義済みユーザロール

network-admin

パラメータ

module-name: モジュールの名前を指定します。たとえば、FTP の情報を出力する場合、FTP を指定します。装置でサポートされているモジュールを表示する場合、使用します。

default: すべてのモジュールを指定します。

console: コンソールにログを出力します。

logbuffer: ログバッファにログを出力します。

logfile: ログファイルにログを出力します。

loghost: ログホストにログを出力します。

monitor: モニタ端末にログを出力します。

deny: ログの出力を無効にします。

level *severity*: severity レベルを指定します。詳細は表 12-2 を参照してください。出力を許可/拒否されたログのもっとも低い severity レベルを指定することができます。

説明

info-center source コマンドはモジュールのログの出力ルールを設定します。

undo info-center source コマンドはデフォルトに戻します。

モジュールの出力ルールを指定しない場合、**default** パラメータを使用して出力ルールを設定することができます。**default** パラメータを使用しない場合、モジュールはデフォルトの出力ルールを使用します。

モジュールの出力ルールを設定した後、ルールの修正あるいは削除を行う場合、*module-name* パラメータを使用する必要があります。**default** パラメータを使用して設定された新しい出力ルールはモジュールで適用されません。

複数回、モジュールのコマンドを実行した場合、最後に設定したモジュールの出力ルールが適用されます。

複数回、デフォルトモジュールのコマンドを実行した場合、最後に設定したデフォルトモジュールの出力ルールが適用されます。

例

コンソールに emergency 以上の severity の VLAN モジュールの情報を出力します。

<Switch> system-view

[Switch] info-center source default console deny

[Switch] info-center source vlan console level emergency

以前の設定をもとにして、コンソールにシステム情報を出力しないように、VLAN モジュールの情報の出力を無効にします。

<Switch> system-view

[Switch] undo info-center source vlan console

12.1.23 info-center synchronous

Syntax

info-center synchronous

undo info-center synchronous

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

info-center synchronous コマンドは情報の同期出力を有効にします。

undo info-center synchronous コマンドは情報の同期出力を無効にします。

情報の同期出力とは、システムログの出力によりユーザの入力が中断された場合、中断されたところから操作を継続できるようにするため、ログの出力後、編集モードのコマンドプロンプト、あるいは対話モードの“[Y/N]”の文字列を表示し、以前に入力されたコマンドおよび、コマンドプロンプトを表示させることができます。

例

情報の同期出力を有効にし、装置の現在の設定を表示する **display current-configuration** コマンドを行います。

<Switch> system-view

[Switch] info-center synchronous

Info-center synchronous output is on

[Switch] display current-

このとき、システムがログ情報を受信します。最初にログ情報を表示し、次に直前に入力したコマンドを表示します。この例では、display current-です。

```
%May 21 14:33:19:425 2007 Switch SHELL/4/LOGIN: VTY login from 192.168.1.44
```

[Switch] display current-

display current-configuration コマンドを完全に入力し、Enter キーを押下し、コマンドを実行します。

情報の同期出力を有効にし、現在の設定を保存します。（インタラクティブの情報を入力します）

<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]:
```

このとき、システムがログ情報を受信します。最初にログ情報を表示し、次に[Y/N]を表示します。

```
%May 21 14:33:19:425 2007 Switch SHELL/4/LOGIN: VTY login from 192.168.1.44
[Y/N]:
```

入力を完了するため、“Y”あるいは“N”を入力します。

12.1.24 info-center syslog min-age

Syntax

info-center syslog min-age *min-age*

undo info-center syslog min-age

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

min-age: ログの最小保存期間を指定します。設定範囲は 1～8760 時間です。

説明

info-center syslog min-age コマンドはログをログバッファとログホストに保存する最小保存期間を設定します。

undo info-center syslog min-age コマンドはデフォルトに戻します。

例

ログの最小保存期間を 168 時間に設定します。

<Switch> system-view

[Switch] info-center syslog min-age 168

12.1.25 info-center timestamp

Syntax

info-center timestamp { **boot** | **date** | **none** }

undo info-center timestamp

デフォルト

date

View

System view

定義済みユーザロール

network-admin

パラメータ

boot: システムが起動してからの経過時間のタイムスタンプを指定します。形式は xxx.yyy です。xxx は上位 32 ビットです。単位はミリ秒です。yyy は下位 32 ビットです。たとえば 0.21990989 は Jun 25 14:09:26:881 2007 です。

date: 現在のシステム時間のタイムスタンプを指定します。形式は MMM DD hh:mm:ss:xxx YYYY です。たとえば、Dec 8 10:12:21:708 2007 です。

- MMM: 省略した月です。Jan、Feb、Mar、Apr、May、Jun、Jul、Aug、Sep、Oct、Nov、Dec があります。
- DD: 日です。9 日までの場合はスペースで始まります。たとえば、7 です。
- hh:mm:ss:xxx: ローカル時間です。hh の設定範囲は 00～23 で、mm と ss の設定範囲は 00～59 です。xxx の設定範囲は 0～999 です。
- YYYY: 年です。

none: 時間の情報を提供しないように指定します。

説明

info-center timestamp コマンドはコンソール、モニタ、ログバッファ、ログファイルに送信するシステム情報のタイムスタンプの形式を設定します。

undo info-center timestamp コマンドはデフォルトに戻します。

例

ログ情報のタイムスタンプの形式を boot に設定します。

<Switch> system-view

[Switch] info-center timestamp boot

関連コマンド

info-center timestamp loghost

12.1.26 info-center timestamp loghost

Syntax

info-center timestamp loghost { **date** | **iso** | **no-year-date** | **none** }

undo info-center timestamp loghost

デフォルト

date

View

System view

定義済みユーザロール

network-admin

パラメータ

date: 現在のシステム時間のタイムスタンプを指定します。形式は mmm dd hh:mm:ss yyyy です。たとえば、Dec 8 10:12:21 2007 です。

iso: iso 8601 形式のタイムスタンプを指定します。たとえば、2009-09-21T15:32:55 です。

no-year-date: 年を除く現在のシステム日時のタイムスタンプを指定します。

none: 時間の情報を提供しないように指定します。

説明

info-center timestamp loghost コマンドはログホストに送信するシステム情報のタイムスタンプの形式を設定します。

undo info-center timestamp loghost コマンドはデフォルトに戻します。

例

ログホストに送信するシステム情報のタイムスタンプの形式を no-year-date に設定します。

<Switch> system-view

[Switch] info-center timestamp loghost no-year-date

関連コマンド

info-center timestamp

12.1.27 logfile save

Syntax

logfile save

View

すべての view

定義済みユーザロール

network-admin

説明

logfile save コマンドはログファイルにログファイルバッファのログを手動で保存します。

info-center logfile directory コマンドを使用して、ログファイルに保存するディレクトリを指定することができます。

自動あるいは手動でバッファからログファイルにログを保存したのち、ログファイルのバッファを削除します。

ログファイルバッファが空の場合、コマンドはログをログファイルに保存できませんでしたというメッセージを表示します。

例

ログファイルバッファからログファイルにログを手動で保存します。

<Switch> logfile save

```
The contents in the log file buffer have been saved to the file
flash:/logfile/logfile.log.
```

関連コマンド

- **info-center logfile enable**
- **info-center logfile directory**

12.1.28 reset logbuffer

Syntax

reset logbuffer

View

User view

定義済みユーザロール

network-admin

説明

reset logbuffer コマンドはログバッファを削除します。

例

ログバッファを削除します。

<Switch> reset logbuffer

関連コマンド

display logbuffer

12.1.29 snmp-agent trap enable syslog

Syntax

snmp-agent trap enable syslog

undo snmp-agent trap enable syslog

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

snmp-agent trap enable syslog コマンドはログメッセージの SNMP notification の送信を有効にします。

undo snmp-agent trap enable syslog コマンドはログメッセージの SNMP notification の送信を無効にします。

snmp-agent trap enable syslog コマンドを有効にすると、装置はシスログメッセージによる SNMP notification の送信を有効にします。

装置は SNMP notification をカプセル化し、SNMP モジュールとログバッファに送信します。

SNMP モジュールが受信した SNMP notification を正常に送信するため、装置で SNMP の設定を行ってください。SNMP の設定については、オペレーションマニュアルのセクション 11 *システム管理 “SNMP”* を参照してください。

例

ログメッセージの SNMP notification の送信を有効にします。

<Switch> system-view

[Switch] snmp-agent trap enable syslog

12.1.30 terminal debugging

Syntax

terminal debugging

undo terminal debugging

デフォルト

無効

View

User view

定義済みユーザロール

network-admin

説明

terminal debugging コマンドは現在の端末にデバッグ情報を表示することを有効にします。

undo terminal debugging コマンドは現在の端末にデバッグ情報を表示することを無効にします。

コンソールでデバッグ情報を表示する場合、以下の処理を実行します。

1) **terminal debugging** コマンドを実行します。
2) Information Center を有効にします。（デフォルトで有効です）
3) 関連するデバッグを有効にするため、**debugging** コマンドを使用します。

モニタ端末でデバッグ情報を表示する場合、以下の処理を実行します。

1) **terminal monitor** コマンド、**terminal debugging** コマンドを実行します。

2) Information Center を有効にします。（デフォルトで有効です）
3) 関連するデバッグを有効にするため、**debugging** コマンドを使用します。

このコマンドの設定は端末と装置における現在の接続のみ有効です。新しい接続が確立された場合、デフォルトに戻ります。

端末におけるデバッグ情報の表示設定はデフォルト（無効）となります。

terminal logging level 7 コマンドを実行し、現在の端末でデバッグ情報を表示することができます。**terminal debugging** コマンドとの相違を以下に示します。

- **terminal logging level 7** コマンドは現在の端末のすべてのレベル（レベル 0～レベル 7）のためにログを表示します。
- **terminal logging** コマンドは以下の severity レベルのためにログを表示します。
  - debug レベル（レベル 7）
  - **terminal logging level** のコマンドによって指定された severity 以上のレベルのために **terminal debugging** コマンドはログを表示します。

例

現在の端末でデバッグ情報を表示することを有効にします。

<Switch> terminal debugging

```
The current terminal is enabled to display debugging information.
```

関連コマンド

- **terminal logging level**
- **terminal monitor**

12.1.31 terminal logging level

Syntax

terminal logging level *severity*

undo terminal logging level

デフォルト

6

View

User view

定義済みユーザロール

network-admin

パラメータ

severity: 現在の端末に出力できるログのもっとも低いレベルを指定します。設定範囲は 0～7 です。

説明

terminal logging level コマンドは現在の端末に出力できるログのもっとも低いレベルを設定します。

undo terminal logging level コマンドはデフォルトに戻します。

現在の端末に出力できるログのもっとも低いレベルを指定した場合、装置は指定されたレベル以上の severity レベルのログを出力します。たとえば、現在の端末に出力できるログのもっとも低いレベルを 6（informational）に指定した場合、0～6 の severity レベルのログを設定します。

このコマンドの設定は端末と装置における現在の接続のみ有効です。新しい接続が確立された場合、デフォルトに戻ります。

例

現在の端末に出力できるログのもっとも低いレベルを 7（debug）に設定します。

<Switch> terminal logging level 7

12.1.32 terminal monitor

Syntax

terminal monitor

undo terminal monitor

デフォルト

ログの出力はコンソールで有効です。モニタ端末は無効です。

View

User view

定義済みユーザロール

network-admin

説明

terminal monitor コマンドは現在の端末にログを表示することを有効にします。

undo terminal monitor コマンドは現在の端末にログを表示することを無効にします。

このコマンドの設定は端末と装置における現在の接続のみ有効です。新しい接続が確立された場合、デフォルトに戻ります。

例

現在の端末にログを表示することを有効にします。

<Switch> terminal monitor

```
The current terminal is enabled to display logs.
```

目次

このセクションのページは **11-x-x** です。

13 章 NetMeister 13-1
13.1 Netmeister 設定コマンド 13-1
13.1.1 display netmeister 13-1
13.1.2 netmeister account 13-2
13.1.3 netmeister alarm enable notice 13-4
13.1.4 netmeister enable 13-5
13.1.5 netmeister management ip 13-5
13.1.6 netmeister mode 13-6
13.1.7 netmeister parent ip 13-7
13.1.8 netmeister parent-mode mqtt port 13-8
13.1.9 netmeister parent-mode sitename 13-9
13.1.10 netmeister proxy 13-10
13.1.11 netmeister update 13-11

13章 NetMeister

🕮 **メモ:**

Version 7.1.11 を含む以降のソフトウェアから親機モードでの NetMeister への接続をサポートしています。

IRF スタックでの NetMeister 利用は、Version7.1.8 を含む以降のソフトウェアからサポートしています。IRF スタックで利用する場合、MAC アドレスが Master 選定によって変化しないように **irf mac-address persistent always** コマンドを設定してください。また、IRF 分裂によって同一 MAC の装置が複数登録されないように MAD 機能を利用して下さい。

13.1 Netmeister設定コマンド

13.1.1 display netmeister

Syntax

display netmeister

View

すべての view

定義済みユーザロール

network-admin

説明

display netmeister コマンドは NetMeister 及び親機との接続情報を表示します。

例

```
# NetMeisetr 及び親機との接続情報を表示します。
<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
```

表 13-1 コマンド出力

フィールド	説明
NetMeister state	NetMeister機能の状態です。 ● **Enabled** —有効 ● **Disabled** —無効
Connection state with NetMeister	NetMeisterとの接続状況です。 ● **Connected.**—接続 ● **Disconnected.**—切断
Account name	グループIDです。
Proxy information	NetMeisterプロキシサーバとの接続に関する情報です。
IP address	親機のIPアドレスです。
Port number	親機のポート番号です。
Connection state	NetMeister機能による親機への接続状態です。 ● **Connected.**—接続 ● **Disconnected.**—切断

関連コマンド

netmeister account

netmeister enable

netmeister parent

13.1.2 netmeister account

Syntax

netmeister account *account* **password** { **cipher** *cipherPassword* | **simple** *plainPassword* }

undo netmeister account

デフォルト

設定なし

View

System-view

定義済みユーザロール

network-admin

パラメータ

account: グループ ID を 2～31 文字の文字列で設定します。文字列に使用できるのは小文字、数字、およびハイフン(-)のみで、ハイフン(-)で開始または終了することはできません。

cipher: 暗号テキストのパスワードを設定します。

cipherPassword: 暗号化形式のパスワードを 41～73 文字の文字列で設定します。

simple: プレーンテキストのパスワードを設定します。セキュリティのため、プレーンテキストで設定されたパスワードを含めたすべてのパスワードは、暗号化されて保存されます。

plainPassword: プレーンテキスト形式のパスワードを 8～31 文字の文字列で設定します。文字列には、文字、数字、および!#$%&'()*+,-。/:;<=>@[]^_`{|}~の特殊文字のみを使用できます。文字列には、少なくとも 1 つの文字と 1 桁の数字を含める必要があります。

説明

netmeister account コマンドを使用して、親機への子機認証と NetMeister への装置登録で使用するグループ ID とパスワードを設定します。

undo netmeister account コマンドは、設定したグループ ID とパスワードを削除します。

netmeister account コマンドを設定する前に、**netmeister enable** が無効になっていることを確認してください。

netmeister account コマンドを複数回実行した場合、最新の設定が有効になります。

NetMeister 上で、グループ ID とパスワードがあらかじめ設定されていることを確認して下さい。設定するグループ ID とパスワードが、親機と同じであることを確認してください。

例

親機への子機認証と NetMeister への装置登録のために、グループ ID **nec** と プレーンテキストのパスワード **nec1234** を装置に設定します。

```
<Sysname> system-view
[Sysname] netmeister account nec password simple nec1234
```

関連コマンド

netmeister enable

display netmeister

13.1.3 netmeister alarm enable notice

🕮 **メモ:**

netmeister alarm enable notice コマンドはソフトウェアバージョン 7.4.61 を含む以降のソフトウェアからサポートしています。

Syntax

netmeister alarm enable notice

undo netmeister alarm enable notice

デフォルト

無効

View

System-view

定義済みユーザロール

network-admin

説明

netmeister alarm enable notice コマンドによって NetMeister の注意レベルのアラーム生成を有効にします。

undo netmeister alarm enable notice コマンドによって NetMeister の注意レベルの NetMeister アラーム生成を無効にします。

この機能により、システムは次のイベントの注意レベルのアラームを生成できます。

- 管理者は、Telnet、ssh などを使用してログインまたはログアウトした場合
- 管理者は設定を保存した場合
- 管理者は設定を保存しないまま 10 分が経過した場合

例

NetMeister の注意レベルのアラームの生成を有効にします。

<Switch> system-view

[Switch] netmeister alarm enable notice

13.1.4 netmeister enable

Syntax

netmeister enable

undo netmeister enable

デフォルト

無効

View

System-view

定義済みユーザロール

network-admin

説明

netmeister enable コマンドによって NetMeister 機能を有効にします。

undo netmeister enable コマンドによってデフォルトに戻します。

例

NetMeister 機能を有効にします。

```
<Sysname> system-view
[Sysname] netmeister enable
```

13.1.5 netmeister management ip

Syntax

netmeister management ip *ip-address*

undo netmeister management ip

デフォルト

無効

View

System-view

定義済みユーザロール

network-admin

説明

netmeister management ip コマンドによって NetMeister 機能[閉域網でリモートログインする]で表示する管理用 IP アドレスを設定します。

undo netmeister management ip コマンドによってデフォルトに戻します。

NetMeister 機能については NetMeister が提供している操作ガイドを参照してください。

例

NetMeister 機能[閉域網でリモートログインする]で表示する管理用 IP アドレスを 10.1.1.10 に設定します。

```
<Sysname> system-view
[Sysname] netmeister management ip 10.1.1.10
```

🕮 **メモ:**

netmeister management ip コマンドは Version7.1.8 を含む以降のソフトウェアからサポートしています。

13.1.6 netmeister mode

🕮 **メモ:**

netmeister mode コマンドは Version 7.1.11 を含む以降のソフトウェアからサポートしています。

Syntax

netmeister mode parent

undo netmeister mode parent

View

System-view

デフォルト

子機モード

定義済みユーザロール

network-admin

説明

netmeister mode parent コマンドを利用して NetMeister への接続モードを親機モードにします。

親機モードは NetMeister 機能を有する親機ルータがいない環境において、NetMeisterPrime(有償サービス)を利用して NetMeister で管理する場合に利用します。NetMeister 機能を有する親機ルータがある環境では、それらの機器を親機とし、子機モードで利用して下さい。

undo netmeister mode parent コマンドを利用して NetMeister への接続モードを子機モードに戻します。

netmeister mode parent コマンドを設定する前に、**netmeister enable** や子機モード時に利用する **netmeister parent ip** コマンドが無効になっていることを確認してください。

例

NetMeister 機能を有する親機ルータがいない環境で QX を NetMeister によって管理するために、親機モードを設定します。

<Switch> system-view

[Switch] netmeister mode parent

関連コマンド

netmeister enable
display netmeister

13.1.7 netmeister parent ip

Syntax

netmeister parent ip *ip-address* [**port** *port-number*]

undo netmeister parent ip *ip-address*

View

System-view

デフォルト

設定なし

定義済みユーザロール

network-admin

パラメータ

ip *ip-address*: 親機の IP アドレスを設定します。

port *port-number*: 親機のポート番号を 1～65535 の範囲で設定します。デフォルトのポート番号は 443 です。

説明

netmeister parent ip コマンドは、子機として接続する親機の IP アドレスとポート番号を設定します。

undo netmeister parent ip を使用して、子機として接続する親機の IP アドレスとポート番号を削除します。

netmeister parent ip コマンドを設定する前に、**netmeister enable** が無効になっていることを確認してください。

netmeister parent ip コマンドと **netmeister account** コマンドを設定し、**netmeister enable** コマンドを有効にすると、子機は認証応答を受信するまで親機に子機認証の要求を送信します。**netmeister parent ip** コマンドが複数設定されている場合、装置は設定されたすべてのアドレスに要求を送信し、それぞれの親機との接続を確立します。これにより、親機の障害によるサービスの中断を防ぎ、ネットワークの可用性が向上します。最大で 2 つまで親機 IP アドレスを設定できます。

例

IP アドレス **192.168.0.254** ポート番号 443 の親機に接続する子機として設定します。

```
<Sysname> system-view
[Sysname] netmeister parent ip 192.168.0.254 port 443
```

IP アドレス **192.168.1.254** の親機に接続する子機として設定します。

```
<Sysname> system-view
[Sysname] netmeister parent ip 192.168.1.254
```

関連コマンド

netmeister enable

display netmeister

13.1.8 netmeister parent-mode mqtt port

🕮 **メモ:**

netmeister parent-mode mqtt port コマンドは Version 7.1.11 を含む以降のソフトウェアからサポートしています。

Syntax

netmeister parent-mode mqtt port [8883 | 443]

undo netmeister mode parent

View

System-view

デフォルト

8883

定義済みユーザロール

network-admin

説明

netmeister parent-mode mqtt port コマンドを利用して親機モードの QX が NetMeister に接続する際の MQTT プロトコルのポート番号を変更します。

undo netmeister mode parent コマンドを利用して NetMeister に接続する際の MQTT プロトコルのポート番号をデフォルトに戻します。

例

NetMeister に接続するためにネットワーク環境で 8883 を開放する必要がない様に、MQTT のポート番号を 443 に変更します。

<Switch> system-view

[Switch] netmeister parent-mode mqtt port 443

関連コマンド

- **netmeister enable**
- **display netmeister**

13.1.9 netmeister parent-mode sitename

🕮 **メモ:**

netmeister parent-mode sitename コマンドは Version 7.1.11 を含む以降のソフトウェアからサポートしています。

Syntax

netmeister parent-mode sitename *name*

undo netmeister parent-mode sitename

View

System-view

デフォルト

なし

定義済みユーザロール

network-admin

説明

netmeister parent-mode sitename コマンドを利用して親機モードの QX が NetMeister に接続する際の拠点名を設定します。

undo netmeister mode parent コマンドを利用して拠点名の設定を削除します。

例

親機モードで NetMeister に接続するために拠点名 test を設定します。

<Switch> system-view

[Switch] netmeister parent-mode sitename test

関連コマンド

- **netmeister enable**
- **display netmeister**

13.1.10 netmeister proxy

Syntax

netmeister proxy url *url* [**username** *username* **password** { **cipher | simple** } *string*]

undo netmeister proxy

View

System-view

デフォルト

設定なし

定義済みユーザロール

network-admin

パラメータ

url *url*:プロキシサーバの URL を指定します。*http://<domain>:<port>*形式で、大文字と小文字を区別して 8 から 128 文字の文字列を指定します。*<domain>*引数はプロキシサーバのドメイン名または IP アドレスを表し、*<port>*引数は 1 から 65535 の範囲のポート番号を表します。デフォルトのポート番号は 80 です。

username *username*:プロキシサーバへのアクセスに使用するユーザー名を指定します。1 から 31 文字の大文字と小文字が区別されます。文字列には、バックスラッシュ (¥) 、引用符 (") 、疑問符 (?) 、スペースを含めることはできません。。

password:プロキシサーバへのアクセスに使用するパスワードを指定します。

cipher:パスワードを暗号化形式で指定します。

simple:プレーンテキスト形式でパスワードを指定します。セキュリティ上の理由から、プレーンテキスト形式で指定されたパスワードは暗号化形式で保存されます。

string:パスワード文字列を指定します。プレーンテキスト形式は、大文字と小文字を区別する 1 から 31 文字の文字列です。暗号化された形式は、大文字と小文字を区別した 33 から 73 文字の文字列です。プレーンテキストのパスワードには、バックスラッシュ、引用符 (") 、疑問符 (?) 、またはスペースを含めることはできません。

説明

netmeister proxy コマンドを使用すると、装置は NetMeister 宛の https 通信のために指定されたプロキシサーバを利用します。親機への https 通信にはプロキシサーバを使用しません。**undo netmeister proxy** を使用して、プロキシサーバの指定を削除します。

netmeister proxy コマンドを設定する前に、netmeister enable が無効になっていることを確認してください。

netmeister proxy 複数回実行した場合、最新の設定が有効になります。

例

IP アドレス **192.168.1.254** の親機に接続する子機とし、NetMeister にはプロキシサーバ 10.1.1.254 (ポート:8080)を使用するように設定します。

<Switch> system-view

[Switch] netmeister parent ip 192.168.1.254

[Switch] netmeister proxy url http://10.1.1.254:8080

関連コマンド

- **netmeister enable**
- **display netmeister**

13.1.11 netmeister update

Syntax

netmeister update

View

System-view

定義済みユーザロール

network-admin

説明

netmeister update コマンドは NetMeister に登録している装置情報を即時更新します。

このコマンドは、10 秒以内に連続して実行しないでください。

このコマンドを実行する前に、netmeister enable コマンドを実行して、NetMeister を有効にする必要があります。

デバイスの NetMeister プロセスが再起動されていない状態で、デバイスは自動的に登録更新要求を 1 時間ごとに一定の間隔で NetMeister クラウドプラットフォームに送信します。この動作は、このコマンドの影響を受けません。

例

NetMeister クラウドプラットフォームへの登録更新リクエストの送信を有効にします。

<Sysname> system-view

[Sysname] netmeister update