NEC

GVT-125432-001-00 1.9

QX-S1100G 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	2020/04	初版発行
1.1	2020/08	・09 システム管理の 11 章 NetMeister に、NetMeister proxy コマンドを追加しました。
1.2	2020/01	・07-セキュリティの 2 章 802.1X のメモを変更 ・07-セキュリティの 3 章 MAC アドレス認証のメモを変更
1.3	2021/05	・07-セキュリティの 10 章 パスワード管理を追加 ・誤記訂正
1.4	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。
1.5	2022/07	・07-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。 ・07-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。 ・07-セキュリティの 2 章 802.1X の dot1x time コマンドの reauth-period reauth-period-value 設定最大値が変更になりました。 ・07-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。 ・07-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。 ・07-セキュリティの 4 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。 ・07-セキュリティの 4 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。 ・09-システム管理の 11 章 NetMiester に、netmeister management ip コマンドを追加しました。 ・誤記訂正

版数	日付	改版内容
1.6	2023/02	・02-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-IP サービスの 5 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 ・06-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-システム管理の 10 章 PoE について、誤記訂正しました。 ・09-システム管理の 11 章 NetMeister について、親機モードをサポートしました。 ・07-セキュリティの 11 章　SSL を追加しました。
1.7	2025/05	・表紙ロゴ色、配置の変更 ・02-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。 ・09-システム管理 10 章 PoE について以下を追加しました。 ・10.1.12 poe high-inrush を追加しました。 ・10.1.20 poe track を追加しました。 ・09-システム管理 11 章 Netmeister の 11.1.3 netmeister alarm enable notice を追加しました。 ・09-システム管理 11 章 Netmeister の 11.1.9 netmeister update を追加しました。
1.8	2025/07	・05-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。 ・05-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。 ・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
1.9	2026/10	・QX-S1100G シリーズ Ethernet スイッチマニュアル訂正資料 5.0 版の修正内容を反映しました。

Copyright © NEC Corporation 2020-2026

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-S*1100G 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-S1100G 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、S1100G シリーズ Ethernet スイッチに関する詳細な説明があります。

マニュアル	内容
QX-S1100G シリーズ 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-S1100G シリーズ 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-S1100G 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-S1100G 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。

- **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**

  デフォルトルーティング（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。

- **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**

  DLDP 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。

表記規則	説明
[ ]	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**	表示を無視して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**	表示を無視して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。

表記規則	説明
	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 9 個のセクションで構成されています。

01 - はじめに

02 - アクセス

03- IP サービス

04 - ルーティングプロトコル

05 - マルチキャスト

06- ACL and QoS

07 - セキュリティ

08 - 高可用性

09- システム管理

QX-S1100G 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-ログイン

03-RBAC

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 [| [by-linenum] { begin | exclude | include }] 1-3
1.1.3 display > 1-5
1.1.4 display >> 1-6
1.1.5 display alias 1-7
1.1.6 display history-command 1-8
1.1.7 display history-command all 1-9
1.1.8 display hotkey 1-10
1.1.9 hotkey 1-11
1.1.10 quit 1-12
1.1.11 return 1-13
1.1.12 screen-length disable 1-14
1.1.13 system-view 1-14

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 [| [by-linenum] { begin | exclude | include }]

Syntax

display *command* [| [**by-linenum**] { **begin** | **exclude** | **include** } *regular-expression*]&<1-128>

View

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。

[| [**by-linenum**] { **begin** | **exclude** | **include** } *regular-expression*]&<1-128>: 最大 128 のフィルタ条件を指定します。

- **by-linenum**: 出力行に番号を付けます。1 つのフィルタ条件でのみ指定する必要があります。
- **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 [| [**by-linenum**] { **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。

display コマンドの出力の特定の行をすばやく見つけるには、正規表現を使用して出力をフィルタ処理し、各出力行の前に数字を表示できます。正規表現の詳細は、セクション 1 *はじめに オペレーションマニュアル*の”*CLI*”を参照してください。

複数のフィルタ条件を指定すると、システムはすべての条件を満たす出力行を表示します。

行番号は５文字の文字列で、通常はコロン(:)が続きます。**by-linenum** オプションと **begin** *regular-expression* オプションの両方を指定すると、行番号の後にコロンまたはハイフン（-）が続く場合があります。

- **Colon**—行は正規表現と一致します。
- **Hyphen**—行は正規表現と一致しません。

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
```

SHELL と **VTY** の両方を含むログバッファのログエントリを表示します。

<Switch> display logbuffer | include SHELL | include VTY

```
%Sep  6 10:38:12:320 2018 Sysname SHELL/5/SHELL_LOGIN: VTY logged in from
169.254.100.171.
%Sep  6 10:52:32:576 2018 Sysname SHELL/5/SHELL_LOGOUT: VTY logged out from
169.254.100.171.
%Sep  6 16:03:27:100 2018 Sysname SHELL/5/SHELL_LOGIN: VTY logged in from
169.254.100.171.
%Sep  6 16:44:18:113 2018 Sysname SHELL/5/SHELL_LOGOUT: VTY logged out from
169.254.100.171.
```

user-group を含む最初の行から開始し、出力行に番号を付けて、実行中の設定を表示します。

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

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

1.1.3 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
```

1.1.4 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
```

1.1.5 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

1.1.6 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

1.1.7 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

1.1.8 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_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_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.
          -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

1.1.9 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

1.1.10 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>

1.1.11 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>

1.1.12 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

1.1.13 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 ログイン 2-1
2.1 ログイン設定コマンド 2-1
2.1.1 authentication-mode 2-1
2.1.2 auto-execute command 2-3
2.1.3 databits 2-4
2.1.4 display ip http 2-5
2.1.5 display ip https 2-6
2.1.6 display line 2-7
2.1.7 display telnet client 2-9
2.1.8 display user-interface 2-10
2.1.9 display users 2-12
2.1.10 display web users 2-13
2.1.11 escape-key 2-14
2.1.12 free line 2-17
2.1.13 free user-interface 2-18
2.1.14 free web users 2-19
2.1.15 history-command max-size 2-19
2.1.16 idle-timeout 2-20
2.1.17 ip http acl 2-21
2.1.18 ip http enable 2-22
2.1.19 ip http port 2-23
2.1.20 ip https acl 2-24
2.1.21 ip https certificate access-control-policy 2-25
2.1.22 ip https enable 2-26
2.1.23 ip https port 2-27
2.1.24 ip https ssl-server-policy 2-27
2.1.25 line 2-28
2.1.26 line class 2-29
2.1.27 lock 2-30
2.1.28 parity 2-31
2.1.29 protocol inbound 2-32
2.1.30 screen-length 2-34
2.1.31 send 2-36
2.1.32 set authentication password 2-37
2.1.33 shell 2-38
2.1.34 speed 2-39

2.1.35 stopbits 2-40
2.1.36 telnet 2-41
2.1.37 telnet client source 2-42
2.1.38 telnet ipv6 2-43
2.1.39 telnet server acl 2-44
2.1.40 telnet server dscp 2-45
2.1.41 telnet server enable 2-46
2.1.42 telnet server ipv6 acl 2-46
2.1.43 telnet server ipv6 dscp 2-47
2.1.44 terminal type 2-48
2.1.45 user-interface 2-49
2.1.46 user-interface class 2-50
2.1.47 user-role 2-52
2.1.48 web idle-timeout 2-53

2章 ログイン

2.1 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。

2.1.1 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 の詳細はセクション 8 *セキュリティ オペレーションマニュアル*の”*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。AUX line class view では、**none** 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 つの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

2.1.2 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。

2.1.3 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

2.1.4 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
Operation status: Enabled
```

表 2-1 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。
Operation 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**

2.1.5 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
Operation status: Enabled
```

表 2-2 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。
Operation 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**

2.1.6 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 2-3 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


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

表 2-4 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。

2.1.7 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

2.1.8 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 2-5 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


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

表 2-6 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。

2.1.9 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   :
       User role list: network-admin network-operator
       Location: 192.168.1.107
VTY 2   :
       User role list: level-0 network-admin network-operator
       Location: 192.168.1.134
 +    : Current operation user.
 F    : Current operation user works in async mode.
```

表 2-7 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。
User name	ユーザが使用するユーザ名です。 このフィールドは、ユーザがログイン時の認証にユーザ名とパスワードを提供した場合にのみ表示されます。
User role list	ユーザに割り当てられたユーザロールです。
Location	カレントユーザのIPアドレスです。

2.1.10 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 2-8 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。

2.1.11 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 2-9 を参照してください。

表 2-9 Ctrl キーを使用する ASCII コード

フィールド	説明
Ctrl+A	1
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

フィールド	説明
Ctrl+X	24
Ctrl+Y	25
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。

1)　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
```

2)　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>
```

2.1.12 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]
```

2.1.13 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]
```

2.1.14 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

2.1.15 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。詳細はセクション 1 *はじめに オペレーションマニュアル*の“*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

2.1.16 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

2.1.17 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（セクション 7 ACL and QoS コマンドマニュアル）

2.1.18 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

2.1.19 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

2.1.20 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（セクション 7 ACL and QoS コマンドマニュアル）

2.1.21 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

2.1.22 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

2.1.23 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

2.1.24 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

2.1.25 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

2.1.26 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

2.1.27 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>
```

2.1.28 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

2.1.29 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   :
       User role list: network-admin network-operator
       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

2.1.30 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

2.1.31 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.
```

2.1.32 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 Versioin7.1.3 では、1～16 文字、Version7.1.5 を含むそれ以降のバージョンでは、4～16 文字です。なお、Version7.1.5 を含むそれ以降のバージョンでは、2 種類以上の文字タイプを使用する必要があります。

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。

2.1.33 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]
```

2.1.34 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

2.1.35 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

2.1.36 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

2.1.37 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

2.1.38 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

2.1.39 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 の詳細はセクション *7 ACL and QoS オペレーションマニュアル*の”*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

2.1.40 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

2.1.41 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

2.1.42 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 の詳細はセクション 7 *ACL and QoS オペレーションマニュアル*の”*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

2.1.43 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

2.1.44 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

2.1.45 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

2.1.46 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

2.1.47 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。

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

2.1.48 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。

3 章 RBAC 3-1
3.1 RBAC 設定コマンド 3-1
3.1.1 description 3-1
3.1.2 display role 3-2
3.1.3 display role feature 3-10
3.1.4 display role feature-group 3-13
3.1.5 feature 3-15
3.1.6 interface policy deny 3-16
3.1.7 permit interface 3-18
3.1.8 permit vlan 3-20
3.1.9 role 3-22
3.1.10 role default-role enable 3-23
3.1.11 role feature-group 3-24
3.1.12 rule 3-25
3.1.13 super 3-29
3.1.14 super authentication-mode 3-30
3.1.15 super default role 3-31
3.1.16 super password 3-32
3.1.17 vlan policy deny 3-34

3章 RBAC

3.1 RBAC設定コマンド

3.1.1 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**

3.1.2 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 3-1 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

3.1.3 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 3-2 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 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。
(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。

フィールド	説明
(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

3.1.4 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: 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: ofp           (OFP related commands)
Feature: port-security   (Port-security related commands)
Feature: l2pt          (L2PT related commands)
Feature: dot1xc         (Dot1x client related commands)

Feature group: L3
Feature: route         (Route management related commands)
Feature: staticrt       (Unicast static route related commands)
Feature: lisp          (LISP protocol related commands)
Feature: multicast      (Multicast 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 3-2 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 ; user-profile * ; igmp-snooping *    (W)
  system-view ; vlan * ; igmp-snooping *    (W)
  system-view ; vlan * ; pim-snooping *    (W)
  system-view ; interface * ; igmp-snooping *    (W)
  display igmp-snooping *    (R)
  display pim-snooping *    (R)
  display l2-multicast *    (R)
  system-view ; probe ; display system internal l2-multicast *    (R)
  reset igmp-snooping *    (W)
  reset pim-snooping *    (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 ; user-profile * ; mld-snooping *    (W)
  system-view ; vlan * ; mld-snooping *    (W)
```

```
  system-view ; vlan * ; ipv6 pim-snooping *    (W)
  system-view ; interface * ; mld-snooping *    (W)
  display mld-snooping *    (R)
  display ipv6 pim-snooping *    (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 l2-multicast *    (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: lisp           (LISP protocol related commands)
```

関連コマンド

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

3.1.5 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**

3.1.6 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**

3.1.7 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**

3.1.8 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。

デフォルトでは、すべてのアクセスポートは VLAN 1 に属します。**port access vlan** コマンドを使用してアクセスポートを他の VLAN に割り当てるには、VLAN 1 と新しい VLAN の両方にアクセスできるユーザロールがあることを確認します。

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 1、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 1 2 4 50 to 100

[Switch-role-role1-vlanpolicy] quit

[Switch-role-role1] quit

2) VLAN 1、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**

3.1.9 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**

3.1.10 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

3.1.11 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**

3.1.12 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 3-3 のガイドラインに従ってください。

表 3-3 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。
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。

ルール	ガイドライン
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**
- **role**

3.1.13 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

- **super authentication-mode**
- **super password**

3.1.14 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、セクション 8 *セキュリティ オペレーションマニュアル*の“*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

super password

3.1.15 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**

3.1.16 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。

グローバルパスワード制御機能を有効にすると、すべての履歴スーパーパスワードがハッシュ形式で保存されます。

- プレーンテキスト形式で新しいスーパーパスワードを設定する場合、新しいスーパーパスワードが現在のスーパーパスワードと履歴スーパーパスワードレコードに保存されているものと異なることを確認してください。
- ハッシュ形式で新しいスーパーパスワードを設定すると、システムは新しいスーパーパスワードを現在のスーパーパスワードまたは履歴スーパーパスワードレコードに保存されているパスワードと比較しません。

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**

3.1.17 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。

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 dscp 4-6
4.1.8 ftp server enable 4-7
4.1.9 ftp server ipv6 dscp 4-7
4.1.10 ftp timeout 4-8
4.2 FTP クライアント設定コマンド 4-9
4.2.1 ? 4-9
4.2.2 ascii 4-10
4.2.3 binary 4-11
4.2.4 bye 4-12
4.2.5 cd 4-12
4.2.6 cdup 4-13
4.2.7 close 4-14
4.2.8 debug 4-15
4.2.9 delete 4-16
4.2.10 dir 4-16
4.2.11 disconnect 4-18
4.2.12 display ftp client source 4-18
4.2.13 ftp 4-19
4.2.14 ftp client ipv6 source 4-20
4.2.15 ftp client source 4-21
4.2.16 ftp ipv6 4-22
4.2.17 get 4-24
4.2.18 help 4-25
4.2.19 lcd 4-26
4.2.20 ls 4-27
4.2.21 mkdir 4-28
4.2.22 newer 4-29
4.2.23 open 4-30

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

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 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

4.1.8 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

4.1.9 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

4.1.10 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 ?

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

4.2.2 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

4.2.3 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

4.2.4 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

4.2.5 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セクション 1 *はじめに オペレーションマニュアル*の“*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**

4.2.6 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**

4.2.7 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

4.2.8 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).
```

4.2.9 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
```

4.2.10 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

4.2.11 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

4.2.12 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.
```

4.2.13 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>
```

4.2.14 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

4.2.15 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

4.2.16 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、セクション 4 *IP サービス オペレーションマニュアルの“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
```

4.2.17 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

4.2.18 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

?

4.2.19 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
```

4.2.20 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

4.2.21 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
```

4.2.22 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)
```

4.2.23 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>
```

4.2.24 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.
```

4.2.25 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

4.2.26 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
```

4.2.27 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

4.2.28 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。
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。

フィールド	説明
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。

4.2.29 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

4.2.30 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.
```

4.2.31 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)
```

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、セクション 4 *IP サービス オペレーションマニュアル*の“*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-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 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 6-22
6.1.20 undelete 6-23

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**：

- 記憶媒体、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。詳細はセクション 1 *はじめに オペレーションマニュアル*の“*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	セクション1 *はじめに オペレーションマニュアル*の“*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:/
...
```

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: ごみ箱を空にする操作を除き、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、ごみ箱を空にする操作を除き、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。

重要：

このコマンドに **screen** パラメータを指定する前に、**tar list** コマンドを使用して、アーカイブされたファイルのタイプを識別します。ベストプラクティスとして、すべてのアーカイブファイルがテキストファイルである場合にのみパラメータを指定します。端末制御文字を含むアーカイブされた非テキストファイルのコンテンツを表示すると、文字化けが発生し、端末が正しく動作しなくなる場合があります。ターミナルを再度使用するには、現在の接続を閉じて、装置に再度ログインする必要があります。

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 7-6
7.1.6 display saved-configuration 7-8
7.1.7 display startup 7-9
7.1.8 display this 7-10
7.1.9 reset saved-configuration 7-11
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。

このコマンドは、起動構成を以下の順序で検索します。

1) cfg メイン next-startup 構成ファイル。
2) cfg メイン next-startup 構成ファイルが使用できない場合、.cfg バックアップ next-startup 構成ファイル。

両方の構成ファイルが使用できない場合、システムは次回起動時の構成ファイルが存在しないことを示すメッセージを表示します。

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*－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*－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*－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*－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。

フィールド	説明
- 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。

startup-configuration パラメータを指定すると、システムは起動設定を以下の順序で検索します

1) cfg メイン next-startup 構成ファイル。
2) cfg メイン next-startup 構成ファイルが使用できない場合は、.cfg バックアップ next-startup 構成ファイル

両方の構成ファイルが使用できない場合、システムは次回起動時の構成ファイルが存在しないことを示すメッセージを表示します。

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。

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

```
MainBoard:
 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
MainBoard	装置上のスタートアップ構成ファイルを表示します。
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。フィールドの末尾にアスタリスク（*）が付いている場合、スタートアップ構成ファイルはバイナリ構成ファイルです。

フィールド	説明
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

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大文字、小文字を区別せず、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。

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。

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。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。

slot *slot-number*: 装置のスロット番号を指定します。これは 1 に固定されています。

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

startup saved-configuration コマンドは、ファイルを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。

undo startup saved-configuration コマンドは、次回の起動時に工場出荷状態で起動するようにコンフィグレーションファイルの指定をリセットします。

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の属性を NULL に変更します。2 つのコンフィグレーションファイルを削除しません。

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 8-3
8.1.3 display boot-loader 8-4

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。この設定範囲にはスロット番号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セクション 1 の*はじめに オペレーションマニュアル*の“*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。この設定範囲にはスロット番号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セクション 1 の*はじめに オペレーションマニュアル*の“*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。この設定範囲にはスロット番号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セクション 1 の*はじめに オペレーションマニュアル*の“*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*: 装置のスロット番号を指定します。これは 1 に固定されています。

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。

装置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

装置のメンバ 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
  feature.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.
File flash:/feature.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.
Decompressing               file               feature.bin               to
flash:/feature.bin.....Done.
```

```
Verifying the file flash:/boot.bin on slot 1...Done.
Verifying the file flash:/system.bin on slot 1.............Done.
Verifying the file flash:/feature.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.
```

関連コマンド

display boot-loader

8.1.2 bootrom update

Syntax

bootrom update file *file* **slot** *slot-number*

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*: 装置のスロット番号を指定します。これは 1 に固定されています。

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*: 装置のスロット番号を指定します。これは 1 に固定されています。

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
  flash:/feature.bin
Main startup software images:
  flash:/boot.bin
  flash:/system.bin
  flash:/feature.bin
Backup startup software images:
  flash:/boot.bin
```

```
flash:/system.bin
flash:/feature.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 copyright-info enable 9-6
9.1.6 display clock 9-6
9.1.7 display cpu-usage 9-7
9.1.8 display cpu-usage history 9-8
9.1.9 display device 9-10
9.1.10 display device manuinfo 9-11
9.1.11 display diagnostic-information 9-12
9.1.12 display environment 9-14
9.1.13 display fan 9-15
9.1.14 display memory 9-16
9.1.15 display memory-threshold 9-17
9.1.16 display power 9-19
9.1.17 display transceiver interface 9-19
9.1.18 display version 9-21
9.1.19 header 9-22
9.1.20 locator blink 9-23
9.1.21 memory-threshold 9-24
9.1.22 monitor cpu-usage enable 9-25
9.1.23 monitor cpu-usage interval 9-26
9.1.24 monitor cpu-usage threshold 9-27
9.1.25 password-recovery enable 9-28
9.1.26 reboot 9-29
9.1.27 shutdown-interval 9-31
9.1.28 sysname 9-32
9.1.29 temperature-limit 9-32

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 の詳細はセクション 10 *システム管理 オペレーションマニュアル*の”*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 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

9.1.6 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**

9.1.7 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*: 装置のスロット番号を指定します。これは 1 に固定されています。

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。

9.1.8 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*: 装置のスロット番号を指定します。これは 1 に固定されています。

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**

9.1.9 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*: 装置のスロット番号を指定します。これは 1 に固定されています。

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

Display device information.

<Switch> display device

```
Slot 1
Slot Type            State    Subslot  Soft Ver          Patch Ver
1    QX-S1148GT-4G    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	装置の役割です。
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。 装置で増分パッチイメージと非増分パッチイメージの両方が実行されている場合、このフィールドには最新リリースの増分パッチイメージバージョンが表示されます。 パッチイメージタイプの詳細については、セクション1 *はじめにオペレーションマニュアルの“ソフトウェアのアップグレード”*を参照してください。

9.1.10 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*: 装置のスロット番号を指定します。これは 1 に固定されています。

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-S1108GT-2G-PW
DEVICE_SERIAL_NUMBER : 219801A1B19173Q00020
MAC_ADDRESS         : 9C06-1B4F-504C
MANUFACTURING_DATE   : 2017-03-11
VENDOR_NAME         : NEC
Power 1:
The operation is not supported on the specified power.
```

9.1.11 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**

9.1.12 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*: 装置のスロット番号を指定します。これは 1 に固定されています。

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	センサ温度です。 **hotspot**—ホットスポットセンサ

フィールド	説明
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。

9.1.13 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*: 装置のスロット番号を指定します。これは 1 に固定されています。

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	装置のスロット番号です。常に1を示します。
Fan 1	内蔵ファンの番号です。
State	ファントレイ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**–ファントレイが正常に動作しています。 ● **Fault**–ファントレイに問題があります。

9.1.14 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*: 装置のスロット番号を指定します。これは 1 に固定されています。

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。

9.1.15 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*: 装置のスロット番号を指定します。これは 1 に固定されています。

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
```

9.1.16 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*: 装置のスロット番号を指定します。これは 1 に固定されています。

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       --          --          --
```

9.1.17 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 9-6 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。

フィールド	説明
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。

9.1.18 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

```
H3C Comware Software, Version 7.1.070, Test 6803
Copyright (c) 2004-2019 New H3C Technologies Co., Ltd. All rights reserved.
H3C QX-S1116GT-4G-PW uptime is 0 weeks, 0 days, 6 hours, 43 minutes
```

```
Last reboot reason : Cold reboot

Boot image: flash:/s1116gt_4g-cmw710-boot-t6803.bin
Boot image version: 7.1.070, Test 6803
  Compiled Jan 21 2019 11:00:00
System image: flash:/s1116gt_4g-cmw710-system-t6803.bin
System image version: 7.1.070, Test 6803
  Compiled Jan 21 2019 11:00:00
Boot image: flash:/s1116gt_4g-cmw710-boot-f6123.bin
Boot image version: 7.1.070, Feature 6123
  Compiled Aug 24 2017 16:00:00
System image: flash:/s1116gt_4g-cmw710-system-f6123.bin
System image version: 7.1.070, Feature 6123
  Compiled Aug 24 2017 16:00:00
...
```

9.1.19 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、セクション 1 *はじめに オペレーションマニュアル*の”*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%
```

9.1.20 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 Version 7.1.9 を含む以降のソフトウェアからサポートしています。

9.1.21 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*: 装置のスロット番号を指定します。これは 1 に固定されています。

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。

メモリアラームが発生した場合は、未使用の構成アイテムを削除するか、一部の機能を無効にしてメモリの空き容量を増やします。 メモリスペースが不足しているため、一部の構成アイテムを削除できない場合があります。

しきい値の詳細はセクション 1 *はじめに オペレーションマニュアルの”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

9.1.22 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*: 装置のスロット番号を指定します。これは 1 に固定されています。

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 history**
- **monitor cpu-usage interval**

9.1.23 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*: 装置のスロット番号を指定します。これは 1 に固定されています。

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 history**
- **monitor cpu-usage enable**

9.1.24 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*: 装置のスロット番号を指定します。これは 1 に固定されています。

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

9.1.25 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 メニューから装置構成と 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

9.1.26 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*: 装置のスロット番号を指定します。これは 1 に固定されています。

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。

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...
```

9.1.27 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

9.1.28 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]

9.1.29 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 9-7 に温度アラームのしきい値のデフォルトを示します。

表 9-7 温度アラームのしきい値のデフォルトと推奨値(QX-S1100G シリーズ)

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-S1108GT-2G	Hotspot 1	0	87	84	92	98
	Hotspot 2	0	85	100	90	110
QX-S1116GT-4G	Hotspot 1	0	80	84	85	98
	Hotspot 2	0	88	100	93	110
	Hotspot 3	0	95	100	100	110
QX-S1124GT-4G	Hotspot 1	0	87	84	92	98
	Hotspot 2	0	99	100	104	110
	Hotspot 3	0	105	100	110	110
	Hotspot 4	0	104	100	109	110
QX-S1148GT-4G	Hotspot 1	0	88	84	93	98
	Hotspot 2	0	93	84	98	98
	Hotspot 3	0	108	100	113	110
	Hotspot 4	0	109	100	114	110
	Hotspot 5	0	80	100	85	110
	Hotspot 6	0	84	100	89	110
	Hotspot 7	0	83	100	88	110
	Hotspot 8	0	88	100	93	110
QX-S1108GT-2G-PW	Hotspot 1	0	77	84	82	98
	Hotspot 2	0	93	100	98	110
	Hotspot 3	0	87	110	92	130

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-S1116GT-4G-PW	Hotspot 1	0	72	84	77	98
	Hotspot 2	0	69	100	74	110
	Hotspot 3	0	80	100	85	110
	Hotspot 4	0	78	110	83	130
QX-S1124GT-4G-PW	Hotspot 1	0	63	84	68	98
	Hotspot 2	0	77	100	82	110
	Hotspot 3	0	88	100	93	110
	Hotspot 4	0	87	100	92	110
	Hotspot 5	0	61	100	66	110
	Hotspot 6	0	63	100	68	110
	Hotspot 7	0	71	110	76	130

View

System view

定義済みユーザロール

network-admin

パラメータ

slot *slot-number*: 装置のスロット番号を指定します。これは 1 に固定されています。

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 9-8 温度アラームのしきい値の設定範囲(QX-S1100G シリーズ)

装置	センサ	下限温度	ワーニング温度	アラーム温度
QX-S1108GT-2G	Hotspot 1～4	-10℃ ～ +70℃	15℃ ～ 125℃	20℃ ～ 135℃
QX-S1116GT-4G	Hotspot 1～4	-10℃ ～ +70℃	15℃ ～ 125℃	20℃ ～ 135℃
QX-S1124GT-4G	Hotspot 1～4	-10℃ ～ +70℃	15℃ ～ 125℃	20℃ ～ 135℃
QX-S1148GT-4G	Hotspot 1～8	-10℃ ～ +70℃	15℃ ～ 125℃	20℃ ～ 135℃
QX-S1108GT-2G-PW	Hotspot 1～3	-10℃ ～ +70℃	15℃ ～ 125℃	20℃ ～ 135℃
QX-S1116GT-4G-PW	Hotspot 1～4	-10℃ ～ +70℃	15℃ ～ 125℃	20℃ ～ 135℃
QX-S1124GT-4G-PW	Hotspot 1～7	-10℃ ～ +70℃	15℃ ～ 125℃	20℃ ～ 135℃
QX-S1148GT-4G-PW	Hotspot 1～9	-10℃ ～ +70℃	15℃ ～ 125℃	20℃ ～ 135℃
QX-S1108GT-2G-I	Hotspot 1～2	-10℃ ～ +70℃	15℃ ～ 125℃	20℃ ～ 135℃
QX-S1108GT-2G-PW-I	Hotspot 1～3	-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

装置の 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

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 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-S1100G シリーズ Ethernet スイッチ

コマンドマニュアル

2. 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-Voice VLAN

12-LLDP

13- L2PT

14- Private VLAN

目次

このセクションのページは **2-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 1-22
1.1.8 eee enable 1-23
1.1.9 flow-control 1-24
1.1.10 flow-interval 1-25
1.1.11 ifmonitor crc-error 1-26
1.1.12 ifmonitor input-error 1-27
1.1.13 ifmonitor output-error 1-29
1.1.14 interface 1-30
1.1.15 jumboframe enable 1-31
1.1.16 link-delay 1-32
1.1.17 loopback 1-33
1.1.18 multicast-suppression 1-34
1.1.19 port auto-power-down 1-36
1.1.20 reset counters interface 1-37
1.1.21 shutdown 1-38
1.1.22 speed 1-39
1.1.23 unicast-suppression 1-40
1.2 レイヤ 2 Ethernet インタフェース設定コマンド 1-42
1.2.1 display storm-constrain 1-42
1.2.2 mdix-mode 1-44
1.2.3 speed auto 1-45
1.2.4 storm-constrain 1-46
1.2.5 storm-constrain control 1-48
1.2.6 storm-constrain enable log 1-49
1.2.7 storm-constrain enable trap 1-50
1.2.8 storm-constrain interval 1-51
1.2.9 virtual-cable-test 1-52

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 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-S1124GT-4G-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。

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

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 (pps)	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 (pps)	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 (pps)	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 の詳細情報を表示します。

<Switch> display interface gigabitethernet 1/0/1

```
GigabitEthernet1/0/1
Current state: DOWN
Line protocol state: DOWN
IP packet frame type: Ethernet II, hardware address: 000c-2963-b767
Description: GigabitEthernet1/0/1 Interface
Bandwidth: 100000 kbps
Loopback is not set
Media type is twisted pair,port hardware type is 1000_BASE_T_AN_SFP
Unknown-speed mode, unknown-duplex mode
Link speed type is autonegotiation, link duplex type is autonegotiation
Flow-control is not enabled
Maximum frame length: 9216
Allow jumbo frame to pass
Broadcast max-ratio: 100%
Multicast max-ratio: 100%
Unicast max-ratio: 100%
PVID: 1
MDI type: Automdix
Port link-type: Access
 Tagged VLANs:   None
 UnTagged VLANs: 1
Port priority: 2
Last link flapping: 6 hours 39 minutes 25 seconds
```

```
Last clearing of counters:  14:34:09 Tue 11/01/2011
Current system time:2018-08-10 14:58:27
Last time when physical state changed to up:-
Last time when physical state changed to down:2018-08-10 14:57:58
 Peak input rate: 0 bytes/sec, at 2013-07-17 22:06:19
 Peak output rate: 0 bytes/sec, at 2013-07-17 22:06:19
 Last 300 seconds input:  0 packets/sec 0 bytes/sec -%
 Last 300 seconds output:  0 packets/sec 0 bytes/sec -%
Input (total):  0 packets, 0 bytes
         0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
 Input (normal):  0 packets, 0 bytes
         0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
 Input:  0 input errors, 0 runts, 0 giants, 0 throttles
         0 CRC, 0 frame, 0 overruns, 0 aborts
         0 ignored, 0 parity errors
 Output (total): 0 packets, 0 bytes
         0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
 Output (normal): 0 packets, 0 bytes
         0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
 Output: 0 output errors, 0 underruns, 0 buffer failures
         0 aborts, 0 deferred, 0 collisions, 0 late collisions
         0 lost carrier, 0 no carrier
```

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。 ● **DOWN (Monitor-Link uplink down)**— インタフェースはモニタリンクによってシャットダウンされました。 ● **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。 ● **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。
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。
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。

フィールド	説明
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。
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。

フィールド	説明
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。
Current system time	YYYY / MM / DD HH：MM：SS形式の現在のシステム時刻です。タイムゾーンが設定されている場合、このフィールドはYYYY / MM / DD HH：MM：SSゾーン名±HH：MM：SS形式です。zone-name引数はローカルタイムゾーンです。

フィールド	説明
Last time when physical state changed to up	インタフェースの物理状態が最後に変更された最後の時間です。 タイムゾーンが設定されている場合、このフィールドは YYYY / MM / DD HH : MM : SSゾーン名±HH : MM : SS形式です。 zone-name引数はローカルタイムゾーンです。 ハイフン（-）は、インタフェースの物理状態が変更されていないことを示します。
Last time when physical state changed to down	インタフェースの物理状態が最後にダウンしたときです。 タイムゾーンが設定されている場合、このフィールドは YYYY / MM / DD HH : MM : SSゾーン名±HH : MM : SS形式です。 zone-name引数はローカルタイムゾーンです。 ハイフン（-）は、インタフェースの物理状態が変更されていないことを示します
Last 300 seconds input: 0 packets/sec 0 bytes/sec 0% Last 300 seconds 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。
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。

フィールド	説明
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。
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。

フィールド	説明
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。
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。

フィールド	説明
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。
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    aaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

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
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。
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。

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**—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。 • **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。 • **Port Security Disabled**—インタフェースが不正なパケットを受信したため、侵入検知メカニズムによってインタフェースがシャットダウンされました。

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 を含む 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:**

このコマンドは光ファイバのトランシーバモジュールで動作する SFP ポートで未サポートです。

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 EEE 省電力機能を有効にします。

undo eee enable コマンドはデフォルトに戻します。

EEE 省電力機能を有効にすることで、ポートで一定期間、パケットを受信しない場合、アップリンクポートを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、ポート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-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

1.1.11 ifmonitor crc-error

メモ:

Ifmonitor 機能は Version7.1.16 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

1.1.12 ifmonitor input-error

🕮 メモ:

Ifmonitor 機能は Version7.1.16 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

1.1.13 ifmonitor output-error

🕮 **メモ:**

Ifmonitor 機能は Version7.1.16 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

1.1.14 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]

1.1.15 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

1.1.16 link-delay

Syntax

link-delay { **down** | **up** } [**msec**] *delay-time*

undo link-delay { **down** | **up** }

デフォルト

0 秒

View

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、0～120 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。インタフェースで **link-delay** コマンドを複数回実行する場合、次の規則が適用されます。

- リンクアップイベントとリンクダウンイベントの抑制間隔を個別に設定できます。
- リンクアップイベントまたはリンクダウンイベントの抑制間隔を複数回設定すると、最新の設定が有効になります。

スパニングツリープロトコルまたは Smart Link が有効になっているインタフェースでは、このコマンドを実行しないでください。

このコマンド、**dampening** コマンド、および **port link-flap protect enable** コマンドは、イーサネットインタフェース上で相互に排他的です。

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

1.1.17 loopback

Syntax

loopback { **external** | **internal** }

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。

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

1.1.18 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 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**

1.1.19 port auto-power-down

重要:

- **port auto-power-down** コマンドは SFP ポートで未サポートです。
- **port auto-power-down** コマンドは QX-S1100G シリーズで未サポートです。

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

1.1.20 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 interface

1.1.21 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

1.1.22 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 を含む 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

1.1.23 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 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**

1.2 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 - unknown unicast;
             KNUC - known unicast; FW - forwarding
 Flow Statistic Interval: 5 (in seconds)
Port         Type Lower    Upper    Unit  Mode    Status   Trap Log StateChg
------------------------------------------------------------------------------
---
```

表 1-5 GE1/0/1　　MC　100　　200　　kbps　shutdown shutdown off　on　10 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。
Mode	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。
StateChg	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 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 ポート、10/100M 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。

このコマンドは、ファイバーポートでは使用できません。

イーサネットインタフェースのリンクがアップしている場合、ケーブル接続をテストすると、リンクがダウンしてからアップします。

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 **2-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。**loopback** キーワードを指定し、interface-number を指定しない場合、コマンドは装置上のすべての既存のループバックインタフェースに関する情報を表示します。

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。
baudrate	ボーレート（単位はKbpsです）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。**null** キーワードを指定しない場合、コマンドはすべてのインタフェースに関する情報を表示します。

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、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, baudrate: 1000000 kbps
Last clearing of counters: Never
Last 300 seconds input rate:  0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate:  0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops
```

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 および表 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。**loopback** キーワードを指定しない場合、コマ

ンドはすべてのインタフェースの統計情報をクリアします。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。null キーワードを指定しない場合、コマンドはすべてのインタフェースの統計情報を削除します。

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 **2-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。インタフェース範囲を指定する場合、インタフェースはすべて固定インタフェースであるか、同じインタフェースカード上にある必要があります。*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。

装置は、インタフェースレンジ設定プロセス中にプロンプトまたはアラームメッセージを出力しません。 インタフェースレンジ設定の影響を十分に認識してください。

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。インタフェースの範囲を指定する場合、インタフェースはすべて固定インタフェースであるか、同じインタフェースカード上にある必要があります。*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。

装置は、インタフェースレンジ設定プロセス中にプロンプトまたはアラームメッセージを出力しません。 インタフェースレンジ設定の影響を十分に認識してください。

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 **2-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 4-3
4.1.4 display mac-address mac-learning 4-4
4.1.5 display mac-address mac-move 4-5
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 4-12
4.1.10 mac-learn-mode 4-13
4.1.11 mac-address mac-learning enable 4-14
4.1.12 mac-address mac-move fast-update 4-16
4.1.13 mac-address max-mac-count 4-16
4.1.14 mac-address max-mac-count enable-forwarding 4-17
4.1.15 mac-address notification mac-move 4-18
4.1.16 mac-address notification mac-move suppression (interface view) 4-20
4.1.17 mac-address notification mac-move suppression (system view) 4-21
4.1.18 mac-address timer 4-22
4.1.19 snmp-agent trap enable mac-address 4-23

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**] [**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。

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。

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。 ● **Block**— MAC認証に失敗したユーザの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。
Aging	エントリがエージアウト可能かどうかを示します。 ● **Y**—エントリはエージアウト可能です。 ● **N**—エントリはエージアウトできません。
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 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*: 装置のスロット番号を指定します。これは 1 に固定されています。

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。

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

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。

フィールド	説明
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** | **static** } *mac-address* **vlan** *vlan-id*

undo mac-address { **dynamic** | **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。

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

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*

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 [[*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。

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設定します。装置向け（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 向け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。

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）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

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-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。

注意:

- 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。

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

4.1.11 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、セクション 3 *アクセス オペレーションマニュアル*の“*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

4.1.12 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

4.1.13 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

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 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、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。MAC アドレス移動カウントの数が 20 を超える場合、最初の 20 カウントのみが保持されます。 次に、次の検出間隔で、装置は前の検出間隔で生成されたすべての MAC アドレス移動カウントを破棄し、MAC 移動カウント生成の別のラウンドを開始します。

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 10～630 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 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 の詳細はセクション 10 *システム管理 オペレーションマニュアルの*“*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 **2-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 **2-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 mode 6-21
6.1.13 link-aggregation port-priority 6-22
6.1.14 link-aggregation selected-port maximum 6-23
6.1.15 link-aggregation selected-port minimum 6-24
6.1.16 port link-aggregation group 6-25
6.1.17 reset counters interface 6-26
6.1.18 reset lacp statistics 6-27
6.1.19 shutdown 6-27

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
Line protocol 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               DOWN 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。
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。この例では、デフォルト設定が表示されます。

<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。この例では、ユーザが構成した設定を表示します。

<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。この例では、デフォルト設定を表示します。

<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。この例では、ユーザが構成した設定を表示します。

<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。この出力例では、送信元および宛先IPアドレスと送信元および宛先MACアドレスに基づいて、レイヤ2トラフィックが配信されます。
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。この出力例では、送信元および宛先IPアドレスと送信元および宛先MACアドレスに基づいて、レイヤ3トラフィックが配信されます。
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。

フィールド	説明
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。
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
Creation Mode: Manual
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。 尚、ビットが1の場合には該当のアルファベットを表示しますが、ビットが0の場合は表示しません。 ● **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。
Creation Mode	アグリゲートインタフェースの作成モードです。 ● **Auto.** ● **Manual.**
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、**Index**と**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

6.1.12 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。

アグリゲーションモードを変更するときは、変更がサービスに与える影響を必ず理解してください。

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

6.1.13 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

6.1.14 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選択されたポートの最大数は、選択されたポートの最小数以上である必要があります。

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

6.1.15 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。

アグリゲーショングループの選択集合インタフェースで両方の設定を構成する場合、より高い「選択されたポート番号の制限」が有効になります。ポートの最小数または最小割合を設定できます。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。

アグリゲーショングループの場合、選択されたポートの最小数は、選択されたポートの最大数以下でなければなりません。

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

6.1.16 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

6.1.17 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

6.1.18 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

6.1.19 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 **2-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-S1100G 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 **2-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 edged-port 8-35
8.1.23 stp enable 8-36
8.1.24 stp global config-digest-snooping 8-37
8.1.25 stp global enable 8-38
8.1.26 stp global mcheck 8-39
8.1.27 stp log enable tc 8-40
8.1.28 stp loop-protection 8-41
8.1.29 stp max-hops 8-42
8.1.30 stp mcheck 8-42
8.1.31 stp mode 8-44
8.1.32 stp no-agreement-check 8-45
8.1.33 stp pathcost-standard 8-46
8.1.34 stp point-to-point 8-47

8.1.35 stp port bpdu-protection 8-48
8.1.36 stp port priority 8-49
8.1.37 stp port shutdown permanent 8-50
8.1.38 stp port-log 8-51
8.1.39 stp priority 8-52
8.1.40 stp pvst-bpdu-protection 8-53
8.1.41 stp region-configuration 8-54
8.1.42 stp role-restriction 8-55
8.1.43 stp root primary 8-56
8.1.44 stp root secondary 8-57
8.1.45 stp root-protection 8-58
8.1.46 stp tc-protection 8-59
8.1.47 stp tc-protection threshold 8-60
8.1.48 stp tc-snooping 8-61
8.1.49 stp timer forward-delay 8-61
8.1.50 stp timer hello 8-63
8.1.51 stp timer max-age 8-64
8.1.52 stp timer-factor 8-65
8.1.53 stp transmit-limit 8-66
8.1.54 stp vlan enable 8-67
8.1.55 vlan-mapping modulo 8-68

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*: 装置のスロット番号を指定します。これは 1 に固定されています。

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）
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）

フィールド	説明
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*: 装置のスロット番号を指定します。これは 1 に固定されています。

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 のスロット番号 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 のスロット番号 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。
Port priority	スペースで区切られたルートブリッジID、ルートパスコスト、指定ブリッジID、および指定ポートIDによって形成されるポートプライオリティです。
Designated priority	スペースで区切られたルートブリッジID、ルートパスコスト、指定ブリッジID、および指定ポートIDによって形成される指定優先順位です。

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*: 装置のスロット番号を指定します。これは 1 に固定されています。

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 のスロット番号 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 のスロット番号 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。
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 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**

8.1.23 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**

8.1.24 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**

8.1.25 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**

8.1.26 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**

8.1.27 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

8.1.28 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**

8.1.29 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

8.1.30 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**

8.1.31 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**

8.1.32 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

8.1.33 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**

8.1.34 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

8.1.35 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**

8.1.36 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

8.1.37 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

8.1.38 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。

8.1.39 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

8.1.40 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 *(セクション 1 はじめに コマンドマニュアルの“装置管理”)*

8.1.41 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]

8.1.42 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

8.1.43 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**

8.1.44 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**

8.1.45 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**

8.1.46 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

8.1.47 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

8.1.48 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

8.1.49 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**

8.1.50 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**

8.1.51 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**

8.1.52 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

8.1.53 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

8.1.54 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**

8.1.55 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 **2-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

```
 Loop detection is enabled.
Loop detection interval is 30 second(s).
Loop is detected on following interfaces:
 Interface                   Action mode     VLANs
 GigabitEthernet1/0/3          None           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。 🕮 **メモ：** **loopback-detection action shutdown**コマンドを設定し、ポートでループが検出されたとき、ポートがシャットダウンします。ポートのシャットダウンによってループ状態が解除されるため、**display loopback-detection**コマンド上に検知ポートは表示されません。“Shutdown”状態が表示されることはありません。

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

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。

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。詳細はセクション 1 *はじめに コマンドマニュアル*の“*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 コマンドはデフォルトに戻します。

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

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。

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。詳細はセクション 1 *はじめに コマンドマニュアル*の“*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

有効

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 **2-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。インタフェース番号を指定せずに **vlan-interface** キーワードを指定すると、コマンドはすべての既存の VLAN インタフェースに関する情報を表示します。

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**－設定されていません。 ● **Configured**－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。**vlan-interface** 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。インタフェース番号を指定せずに **vlan-interface** を指定すると、既存のすべての 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。VLAN 1 の View ではサポートされていません。

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。

デフォルトでは、すべてのアクセスポートは VLAN 1 に属します。したがって、このコマンドを使用してアクセスポートを VLAN 1 に割り当てることはできません。アクセスポートを VLAN 1 に移動するには、アクセスポートで **undo port access vlan** コマンドを実行します。

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   Dot1p     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。

フィールド	説明
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。
Dot1p	MACアドレス-VLANエントリのVLANの802.1pプライオリティです。
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* [**dot1p** *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。

dot1p *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 dot1p 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 dot1p 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

目次

このセクションのページは **2-x-x** です。

11 章 Voice VLAN 11-1
11.1 Voice VLAN 設定コマンド 11-1
11.1.1 display voice-vlan mac-address 11-1
11.1.2 display voice-vlan state 11-2
11.1.3 voice-vlan aging 11-3
11.1.4 voice-vlan enable 11-4
11.1.5 voice-vlan mac-address 11-5
11.1.6 voice-vlan mode auto 11-6
11.1.7 voice-vlan qos 11-7
11.1.8 voice-vlan qos trust 11-8
11.1.9 voice-vlan security enable 11-9

11章 Voice VLAN

11.1 Voice VLAN設定コマンド

11.1.1 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 11-1 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

11.1.2 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 11-2 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**－セキュリティモードです。 • **Normal**－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**

11.1.3 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られた後、voice VLAN は voice VLAN エージングタイマによって制御されます。voice VLAN エージングタイマは、voice VLAN のダイナミック MAC アドレスエントリが期限切れになったときにのみ開始されます。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。

voice VLAN のエージング期間は、voice VLAN エージングタイマとそのダイナミック MAC アドレスエントリのエージングタイマの合計に等しくなります。ダイナミック MAC アドレスエントリのエージングタイマの詳細は、セクション 2 *アクセス オペレーション マニュアルの”MAC アドレステーブル”*を参照してください。

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

11.1.4 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**

11.1.5 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 11-3 に示します。

表 11-3 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 fff-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

11.1.6 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

11.1.7 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

11.1.8 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

11.1.9 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 **2-x-x** です。

12 章 LLDP 12-1
12.1 LLDP 設定コマンド 12-1
12.1.1 display lldp local-information 12-1
12.1.2 display lldp neighbor-information 12-7
12.1.3 display lldp statistics 12-15
12.1.4 display lldp status 12-17
12.1.5 display lldp tlv-config 12-20
12.1.6 lldp admin-status 12-24
12.1.7 lldp check-change-interval 12-25
12.1.8 lldp compliance admin-status cdp 12-26
12.1.9 lldp compliance cdp 12-27
12.1.10 lldp enable 12-28
12.1.11 lldp encapsulation snap 12-29
12.1.12 lldp fast-count 12-30
12.1.13 lldp global enable 12-30
12.1.14 lldp hold-multiplier 12-31
12.1.15 lldp management-address-format string 12-32
12.1.16 lldp notification remote-change enable 12-33
12.1.17 lldp timer notification-interval 12-34
12.1.18 lldp timer reinit-delay 12-35
12.1.19 lldp timer tx-interval 12-36
12.1.20 lldp tlv-enable 12-36

12章 LLDP

12.1 LLDP設定コマンド

12.1.1 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         : 9c06-1b4f-5502
 System name        : QX-S14148GT-4G
System description  :
   Comware Platform Software, Software Version 7.1.070,
   NEC QX-S1116GT-4G-PW
 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.A
 FirmwareRev              : 110
 SoftwareRev              : 7.1.2
 SerialNum                : 219801A1AW9173Q00013
 Manufacturer name         : NEC
 Model name               : QX-S1148GT-4G
 Asset tracking identifier  : Unknown

LLDP local-information of port 48[GigabitEthernet1/0/48]:
 Port ID type       : Interface name
 Port ID           : GigabitEthernet1/0/48
 Port description    : GigabitEthernet1/0/48 Interface
 LLDP agent nearest-bridge management address:
 Management address type          : All802
 Management address              : 9c06-1b4f-555b
 Management address interface type : IfIndex
 Management address interface ID   : Unknown
 Management address OID           : 0
 LLDP agent nearest-nontpmr management address:
 Management address type          : All802
 Management address              : 9c06-1b4f-555b
 Management address interface type : IfIndex
 Management address interface ID   : Unknown
 Management address OID           : 0
 LLDP agent nearest-customer management address:
 Management address type          : All802
 Management address              : 9c06-1b4f-555b
 Management address interface type : IfIndex
 Management address interface ID   : Unknown
 Management address OID           : 0
 Port VLAN ID(PVID)  : 1
 VLAN name of VLAN 1       : VLAN 0001
 Management VLAN ID  : 0
 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        : 10000
Transmit Tw              : 0 us
Receive Tw               : 0 us
Fallback Tw              : 0 us
Echo Transmit Tw          : 0 us
Echo Receive Tw           : 0 us
PoE PSE power source      : Primary
Port PSE priority         : Critical
Port available power value : 0.0 w
```

表 12-1 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。

フィールド	説明
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。
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。

フィールド	説明
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。
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**－クラス0です。 ● **Class 1**－クラス1です。 ● **Class 2**－クラス2です。 ● **Class 3**－クラス3です。 ● **Class 4**－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

フィールド	説明
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。
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。

フィールド	説明
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。

12.1.2 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-S5224GT-4X
System description  :
   Comware Platform Software, Software Version 7.1.070,
   NEC QX-S1116GT-4G-PW
 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-S5224GT-4X       GE1/0/48       5cdd-70b1-81fe  GigabitEthernet1/0/23
```

表 12-2 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。

フィールド	説明
Chassis type	装置IDタイプです。 ● **Chassis component**－装置構成です。 ● **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。 ● **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。
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。

フィールド	説明
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。
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。

フィールド	説明
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。
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

フィールド	説明
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。
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

フィールド	説明
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。
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。

フィールド	説明
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。

12.1.3 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 12-3 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。

12.1.4 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 12-4 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。
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。

フィールド	説明
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。

12.1.5 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
 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
 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
 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 12-5 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。

フィールド	説明
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 TL**V－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。 • **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。
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。

フィールド	説明
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**－ソフトウェアレビジョン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。

12.1.6 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

12.1.7 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

12.1.8 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

12.1.9 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**

12.1.10 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

12.1.11 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

12.1.12 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

12.1.13 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

12.1.14 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

12.1.15 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

12.1.16 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

12.1.17 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

12.1.18 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

12.1.19 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

12.1.20 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* | **interface loopback** *interface-number*] } | **dot1-tlv** { **all** | **port-vlan-id** | **link-aggregation** | **vlan-name** [*vlan-id*] | **management-vid** [*mvlan-id*] } | **dot3-tlv** { **all** | **link-aggregation** | **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* | **interface loopback** *interface-number*] } | **dot1-tlv** { **all** | **port-vlan-id** | **link-aggregation** | **vlan-name** | **management-vid** } | **dot3-tlv** { **all** | **link-aggregation** | **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** } | **dot3-tlv** { **all** | **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** } | **dot3-tlv** { **all** | **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 { **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 { **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
  - 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。

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、ソフトウェアレビジョン、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 VLAN 名と管理 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 **2-x-x** です。

13 章 L2PT 13-1
13.1 L2PT 設定コマンド 13-1
13.1.1 display l2protocol statistics 13-1
13.1.2 l2protocol tunnel dot1q 13-3
13.1.3 l2protocol tunnel-dmac 13-5
13.1.4 reset l2protocol statistics 13-5

13章 L2PT

13.1 L2PT設定コマンド

13.1.1 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 13-1 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。

13.1.2 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** } **tunnel dot1q**

undo l2protocol { **gvrp** | **mvrp** | **pvst** | **stp** | **vtp** } **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

13.1.3 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

13.1.4 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

目次

このセクションのページは **2-x-x** です。

14 章 Private VLAN 14-1
14.1 Private VLAN 設定コマンド 14-1
14.1.1 display private-vlan 14-1
14.1.2 port private-vlan host 14-4
14.1.3 port private-vlan promiscuous 14-5
14.1.4 port private-vlan trunk promiscuous 14-8
14.1.5 port private-vlan trunk secondary 14-11
14.1.6 private-vlan (VLAN interface view) 14-15
14.1.7 private-vlan (VLAN view) 14-17
14.1.8 private-vlan isolated 14-18
14.1.9 private-vlan primary 14-20

14章 Private VLAN

14.1 Private VLAN設定コマンド

14.1.1 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 14-1 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**

14.1.2 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**

14.1.3 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**

14.1.4 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。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

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**

14.1.5 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**

14.1.6 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**

14.1.7 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。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 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**

14.1.8 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**

14.1.9 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**

QX-S1100G シリーズ Ethernet スイッチ

コマンドマニュアル

3. 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-IP アドレス

04-DHCP

05-DHCP サーバ

06-DHCP クライアント

07-DHCP スヌーピング

08-BOOTP クライアント

09-DNS

10-IP フォワーディングの基本

11-IP パフォーマンスの最適化

12-UDP ヘルパー

13-IPv6 の基本

14-Proxy ARP

15-DHCPv6

16-DHCPv6 クライアント

17-ARP snooping

目次

このセクションのページは **3-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 1-4
1.1.5 arp static 1-5
1.1.6 arp timer aging 1-6
1.1.7 display arp 1-8
1.1.8 display arp *ip-address* 1-11
1.1.9 display arp timer aging 1-12
1.1.10 reset arp 1-12

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 アドレスではありません。
- 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 の詳細はセクション 10 *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。

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

関連コマンド

display mac-address (*セクション 2 アクセス コマンドマニュアル*)

1.1.4 arp max-learning-num

Syntax

arp max-learning-num *number*

undo arp max-learning-num

デフォルト

256

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 0～256 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 static

Syntax

arp static *ip-address mac-address* [*vlan-id interface-type interface-number*]

undo arp *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: 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。

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。

- 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**

1.1.6 arp timer aging

Syntax

arp timer aging *aging-time*

undo arp timer aging

デフォルト

20 分

View

System view

VLAN interface 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。

system view または interface view で、ダイナミック ARP エントリのエージングタイマを設定できます。interface view で設定されたエージングタイマは、system view で設定されたエージングタイマよりも優先されます。

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

#VLAN インタフェース 2 でダイナミック ARP エントリのエージングタイマを 200 秒に設定します。

<Switch> system-view

[Switch] interface vlan-interface 2

[Switch-Vlan-interface2] arp timer aging second 200

関連コマンド

display arp timer aging

1.1.7 display arp

Syntax

display arp [[**all** | **dynamic** | **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。

static: スタティック ARP エントリを表示します。

slot *slot-number*: 装置のスロット番号を指定します。これは 1 に固定されています。

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    VLAN/VSI   Interface             Aging Type
1.1.1.1         02e0-f102-0023 1          GE1/0/1               --    S
1.1.1.2         f474-8800-0001 12         GE1/0/2               960   D
1.1.1.4         00e0-fe60-5000 0          --                    --    M
```

すべての ARP エントリの詳細情報を表示します。

```
IP address        : 1.1.1.1          MAC address    : 02e0-f102-0023
Type             : Static           Aging         : --
Interface         : GE1/0/1          VLAN          : 1
VPN instance       : --
Link ID           : --
Service instance    : 1
VXLAN ID          : --
VSI name          : --
VSI interface      : --
Nickname          : --

IP address        : 1.1.1.2          MAC address    : 0015-e944-adc5
Type             : Dynamic          Aging         : 960 sec
Interface         : GE1/0/2          VLAN          : 12
VPN instance       : --
Link ID           : --
Service instance    : --
VXLAN ID          : --
VSI name          : --
VSI interface      : --
Nickname          : --

IP address        : 1.1.1.4              MAC address    : 00e0-fe60-5000
Type             : Multiport            Aging         : --
Interface         : --                   VLAN          : --
VPN instance       : --
Link ID           : --
Service instance    : --
VXLAN ID          : --
VSI name          : --
VSI interface      : --
Nickname          : --
```

-# 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 : 3
```

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
VLAN/VSI	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、ハイフン（-）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	ARPエントリの出力インタフェースです。以下のどちらかの状態である場合、ハイフン（-）と表示されます。 ● ARPエントリは、未解決のショートスタティックARPエントリです。 ● ARPエントリはマルチポートARPエントリであり、出力インタフェース情報はありません。 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。
Link ID	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。 ARPエントリのリンクIDです。ARPエントリがVSIに属していない場合、このフィールドにはハイフン（-）が表示されます。
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。 ● **O**—OpenFlow.（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） ● **I**–無効なARPエントリです。.
VPN Instance	VPNインスタンス名です。ARPエントリにVPNインスタンスが設定されていない場合、ハイフン（-）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。

フィールド	説明
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**

1.1.8 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*: 装置のスロット番号を指定します。これは 1 に固定されています。
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    VLAN/VSI   Interface             Aging Type
20.1.1.1        f474-8800-0001 --         --                    --    S
```

関連コマンド

- **arp static**
- **reset arp**

1.1.9 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

1.1.10 reset arp

Syntax

reset arp { **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 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。

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*: 装置のスロット番号を指定します。これは 1 に固定されています。
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 **3-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-learning enable 2-3
2.1.4 gratuitous-arp-sending enable 2-4

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とき、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、設定した値よりも長くなります。

- 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-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

2.1.4 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 **3-x-x** です。

3 章 IP アドレス 3-1
3.1 IP アドレス設定コマンド 3-1
3.1.1 display ip interface 3-1
3.1.2 display ip interface brief 3-4
3.1.3 ip address 3-6

3章 IP アドレス

3.1 IPアドレス設定コマンド

3.1.1 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 3-1 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。
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。）
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**

3.1.2 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...
```

#完全なインタフェースの説明を含む、VLAN インタフェースの簡単な IP 設定を表示します。

<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 3-2 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。
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インスタンス名です。最大12文字です。VPNインスタンス名が12文字より長い場合、最初の9文字が表示され、省略記号（...）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、ハイフン（--）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。

フィールド	説明
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、省略記号（...）が続きます。説明が設定されていない場合、ハイフン（--）と表示されます。

関連コマンド

- **display ip interface**
- **ip address**

3.1.3 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。インタフェースで異なるプライマリ IP アドレスを指定するためにこのコマンドを複数回実行すると、最新の構成が有効になります。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**

目次

このセクションのページは **3-x-x** です。

4 章 DHCP 4-1
4.1 DHCP 設定コマンド 4-1
4.1.1 dhcp dscp 4-1
4.1.2 dhcp enable 4-2
4.1.3 dhcp select 4-2

4章 DHCP

4.1 DHCP設定コマンド

4.1.1 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

4.1.2 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

4.1.3 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 **3-x-x** です。

5 章 DHCP サーバ 5-1
5.1 DHCP サーバ設定コマンド 5-1
5.1.1 address range 5-1
5.1.2 bims-server 5-2
5.1.3 bootfile-name 5-3
5.1.4 class option-group 5-4
5.1.5 dhcp class 5-5
5.1.6 dhcp option group 5-6
5.1.7 dhcp server apply ip-pool 5-7
5.1.8 dhcp server forbidden-ip 5-8
5.1.9 dhcp server ip-pool 5-9
5.1.10 dhcp server ping packets 5-10
5.1.11 dhcp server ping timeout 5-11
5.1.12 dhcp server relay information enable 5-12
5.1.13 display dhcp server conflict 5-13
5.1.14 display dhcp server expired 5-14
5.1.15 display dhcp server free-ip 5-15
5.1.16 display dhcp server ip-in-use 5-17
5.1.17 display dhcp server pool 5-18
5.1.18 display dhcp server statistics 5-21
5.1.19 dns-list 5-23
5.1.20 domain-name 5-24
5.1.21 expired 5-25
5.1.22 forbidden-ip 5-26
5.1.23 gateway-list 5-27
5.1.24 if-match 5-28
5.1.25 nbns-list 5-31
5.1.26 netbios-type 5-32
5.1.27 network 5-33
5.1.28 next-server 5-34
5.1.29 option 5-35
5.1.30 reset dhcp server conflict 5-37
5.1.31 reset dhcp server expired 5-37
5.1.32 reset dhcp server ip-in-use 5-38
5.1.33 reset dhcp server statistics 5-39
5.1.34 static-bind 5-39

5.1.35 tftp-server domain-name 5-41
5.1.36 tftp-server ip-address 5-42
5.1.37 voice-config 5-43

5章 DHCP サーバ

5.1 DHCPサーバ設定コマンド

5.1.1 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**

5.1.2 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

5.1.3 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**

5.1.4 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

5.1.5 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**

5.1.6 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**

5.1.7 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

5.1.8 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**

5.1.9 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**

5.1.10 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**

5.1.11 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**

5.1.12 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

5.1.13 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 5-1 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

5.1.14 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 5-2 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

5.1.15 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 5-3 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**

5.1.16 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 5-4 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

5.1.17 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 day 1 hour 2 minute 3 second 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 day 1 hour 0 minute 0 second 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 day 1 hour 0 minute 0 second 0

Pool name: 3
  static bindings:
    ip-address 10.10.1.2 mask 255.0.0.0
      hardware-address 3080-9bfc-0001 ethernet
    ip-address 10.10.1.3 mask 255.0.0.0
      client-identifier aaaa-bbbb
  expired unlimited
```

表 5-5 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。

5.1.18 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 5-6 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

5.1.19 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

5.1.20 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

5.1.21 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**

5.1.22 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**

5.1.23 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

5.1.24 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

5.1.25 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**

5.1.26 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**

5.1.27 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**

5.1.28 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

5.1.29 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

5.1.30 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

5.1.31 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

5.1.32 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

5.1.33 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

5.1.34 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

5.1.35 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**

5.1.36 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**

5.1.37 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 **3-x-x** です。

6 章 DHCP クライアント 6-1
6.1 DHCP クライアント設定コマンド..... 6-1
6.1.1 dhcp client dad enable 6-1
6.1.2 dhcp client dscp..... 6-1
6.1.3 display dhcp client..... 6-2
6.1.4 ip address dhcp-alloc 6-5

6章 DHCP クライアント

6.1 DHCPクライアント設定コマンド

6.1.1 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

6.1.2 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

6.1.3 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 6-1 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

- **ip address dhcp-alloc**

6.1.4 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 **3-x-x** です。

7 章 DHCP スヌーピング 7-1
7.1 DHCP snooping 設定コマンド 7-1
7.1.1 dhcp snooping binding record 7-1
7.1.2 dhcp snooping enable 7-2
7.1.3 dhcp snooping information circuit-id 7-2
7.1.4 dhcp snooping information enable 7-4
7.1.5 dhcp snooping information remote-id 7-5
7.1.6 dhcp snooping information strategy 7-7
7.1.7 dhcp snooping trust 7-8
7.1.8 display dhcp snooping binding 7-9
7.1.9 display dhcp snooping information 7-10
7.1.10 display dhcp snooping packet statistics 7-13
7.1.11 display dhcp snooping trust 7-13
7.1.12 reset dhcp snooping binding 7-14
7.1.13 reset dhcp snooping packet statistics 7-15

7章 DHCP スヌーピング

7.1 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。

7.1.1 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

7.1.2 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

7.1.3 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: 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。装置名を設定するときに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 7-1 に異なるモードのパディング形式を示します。

表 7-1 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。	―	―
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**

7.1.4 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**

7.1.5 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**

7.1.6 dhcp snooping information strategy

Syntax

dhcp snooping information strategy { **append** | **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

append: DHCP メッセージを次のように処理します。

- DHCP メッセージに Option 82 が含まれていない場合、装置はパディング設定に従って Option 82 を追加した後にメッセージを転送します。
- DHCP メッセージにオプション 82 が含まれている場合、装置は次のようにメッセージを処理します。
- ベンダ固有のサブオプションに **dhcp snooping information vendor-specific** コマンドで指定されたコンテンツをパディングした後、メッセージを転送します。
- **dhcp snooping information vendor-specific** コマンドが設定されていない場合、オプション 82 を変更せずにメッセージを転送します。

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。DHCP メッセージにオプション 82 が含まれていない場合、装置は、DHCP メッセージを転送する前に、パディング構成に従ってオプション 82 を追加します。

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**

7.1.7 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

7.1.8 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 7-2 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**

7.1.9 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 7-3 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。

フィールド	説明
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。
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。 ● ベンダ固有の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。 ● リモート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。 ● ベンダ固有のサブオプションの場合、ノード識別子は**MAC**、**Sysname**、または**User Defined**（**string**）です。括弧内の文字列はユーザ定義の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	circuit IDサブオプションの内容です。
Vendor-specific	ベンダ固有のサブオプションの内容です。 このフィールドは、ベンダ固有の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とremote IDおよび、ベンダ固有のサブオプションのパディングです。

7.1.10 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*: 装置のスロット番号を指定します。これは 1 に固定されています。

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

7.1.11 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

```
Interface                          Trusted  VLAN
============================       =======  ================
GE1/0/1                            Trusted  -
GE1/0/2                            -        100

VSI name                           Tunnel trusted
============================       ==============
a                                  Trusted

AC                                 Trusted
============================       ============
GE1/0/1 srv 1                      Trusted
```

関連コマンド

dhcp snooping trust

7.1.12 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

7.1.13 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*: 装置のスロット番号を指定します。これは 1 に固定されています。

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 **3-x-x** です。

8 章 BOOTP クライアント 8-1
8.1 BOOTP クライアント設定コマンド 8-1
8.1.1 display bootp client 8-1
8.1.2 ip address bootp-alloc 8-2

8章 BOOTP クライアント

8.1 BOOTPクライアント設定コマンド

8.1.1 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 8-1 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

8.1.2 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 **3-x-x** です。

9 章 DNS 9-1
9.1 DNS 設定コマンド 9-1
9.1.1 display dns domain 9-1
9.1.2 display dns host 9-2
9.1.3 display dns server 9-3
9.1.4 display ipv6 dns server 9-5
9.1.5 dns domain 9-6
9.1.6 dns dscp 9-7
9.1.7 dns proxy enable 9-7
9.1.8 dns server 9-8
9.1.9 ip host 9-9
9.1.10 ipv6 dns server 9-10
9.1.11 ipv6 host 9-11
9.1.12 reset dns host 9-12

9章 DNS

9.1 DNS設定コマンド

9.1.1 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 9-1 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

9.1.2 display dns host

Syntax

display dns host [**ip** | **ipv6**]

View

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 9-2 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**

9.1.3 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 9-3 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

9.1.4 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 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 9-4 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

9.1.5 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

9.1.6 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

9.1.7 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

9.1.8 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

9.1.9 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セクション 10 *システム管理* コマンドマニュアルの”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

9.1.10 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に最大 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

9.1.11 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セクション 10 *システム管理 コマンドマニュアルの”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

9.1.12 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 **3-x-x** です。

10 章 IP フォワーディングの基本 10-1
10.1 IP フォワーディングの基本設定コマンド 10-1
10.1.1 display fib 10-1

10章 IP フォワーディングの基本

10.1 IPフォワーディングの基本設定コマンド

10.1.1 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 10-1 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 **3-x-x** です。

11 章 IP パフォーマンスの最適化 11-1
11.1 IP パフォーマンスの最適化設定コマンド 11-1
11.1.1 display icmp statistics 11-1
11.1.2 display ip statistics 11-2
11.1.3 display rawip 11-4
11.1.4 display rawip verbose 11-5
11.1.5 display tcp 11-8
11.1.6 display tcp statistics 11-9
11.1.7 display tcp verbose 11-12
11.1.8 display udp 11-17
11.1.9 display udp statistics 11-18
11.1.10 display udp verbose 11-18
11.1.11 ip forward-broadcast 11-22
11.1.12 ip icmp error-interval 11-23
11.1.13 ip mtu 11-24
11.1.14 ip redirects enable 11-25
11.1.15 ip ttl-expires enable 11-26
11.1.16 ip unreachables enable 11-27
11.1.17 reset ip statistics 11-28
11.1.18 reset tcp statistics 11-29
11.1.19 reset udp statistics 11-30
11.1.20 tcp path-mtu-discovery 11-30
11.1.21 tcp timer fin-timeout 11-31
11.1.22 tcp timer syn-timeout 11-32
11.1.23 tcp window 11-33

11章 IP パフォーマンスの最適化

11.1 IPパフォーマンスの最適化設定コマンド

11.1.1 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*: 装置のスロット番号を指定します。これは 1 に固定されています。

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
```

11.1.2 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*: 装置のスロット番号を指定します。これは 1 に固定されています。。

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 11-1 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**

11.1.3 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*: 装置のスロット番号を指定します。これは 1 に固定されています。

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 11-2 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。

11.1.4 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*: 装置のスロット番号を指定します。これは 1 に固定されています。。

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

 Connection info: src = 0.0.0.0, dst = 0.0.0.0
 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
 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 11-3 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。
Connection info	送信元IPアドレスと宛先IPアドレスを含む接続情報です。
Location	ソケットの場所です。 このフィールドは、集中型装置では使用できません。
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/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。
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。

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_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。

11.1.5 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*: 装置のスロット番号を指定します。これは 1 に固定されています。

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 11-4 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。

11.1.6 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*: 装置のスロット番号を指定します。これは 1 に固定されています。

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

11.1.7 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*: 装置のスロット番号を指定します。これは 1 に固定されています。

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)

 Connection info: src = 192.168.20.200:179 ,  dst = 192.168.20.14:4181
 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
 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 11-5 コマンド出力

フィールド	説明
TCP inpcb number	TCP IP PCBの数です。
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 宛先ポート番号などの接続情報です。
Location	ソケットの場所です。 このフィールドは、集中型装置では使用できません
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。

フィールド	説明
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。

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。

11.1.8 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*: 装置のスロット番号を指定します。これは 1 に固定されています。

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 11-6 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。
PCB	PCBインデックスです。

11.1.9 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*: 装置のスロット番号を指定します。これは 1 に固定されています。。

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

11.1.10 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*: 装置のスロット番号を指定します。これは 1 に固定されています。

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


 Connection info: src = 0.0.0.0:69, dst = 0.0.0.0:0
 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
 Inpcb flags: N/A
 Inpcb extflag: N/A
 Inpcb vflag: INP_IPV4
 TTL: 255(minimum TTL: 0)
 Send VRF: 0xffff
 Receive VRF: 0xffff
```

表 11-7 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。
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、宛先ポート番号などの接続情報です。
Location	ソケットの場所です。 このフィールドは、集中型装置では使用できません。
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/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。

11.1.11 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

11.1.12 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

11.1.13 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 で IPv4 パケットの 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

11.1.14 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

11.1.15 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

11.1.16 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

11.1.17 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*: 装置のスロット番号を指定します。これは 1 に固定されています。

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**

11.1.18 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

11.1.19 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

11.1.20 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

11.1.21 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

11.1.22 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

11.1.23 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 **3-x-x** です。

12 章 UDP ヘルパー 12-1
12.1 UDP ヘルパー設定コマンド 12-1
12.1.1 display udp-helper interface 12-1
12.1.2 reset udp-helper statistics 12-2
12.1.3 udp-helper enable 12-2
12.1.4 udp-helper port 12-3
12.1.5 udp-helper server 12-4

12章 UDP ヘルパー

12.1 UDPヘルパー設定コマンド

12.1.1 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
```

表 12-1 コマンド出力

フィールド	説明
Interface	インタフェース名です。
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。

フィールド	説明
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**

12.1.2 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

12.1.3 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**

12.1.4 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

12.1.5 udp-helper server

Syntax

udp-helper server *ip-address*

undo udp-helper server [*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: 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。

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

関連コマンド

display udp-helper interface

目次

このセクションのページは **3-x-x** です。

13 章 IPv6 の基本 13-1
13.1 IPv6 の基本設定コマンド 13-1
13.1.1 display ipv6 fib 13-1
13.1.2 display ipv6 interface 13-2
13.1.3 display ipv6 neighbors 13-8
13.1.4 display ipv6 neighbors count 13-11
13.1.5 display ipv6 pathmtu 13-12
13.1.6 display ipv6 rawip 13-13
13.1.7 display ipv6 rawip verbose 13-14
13.1.8 display ipv6 statistics 13-20
13.1.9 display ipv6 tcp 13-22
13.1.10 display ipv6 tcp verbose 13-23
13.1.11 display ipv6 udp 13-31
13.1.12 display ipv6 udp verbose 13-32
13.1.13 ipv6 address 13-38
13.1.14 ipv6 address anycast 13-39
13.1.15 ipv6 address auto 13-40
13.1.16 ipv6 address auto link-local 13-41
13.1.17 ipv6 address eui-64 13-43
13.1.18 ipv6 address link-local 13-44
13.1.19 ipv6 hop-limit 13-45
13.1.20 ipv6 hoplimit-expires enable 13-46
13.1.21 ipv6 icmpv6 error-interval 13-47
13.1.22 ipv6 icmpv6 multicast-echo-reply enable 13-48
13.1.23 ipv6 mtu 13-49
13.1.24 ipv6 nd autoconfig managed-address-flag 13-49
13.1.25 ipv6 nd autoconfig other-flag 13-50
13.1.26 ipv6 nd dad attempts 13-51
13.1.27 ipv6 nd ns retrans-timer 13-52
13.1.28 ipv6 nd nud reachable-time 13-53
13.1.29 ipv6 nd ra halt 13-54
13.1.30 ipv6 nd ra interval 13-55
13.1.31 ipv6 nd ra prefix 13-56
13.1.32 ipv6 nd ra router-lifetime 13-57
13.1.33 ipv6 neighbor 13-58
13.1.34 ipv6 neighbor stale-aging 13-60

13.1.35 ipv6 neighbors max-learning-num 13-61
13.1.36 ipv6 pathmtu 13-62
13.1.37 ipv6 pathmtu age 13-63
13.1.38 ipv6 unreachables enable 13-64
13.1.39 reset ipv6 neighbors 13-64
13.1.40 reset ipv6 pathmtu 13-65
13.1.41 reset ipv6 statistics 13-66

13章 IPv6 の基本

13.1 IPv6の基本設定コマンド

13.1.1 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

#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 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	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。

13.1.2 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:FE65:4322/64 [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 13-2 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 13-3 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。

13.1.3 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: 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*: 装置のスロット番号を指定します。これは 1 に固定されています。

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    IS-Invalid static
IPv6 address              MAC address    VID  Interface         State T  Aging
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
1::4                   6864-6839-0204 1    GE1/0/2           STALE D  136
```

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

```
IPv6 Address     : 1::2
MAC address      : 6864-6839-0202          Type  : Dynamic
State            : STALE                   Aging : 136   seconds
Interface        : GE1/0/1                 VID   : 1
VPN instance     : --
Service instance: --
Link ID          : --
Nickname         : 0x0

IPv6 Address     : FE80::6A64:68FF:FE39:202
MAC address      : 6864-6839-0202          Type  : Dynamic
State            : STALE                   Aging : 126   seconds
Interface        : GE1/0/1                 VID   : 1
VPN instance     : --
Service instance: --
Link ID          : --
Nickname         : 0x0


IPv6 Address     : 1::4
MAC address      : 6864-6839-0204          Type  : Dynamic
State            : STALE                   Aging : 136   seconds
```

```
Interface       : GE1/0/2                   VID   : 1
VPN instance    : --
Service instance: 1
Link ID         : 0x1
Nickname        : 0x0
```

表 13-4 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。
MAC address	ネイバの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。
Interface	ネイバに接続しているインタフェースです。 インタフェース名またはリンクIDが利用できない場合、フィールドには**N/A**が表示されます。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。装置は遅延期間中にNSメッセージを送信しません。 • **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。 • **Static** –スタティックに設定されました。 • **Dynamic**–ダイナミックに取得されました。 • **Openflow**–OpenFlowモジュールから学習しました（サポートされていません）。 • **Rule**–PoEあるいはPortalモジュールから学習しました。 • **Invalid static**–無効です。

フィールド	説明
Aging	ネイバの到達可能時間です。 • 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インスタンスの名前です。 VPNインスタンスが構成されていない場合、このフィールドには（-）が表示されます。 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されていません。
Service instance	Ethernetサービスインスタンスです。 ネイバエントリが関連するレイヤ2 Ethernetインタフェースまたはレイヤ2アグリゲートインタフェースのEthernetサービスインスタンスに属していない場合、このフィールドには（-）が表示されます。 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されていません。
Link ID	ネイバに接続するリンクのIDです。 リンクIDは、最大8つの16進数の文字列です。ネイバエントリがVSIに属していない場合、フィールドには（-）が表示されます。 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されていません
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**

13.1.4 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*: 装置のスロット番号を指定します。これは 1 に固定されています。

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
```

13.1.5 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: 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 13-5 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**

13.1.6 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*: 装置のスロット番号を指定します。これは 1 に固定されています。

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 13-6 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。

13.1.7 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*: 装置のスロット番号を指定します。これは 1 に固定されています。

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

Connection info: src = ::, dst = ::
 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
 Inpcb flags: N/A
 Inpcb extflag: INP_EXTRCVICMPERR INP_EXTFILTER
 Inpcb vflag: INP_IPV6
 Hop limit: 255 (minimum hop limit: 0)
 Send VRF: 0xffff
```

表 13-7 Receive VRF: 0xffff 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。
Connection info	送信元および宛先IPv6アドレスを含む接続情報です。
Location	ソケットの場所です
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。

フィールド	説明
State	ソケットの状態です。 • **NOFDREF**—ユーザは接続を閉じました。 • **ISCONNECTED**—接続が確立されました。 • **ISCONNECTING**—接続が確立されています。 • **ISDISCONNECTING**—接続が中断されています。 • **ASYNC**—非同期モードです。 • **ISDISCONNECTED**—接続は終了しました。. • **PROTOREF**—強力なプロトコルリファレンスを示します。 • **N/A**—上記の状態のいずれでもありません。

フィールド	説明
Options	ソケットのオプションです。 • **SO_DEBUG**—ソケットのデバッグ情報を記録します。 • **SO_ACCEPTCONN**—サーバが接続要求をリッスンできるようにします。 • **SO_REUSEADDR**—ローカルアドレスの再利用を許可します。 • **SO_KEEPALIV**E—接続がまだ有効かどうかをテストするプロトコルが必要です。 • **SO_DONTROUTE**—宛先が直接接続されたネットワークにあるため、発信パケットのルーティングテーブルクエリをバイパスします。 • **SO_BROADCAS**T—ブロードキャストパケットをサポートします。 • **SO_LINGER**—ソケットを閉じます。システムは、ソケット送信バッファ内の残りのデータを送信できます。 • **SO_OOBINLINE**—帯域外データを入力キューに保存します。 • **SO_REUSEPORT**—ローカルポートの再利用を許可します。 • **SO_TIMESTAMP**—ミリ秒単位の正確な受信パケットのタイムスタンプを記録します。このオプションは、接続指向ではないプロトコルに適用できます。 • **SO_NOSIGPIPE**—ソケットによるデータ送信を無効にします。その結果、戻りエラーが発生したときにシグパイプを確立できません。 • **SO_TIMESTAMPNS**—ナノ秒単位の正確なタイムスタンプを持つ同様の関数があります。 • **SO_KEEPALIVETIME**—キープアライブ時間を設定します。このオプションはTCPでサポートされています。 • **SO_FILTER—Supports**パケットフィルタ基準の設定をサポートします。このオプションは、OSI SocketおよびRawIPで使用できます。 • **SO_USCBINDEX**—受信パケットからユーザープロファイルインデックスを取得します。 • **N/A**—オプションは設定されていません。

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	ソケットを使用しているプロトコル番号です。58はICMPを示します。

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RawIP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。 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。
Receive VRF	受信されたインスタンスです。 このフィールドは、現在のソフトウェアバージョンではサポートされていません。

13.1.8 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*: 装置のスロット番号を指定します。これは 1 に固定されています。

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

13.1.9 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*: 装置のスロット番号を指定します。これは 1 に固定されています。

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 13-8 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。

13.1.10 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*: 装置のスロット番号を指定します。これは 1 に固定されています。

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)

Connection info: src = 2001::1->179 ,  dst = 2001::2->4181
 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
 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 13-9 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。
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、宛先ポート番号などの接続情報です。
Location	ソケットの場所です。
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。

フィールド	説明
State	ソケットの状態です。 • **NOFDREF**–ユーザは接続を閉じました。 • **ISCONNECTED**–接続が確立されました。 • **ISCONNECTING**–接続が確立されています。 • **ISDISCONNECTING**–接続が中断されています。 • **ASYNC**–非同期モードです。 • **ISDISCONNECTED**–接続は終了しました。 • **PROTOREF**–強力なプロトコル参照を示します。 • **N/A**–上記の状態のいずれでもありません。

フィールド	説明
Options	ソケットのオプションです。 • **SO_DEBUG**–ソケットのデバッグ情報を記録します。 • **SO_ACCEPTCONN**–サーバが接続要求をリッスンできるようにします。 • **SO_REUSEADDR**–ローカルアドレスの再利用を許可します。. • **SO_KEEPALIVE**–接続がまだ有効かどうかをテストするプロトコルが必要です。 • **SO_DONTROUTE**–宛先が直接接続されたネットワークにあるため、発信パケットのルーティングテーブルクエリをバイパスします。 • **SO_BROADCAST**–ブロードキャストパケットをサポートします。 • **SO_LINGER**–ソケットを閉じます。システムは、ソケット送信バッファ内の残りのデータを送信できます。 • **SO_OOBINLINE**–帯域外データを入力キューに保存します • **SO_REUSEPORT**–ローカルポートの再利用を許可します。 • **SO_TIMESTAMP**–受信パケットのタイムスタンプを正確にミリ秒単位で記録します。このオプションは、接続指向ではないプロトコルに適用できます。 • **SO_NOSIGPIPE**–ソケットによるデータ送信を無効にします。その結果、戻りエラーが発生したときにシグパイプを確立できません • **SO_TIMESTAMPNS**–ナノ秒単位の正確なタイムスタンプを持つ同様の関数があります。. • **SO_KEEPALIVETIME**–キープアライブ時間を設定します。このオプションはTCPでサポートされています。 • **SO_FILTER**–パケットフィルタ基準の設定をサポートします。このオプションは、OSI SocketおよびRawIPで使用できます。 • **SO_USCBINDEX**–受信したパケットからユーザプロファイルインデックスを取得します。 • **N/A**–オプションは設定されていません。.
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。

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RawIP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。 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。
Receive VRF	VRFから受信されたパケットです。 このフィールドは、現在のソフトウェアバージョンではサポートされていません。

13.1.11 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*: 装置のスロット番号を指定します。これは 1 に固定されています。。

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 13-10 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。

13.1.12 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*: 装置のスロット番号を指定します。これは 1 に固定されています。

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
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 13-11 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。
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、宛先ポート番号などの接続情報です。
Location	ソケットの場所です。
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。

フィールド	説明
State	ソケットの状態です。 • **NOFDREF**—ユーザは接続を閉じました。 • **SCONNECTED**—接続が確立されました。 • **SCONNECTING**—接続が確立されています。 • **SDISCONNECTING**—接続が中断されています • **ASYNC**—非同期モードです。 • **ISDISCONNECTED**—接続は終了しました. • **PROTOREF**—強力なプロトコル参照を示します。 • **N/A**—上記の状態のいずれでもありません。

フィールド	説明
Options	ソケットのオプションです。 • **SO_DEBUG**—ソケットのデバッグ情報を記録します。. • **SO_ACCEPTCONN**—サーバが接続要求をリッスンできるようにします。 • **SO_REUSEADDR**—ローカルアドレスの再利用を許可します。. • **SO_KEEPALIVE**—接続がまだ有効かどうかをテストするプロトコルが必要です。. • **SO_DONTROUTE**—宛先が直接接続されたネットワークにあるため、発信パケットのルーティングテーブルクエリをバイパスします。. • **SO_BROADCAST**–ブロードキャストパケットをサポートします。. • **SO_LINGER**—ソケットを閉じます。システムは、ソケット送信バッファ内の残りのデータを送信できます。. • **SO_OOBINLINE** –帯域外データを入力キューに格納します。. • **SO_REUSEPORT** –ローカルポートの再利用を許可します。 • **SO_TIMESTAMP**—ミリ秒単位の正確な入力パケットのタイムスタンプを記録します。このオプションは、接続指向ではないプロトコルに適用できます。 • **SO_NOSIGPIPE**—ソケットによるデータ送信を無効にします。その結果、戻りエラーが発生したときにシグパイプを確立できません。。. • **SO_TIMESTAMPNS**—ナノ秒単位の正確なタイムスタンプを持つ同様の関数があります。. • **SO_KEEPALIVETIME**—パキープアライブ時間を設定します。 このオプションはTCPでサポートされています • **SO_FILTER**—パケットフィルタ基準の設定をサポートします。このオプションは、OSI SocketおよびRawIPで使用できます。. • **SO_USCBINDEX**—受信パケットからユーザプロファイルインデックスを取得します。. • **N/A**—オプションは設定されていません。
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	ソケットを使用したプロトコル数です。17はUDPを示します。

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RawIP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。 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。
Receive VRF	受信されたインスタンスです。 このフィールドは、現在のソフトウェアバージョンではサポートされていません。

13.1.13 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

13.1.14 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

13.1.15 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

13.1.16 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

13.1.17 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。IPv6 アドレスと IPv6 プレフィックス長は、以下の形式をサポートしています。

- *ipv6-address/prefix-length.* 例**:** 2001::1/64.
- *ipv6-address prefix-length*. 例**:** 2001::1 64.

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

13.1.18 ipv6 address link-local

Syntax

ipv6 address *ipv6-address* [*prefix-length*] | *ipv6-address*/*prefix-length* } **link-local**

undo ipv6 address *ipv6-address* [*prefix-length*] | *ipv6-address*/*prefix-length* } **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。

prefix-length: IPv6 プレフィックス長を 1～128 の範囲で指定します.

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。

リンクローカルアドレスを設定する場合、プレフィックスの長さが 10 以上であることを確認してください。そうでない場合、設定は失敗します。

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

#VLAN インタフェース 100 のリンクローカルアドレスを設定し、プレフィックス長を 64 に設定します。

<Switch> system-view

[Switch] interface vlan-interface 100

[Switch -Vlan-interface100] ipv6 address fe80::1 64 link-local

関連コマンド

ipv6 address auto link-local

13.1.19 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

13.1.20 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

13.1.21 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

13.1.22 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

13.1.23 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

13.1.24 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

13.1.25 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

13.1.26 ipv6 nd dad attempts

Syntax

ipv6 nd dad attempts *times*

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

times: 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**

13.1.27 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

13.1.28 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 1200000 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

13.1.29 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

13.1.30 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

13.1.31 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** | **prefix-preference** *level*] *]

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。

prefix-preference *level* : プレフィックス設定を指定します。level は、0～255 の範囲で優先度の値を指定します。値が大きいほど、優先度が高いことを示します。 クライアントは、アドレス生成の優先度が最も高い IPv6 プレフィックスを選択します。 このオプションを指定しない場合、RA メッセージにはプレフィックスの設定が含まれません。

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

13.1.32 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

13.1.33 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**

13.1.34 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。

system view と interface view で、STALE 状態の ND エントリのエージングタイマを設定できます。インタフェースの STALE 状態の ND エントリの場合、interface view のエージングタイマは、system view のエージングタイマよりも優先されます。

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

13.1.35 ipv6 neighbors max-learning-num

Syntax

ipv6 neighbors max-learning-num *max-number*

undo ipv6 neighbors max-learning-num

デフォルト

16384View

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

13.1.36 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**

13.1.37 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

13.1.38 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

13.1.39 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* 装置のスロット番号を指定します。これは 1 に固定されています。

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**

13.1.40 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

13.1.41 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*: 装置のスロット番号を指定します。これは 1 に固定されています。

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 **3-x-x** です。

14 章 Proxy ARP 14-1
14.1 Proxy ARP 設定コマンド 14-1
14.1.1 display local-proxy-arp 14-1
14.1.2 display proxy-arp 14-2
14.1.3 local-proxy-arp enable 14-2
14.1.4 proxy-arp enable 14-4

14章 Proxy ARP

14.1 Proxy ARP設定コマンド

14.1.1 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

14.1.2 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

14.1.3 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

14.1.4 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 **3-x-x** です。

15 章 DHCPv6 15-1
15.1 DHCPv6 設定コマンド 15-1
15.1.1 display ipv6 dhcp duid 15-1
15.1.2 ipv6 dhcp select 15-1

15章 DHCPv6

15.1 DHCPv6設定コマンド

15.1.1 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: 0003000130809bf005552.
```

15.1.2 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

目次

このセクションのページは **3-x-x** です。

16 章 DHCPv6 クライアント 16-1
16.1 DHCPv6 クライアント設定コマンド 16-1
16.1.1 display ipv6 dhcp client 16-1
16.1.2 display ipv6 dhcp client statistics 16-4
16.1.3 ipv6 address dhcp-alloc 16-6
16.1.4 reset ipv6 dhcp client statistics 16-7

16章 DHCPv6 クライアント

16.1 DHCPv6 クライアント設定コマンド

16.1.1 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 16-1 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

16.1.2 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 16-2 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

16.1.3 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

16.1.4 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 **3-x-x** です。

17 章 ARP snooping 17-1
17.1 ARP snooping 設定コマンド 17-1
17.1.1 arp snooping enable 17-1
17.1.2 display arp snooping 17-1
17.1.3 reset arp snooping 17-3

17章 ARP snooping

17.1 ARP snooping設定コマンド

17.1.1 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

17.1.2 display arp snooping

Syntax

display arp snooping vlan [*vlan-id*] [**slot** *slot-number*] [**count**]

display arp snooping vlan 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 の ARP snooping エントリを表示します。

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。このパラメータを指定しない場合、コマンドは ARP snooping エントリを表示します。

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*: 装置のスロット番号を指定します。これは 1 に固定されています。

説明

display arp snooping コマンドは 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
```

#VLAN の IP アドレス 1.1.1.1 の ARP snooping エントリを表示します。

```
<switch> display arp snooping vlan ip 1.1.1.1
IP address     MAC address    VLAN ID Interface  Aging      Status
1.1.1.1        001f-e201-0111 2      GE1/0/1    15         Valid
```

表 17-1 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

17.1.3 reset arp snooping

Syntax

reset arp snooping vlan [*vlan-id*]

reset arp snooping vlan ip *ip-address*

View

User view

定義済みユーザロール

network-admin

パラメータ

vlan：VLAN の ARP snooping エントリを削除します。

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。

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

QX-S1100G シリーズ Ethernet スイッチ

コマンドマニュアル

4. 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-デフォルトルート

目次

このセクションのページは **4-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 display ip routing-table 1-1
1.1.2 display ip routing-table acl 1-5
1.1.3 display ip routing-table ip-address 1-8
1.1.4 display ip routing-table prefix-list 1-10
1.1.5 display ip routing-table protocol 1-11
1.1.6 display ip routing-table statistics 1-13
1.1.7 display ipv6 routing-table 1-14
1.1.8 display ipv6 routing-table acl 1-18
1.1.9 display ipv6 routing-table ipv6-address 1-22
1.1.10 display ipv6 routing-table prefix-list 1-24
1.1.11 display ipv6 routing-table protocol 1-26
1.1.12 display ipv6 routing-table statistics 1-27
1.1.13 reset ip routing-table statistics protocol 1-29
1.1.14 reset ipv6 routing-table statistics protocol 1-29

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 display ip routing-table

Syntax

display ip routing-table [**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: 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内のすべて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

```
VPN instance: public instance
Destinations : 10       Routes : 10

Destination/Mask    Proto  Pre  Cost        NextHop         Interface
0.0.0.0/0         Static 60   0          192.168.47.4    Vlan11
0.0.0.0/32         Direct 0    0          127.0.0.1       InLoop0
127.0.0.0/8        Direct 0    0          127.0.0.1       InLoop0
127.0.0.0/32       Direct 0    0          127.0.0.1       InLoop0
127.0.0.1/32       Direct 0    0          127.0.0.1       InLoop0
127.255.255.255/32  Direct 0    0          127.0.0.1       InLoop0
192.168.1.40/32    Direct 0    0          127.0.0.1       InLoop0
224.0.0.0/4        Direct 0    0          0.0.0.0         NULL0
224.0.0.0/24       Direct 0    0          0.0.0.0         NULL0
```

```
255.255.255.255/32  Direct 0    0          127.0.0.1      InLoop0
```

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。
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: 0.0.0.0/0
   Protocol: Static
 Process ID: 0
  SubProtID: 0x0                 Age: 04h20m37s
       Cost: 0             Preference: 60
      IpPre: N/A           QosLocalID: N/A
        Tag: 0                 State: Active Adv
  OrigTblID: 0x0             OrigVrf: default-vrf
    TableID: 0x2              OrigAs: 0
      NibID: 0x10000003         LastAs: 0
     AttrID: 0xffffffff       Neighbor: 0.0.0.0
      Flags: 0x1008c       OrigNextHop: 192.168.47.4
      Label: NULL          RealNextHop: 192.168.47.4
    BkLabel: NULL            BkNextHop: N/A
    SRLabel: NULL            BkSRLabel: NULL
  Tunnel ID: Invalid          Interface: Vlan-interface11
```

```
BkTunnel ID: Invalid       BkInterface: N/A
   FtnIndex: 0x0          TrafficIndex: N/A
  Connector: 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。
IpPre	IPプレシーデンスです。
QosLocalID	ローカルQoS ID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**—分配できるルートです。 • **Inactive**—非アクティブルートです。 • **NoAdv**—ルータが分配できないルートです。
OrigTblID	もとのルーティングテーブルIDです。
OrigVrf	ルートが所属しているもとのVPNインスタンスです。ルートがパブリックネットワークにある場合、**default-vrf**と表示します。 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。
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。

フィールド	説明
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。
Label	ラベルです。 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。
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。 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。
BkNexthop	バックアップネクストホップです。
SRLabel	セグメントルーティング（SR）ラベルです。
BkSRLabel	バックアップセグメントルーティング（SR）ラベルです。
Tunnel ID	トンネル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。
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。 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。
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。
TrafficIndex	トラフィックのインデックスです。範囲は1～64です。 値が不正である場合、**N/A**と表示されます。
Connector	VPN IPv4ルートとともに、BGPピア間で交換されるBGP接続属性です。値はリモートPE装置のIPアドレスです。BGP接続属性はMD VPNで使用されます。BGP接続属性がサポートされていない場合、**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サポートしていません。

フィールド	説明
Summary Count	ルート数です。

1.1.2 display ip routing-table acl

Syntax

display ip routing-table acl *ipv4-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

ipv4-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 basic 2000

[Switch-acl-ipv4-basic-2000] rule permit source 192.168.1.0 0.0.0.255

[Switch-acl-ipv4-basic-2000] rule deny source any

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

```
Summary count : 4

Destination/Mask    Proto  Pre  Cost        NextHop         Interface
```

```
192.168.1.0/24      Direct 0    0           192.168.1.111   Vlan11
192.168.1.0/32      Direct 0    0           192.168.1.111   Vlan11
192.168.1.111/32    Direct 0    0           127.0.0.1       InLoop0
192.168.1.255/32    Direct 0    0           192.168.1.111   Vlan11
```

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

```
Summary count : 4

Destination: 192.168.1.0/24
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x1                 Age: 04h20m37s
       Cost: 0             Preference: 0
      IpPre: N/A           QosLocalID: N/A
        Tag: 0                 State: Active Adv
  OrigTblID: 0x0             OrigVrf: default-vrf
    TableID: 0x2              OrigAs: 0
      NibID: 0x10000003        LastAs: 0
     AttrID: 0xffffffff       Neighbor: 0.0.0.0
      Flags: 0x10080       OrigNextHop: 192.168.1.111
      Label: NULL         RealNextHop: 192.168.1.111
    BkLabel: NULL           BkNextHop: N/A
    SRLabel: NULL           BkSRLabel: NULL
  Tunnel ID: Invalid         Interface: Vlan-interface11
BkTunnel ID: Invalid       BkInterface: N/A
   FtnIndex: 0x0          TrafficIndex: N/A
  Connector: N/A

Destination: 192.168.1.0/32
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x0                 Age: 04h20m37s
       Cost: 0             Preference: 0
      IpPre: N/A           QosLocalID: N/A
        Tag: 0                 State: Active NoAdv
  OrigTblID: 0x0             OrigVrf: default-vrf
    TableID: 0x2              OrigAs: 0
      NibID: 0x10000003        LastAs: 0
     AttrID: 0xffffffff       Neighbor: 0.0.0.0
      Flags: 0x1008c       OrigNextHop: 192.168.1.111
```

```
     Label: NULL          RealNextHop: 192.168.1.111
   BkLabel: NULL            BkNextHop: N/A
   SRLabel: NULL            BkSRLabel: NULL
 Tunnel ID: Invalid          Interface: Vlan-interface11
BkTunnel ID: Invalid        BkInterface: N/A
  FtnIndex: 0x0           TrafficIndex: N/A
 Connector: N/A

Destination: 192.168.1.111/32
  Protocol: Direct
 Process ID: 0
 SubProtID: 0x1                Age: 04h20m37s
     Cost: 0             Preference: 0
    IpPre: N/A           QosLocalID: N/A
      Tag: 0                State: Active NoAdv
 OrigTblID: 0x0            OrigVrf: default-vrf
   TableID: 0x2             OrigAs: 0
    NibID: 0x10000000        LastAs: 0
   AttrID: 0xffffffff       Neighbor: 0.0.0.0
    Flags: 0x10004       OrigNextHop: 127.0.0.1
    Label: NULL          RealNextHop: 127.0.0.1
   BkLabel: NULL            BkNextHop: N/A
   SRLabel: NULL            BkSRLabel: NULL
 Tunnel ID: Invalid          Interface: InLoopBack0
BkTunnel ID: Invalid        BkInterface: N/A
  FtnIndex: 0x0           TrafficIndex: N/A
 Connector: N/A

Destination: 192.168.1.255/32
  Protocol: Direct
 Process ID: 0
 SubProtID: 0x0                Age: 04h20m37s
     Cost: 0             Preference: 0
    IpPre: N/A           QosLocalID: N/A
      Tag: 0                State: Active NoAdv
 OrigTblID: 0x0            OrigVrf: default-vrf
   TableID: 0x2             OrigAs: 0
    NibID: 0x10000003        LastAs: 0
   AttrID: 0xffffffff       Neighbor: 0.0.0.0
    Flags: 0x1008c       OrigNextHop: 192.168.1.111
    Label: NULL          RealNextHop: 192.168.1.111
   BkLabel: NULL            BkNextHop: N/A
   SRLabel: NULL            BkSRLabel: NULL
```

```
  Tunnel ID: Invalid         Interface: Vlan-interface11
BkTunnel ID: Invalid       BkInterface: N/A
   FtnIndex: 0x0          TrafficIndex: N/A
  Connector: N/A
```

コマンド出力は表 1-2 を参照してください。

1.1.3 display ip routing-table ip-address

Syntax

display ip routing-table *ip-address* [*mask-length* | *mask*] [**longer-match**] [**verbose**]

display ip routing-table *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

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-length: マスク長を指定します。設定範囲は 0～32 です。

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。

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 0.0.0.0 のルートエントリの概要情報を表示します。

<Switch> display ip routing-table 0.0.0.0

```
Summary count : 2

Destination/Mask   Proto   Pre Cost       NextHop         Interface
0.0.0.0/0          Static  60  0          1.1.1.10        Vlan1
0.0.0.0/32         Direct  0   0          127.0.0.1       InLoop0
```

宛先 IP アドレス 0.0.0.0 およびマスク長 0 のルートの概要情報を表示します。

<Switch> display ip routing-table 0.0.0.0 0

```
Summary count : 1
```

```
Destination/Mask   Proto   Pre Cost       NextHop        Interface
0.0.0.0/0         Static  60  0          1.1.1.10       Vlan1
```

1.1.4 display ip routing-table prefix-list

Syntax

display ip routing-table 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

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

```
Summary count : 1

Destination/Mask    Proto  Pre  Cost        NextHop        Interface
1.1.1.0/24         Direct 0    0          1.1.1.2        Vlan11
```

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

```
Summary count : 1

Destination: 1.1.1.0/24
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x1                 Age: 04h20m37s
       Cost: 0             Preference: 0
      IpPre: N/A           QosLocalID: N/A
        Tag: 0                 State: Active Adv
  OrigTblID: 0x0             OrigVrf: default-vrf
    TableID: 0x2              OrigAs: 0
      NibID: 0x10000003        LastAs: 0
     AttrID: 0xffffffff       Neighbor: 0.0.0.0
      Flags: 0x1008c       OrigNextHop: 1.1.1.2
      Label: NULL          RealNextHop: 1.1.1.2
    BkLabel: NULL            BkNextHop: N/A
    SRLabel: NULL            BkSRLabel: NULL
  Tunnel ID: Invalid          Interface: Vlan-interface11
BkTunnel ID: Invalid        BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: 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 protocol

Syntax

display ip routing-table 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

protocol: ルーティングプロトコルを指定します。

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 : 9

Direct Routing table status : <Active>
Summary count : 9

Destination/Mask    Proto  Pre  Cost        NextHop         Interface
0.0.0.0/32          Direct 0    0           127.0.0.1       InLoop0
2.2.2.0/24          Direct 0    0           2.2.2.1         Vlan2
2.2.2.0/32          Direct 0    0           2.2.2.1         Vlan2
2.2.2.2/32          Direct 0    0           127.0.0.1       InLoop0
2.2.2.255/32        Direct 0    0           2.2.2.1         Vlan2
127.0.0.0/8         Direct 0    0           127.0.0.1       InLoop0
127.0.0.0/32        Direct 0    0           127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0           127.0.0.1       InLoop0
127.255.255.255/32  Direct 0    0           127.0.0.1       InLoop0

Direct Routing table status : <Inactive>
Summary count : 0
```

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 : 1

Static Routing table status : <Active>
Summary count : 1

Destination/Mask   Proto   Pre Cost       NextHop         Interface
0.0.0.0/0          Static  60  0          1.1.1.10        Vlan1
```

```
Static Routing table status : <Inactive>
Summary count : 0
```

1.1.6 display ip routing-table statistics

Syntax

display ip routing-table statistics

View

すべての view

定義済みユーザロール

network-admin

network-operator

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。

プロトコルによって指定されたすべてのルート、deleted と記載されたルート、アクティブルート数が含まれます。

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: 13     Active prefixes: 13

Proto     Routes     Active     Added      Deleted
DIRECT    12         12         12         0
STATIC    1          1          1          0
RIP       0          0          0          0
OSPF      0          0          0          0
IS-IS     0          0          0          0
LISP      0          0          0          0
BGP       0          0          0          0
Total     13         13         13         0
```

表 1-3 コマンド出力

フィールド	説明
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。

フィールド	説明
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。

1.1.7 display ipv6 routing-table

Syntax

display ipv6 routing-table [**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: 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内のすべて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 : 2 Routes : 2

Destination: ::1/128                                Protocol  : Direct
NextHop    : ::1                                   Preference: 0
Interface  : InLoop0                                Cost      : 0

Destination: FE80::/10                              Protocol  : Direct
```

```
NextHop    : ::                                  Preference: 0
Interface  : InLoop0                              Cost      : 0
```

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。
Cost	ルートのコストです。
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 ipv6 routing-table verbose

```
Destinations : 6 Routes : 6

Destination: ::1/128
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x0                 Age: 19h23m02s
      Cost: 0             Preference: 0
     IpPre: N/A           QosLocalID: N/A
       Tag: 0                 State: Active NoAdv
  OrigTblID: 0x0             OrigVrf: default-vrf
    TableID: 0xa              OrigAs: 0
      NibID: 0x20000000        LastAs: 0
     AttrID: 0xffffffff       Neighbor: ::
      Flags: 0x10004       OrigNextHop: ::1
      Label: NULL         RealNextHop: ::1
    BkLabel: NULL           BkNextHop: N/A
```

```
  Tunnel ID: Invalid         Interface: InLoopBack0
BkTunnel ID: Invalid       BkInterface: N/A
   FtnIndex: 0x0          TrafficIndex: N/A
  Connector: N/A
    SRLabel: NULL           BkSRLabel: NULL
Destination: 12::/96
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x0                Age: 00h01m47s
       Cost: 0            Preference: 0
      IpPre: N/A          QosLocalID: N/A
        Tag: 0                State: Active Adv
  OrigTblID: 0x0             OrigVrf: default-vrf
    TableID: 0xa              OrigAs: 0
      NibID: 0x20000003        LastAs: 0
     AttrID: 0xffffffff       Neighbor: ::
      Flags: 0x10080       OrigNextHop: ::
      Label: NULL         RealNextHop: ::
    BkLabel: NULL           BkNextHop: N/A
    SRLabel: NULL           BkSRLabel: NULL
  Tunnel ID: Invalid         Interface: Vlan-interface11
BkTunnel ID: Invalid       BkInterface: N/A
   FtnIndex: 0x0          TrafficIndex: N/A
  Connector: N/A               PathID: 0x0
```

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。

フィールド	説明
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**—分配できるルートです。 • **Inactive**—非アクティブルートです。 • **NoAdv**—ルータが分配できないルートです。
OrigTblID	もとのルーティングテーブルIDです。
OrigVrf	ルートが所属しているもとのVPNインスタンスです。ルートがIPv6ブリックネットワークにある場合、**default-vrf**と表示します。 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。
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。
SRLabel	SRラベルです。
BkSRLabel	バックアップSRラベルです。
Tunnel ID	トンネル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
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。 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。
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。
TrafficIndex	トラフィックのインデックスです。範囲は1～64です。 値が不正である場合、**N/A**と表示されます。
Connector	VPN IPv6ルートとともに、BGPピア間で交換されるBGP接続属性です。値はリモートPE装置のIPアドレスです。BGP接続属性はMD VPNで使用されます。BGP接続属性がサポートされていない場合、**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サポートしていません。
Summary Count	ルート数です。

1.1.8 display ipv6 routing-table acl

Syntax

display ipv6 routing-table acl *ipv6-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

ipv6-acl-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

```
Summary count : 6

Destination : ::1/128                          Protocol  : Direct
NextHop     : ::1                             Preference: 0
Interface   : InLoop0                         Cost      : 0

Destination: 12::/96                           Protocol  : Direct
NextHop    : ::                                Preference: 0
Interface  : Vlan11                            Cost      : 0

Destination: 12::1/128                         Protocol  : Direct
NextHop    : ::1                               Preference: 0
Interface  : InLoop0                           Cost      : 0

Destination: FF::11/128                        Protocol  : Direct
NextHop    : 12::2                             Preference: 255
Interface  : Vlan11                            Cost      : 0

Destination: FE80::/10                         Protocol  : Direct
NextHop    : ::                                Preference: 0
Interface  : InLoop0                           Cost      : 0

Destination: FF00::/8                          Protocol  : Direct
NextHop    : ::                                Preference: 0
Interface  : NULL0                             Cost      : 0
```

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

```
Summary count : 5
```

```
Destination: ::1/128
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x0                 Age: 19h29m12s
       Cost: 0             Preference: 0
      IpPre: N/A           QosLocalID: N/A
        Tag: 0                 State: Active NoAdv
  OrigTblID: 0x0             OrigVrf: default-vrf
    TableID: 0xa              OrigAs: 0
      NibID: 0x20000000         LastAs: 0
     AttrID: 0xffffffff       Neighbor: ::
      Flags: 0x10004       OrigNextHop: ::1
      Label: NULL          RealNextHop: ::1
    BkLabel: NULL            BkNextHop: N/A
    SRLabel: NULL            BkSRLabel: NULL
  Tunnel ID: Invalid          Interface: InLoopBack0
BkTunnel ID: Invalid        BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A

Destination: 12::/96
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x0                 Age: 00h07m57s
       Cost: 0             Preference: 0
      IpPre: N/A           QosLocalID: N/A
        Tag: 0                 State: Active Adv
  OrigTblID: 0x0             OrigVrf: default-vrf
    TableID: 0xa              OrigAs: 0
      NibID: 0x20000003         LastAs: 0
     AttrID: 0xffffffff       Neighbor: ::
      Flags: 0x10080       OrigNextHop: ::
      Label: NULL          RealNextHop: ::
    BkLabel: NULL            BkNextHop: N/A
    SRLabel: NULL            BkSRLabel: NULL
  Tunnel ID: Invalid          Interface: Vlan-interface11
BkTunnel ID: Invalid        BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A

Destination: 12::1/128
   Protocol: Direct
 Process ID: 0
```

```
  SubProtID: 0x0                Age: 00h07m55s
       Cost: 0             Preference: 0
      IpPre: N/A           QosLocalID: N/A
        Tag: 0                 State: Active NoAdv
  OrigTblID: 0x0             OrigVrf: default-vrf
    TableID: 0xa              OrigAs: 0
      NibID: 0x20000000        LastAs: 0
     AttrID: 0xffffffff       Neighbor: ::
      Flags: 0x10004       OrigNextHop: ::1
      Label: NULL          RealNextHop: ::1
    BkLabel: NULL            BkNextHop: N/A
    SRLabel: NULL            BkSRLabel: NULL
  Tunnel ID: Invalid          Interface: InLoopBack0
BkTunnel ID: Invalid        BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A

Destination: FE80::/10
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x0                Age: 19h29m12s
       Cost: 0             Preference: 0
      IpPre: N/A           QosLocalID: N/A
        Tag: 0                 State: Active NoAdv
  OrigTblID: 0x0             OrigVrf: default-vrf
    TableID: 0xa              OrigAs: 0
      NibID: 0x20000002        LastAs: 0
     AttrID: 0xffffffff       Neighbor: ::
      Flags: 0x10084       OrigNextHop: ::
      Label: NULL          RealNextHop: ::
    BkLabel: NULL            BkNextHop: N/A
    SRLabel: NULL            BkSRLabel: NULL
  Tunnel ID: Invalid          Interface: InLoopBack0
BkTunnel ID: Invalid        BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A

Destination: FF00::/8
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x0                Age: 19h29m12s
       Cost: 0             Preference: 0
      IpPre: N/A           QosLocalID: N/A
```

```
      Tag: 0                State: Active NoAdv
 OrigTblID: 0x0             OrigVrf: default-vrf
   TableID: 0xa              OrigAs: 0
     NibID: 0x20000001        LastAs: 0
    AttrID: 0xffffffff       Neighbor: ::
     Flags: 0x10014       OrigNextHop: ::
     Label: NULL         RealNextHop: ::
   BkLabel: NULL           BkNextHop: N/A
   SRLabel: NULL           BkSRLabel: NULL
 Tunnel ID: Invalid         Interface: NULL0
BkTunnel ID: Invalid      BkInterface: N/A
  FtnIndex: 0x0         TrafficIndex: N/A
 Connector: N/A
```

コマンド出力は表 1-5 を参照してください。

1.1.9 display ipv6 routing-table ipv6-address

Syntax

display ipv6 routing-table *ipv6-address* [*prefix-length*] [**longer-match**] [**verbose**]

display ipv6 routing-table *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

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 0～128 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 0::0 0 のルートエントリの概要情報を表示します。

<Switch> display ipv6 routing-table 0::0 0

```
Summary count : 1
```

```
Destination: ::/0                                Protocol  : Static
NextHop    : 10::254                             Preference: 60
Interface  : Vlan1                               Cost      : 0
```

宛先 IPv6 アドレス 0::0 0 のルートの詳細情報を表示します。

<Switch> display ipv6 routing-table 0::0 0 verbose

```
Summary count : 1

Destination: ::/0
   Protocol: Static
 Process ID: 0
  SubProtID: 0x1                 Age: 00h08m16s
      Cost: 0             Preference: 60
     IpPre: N/A           QosLocalID: N/A
       Tag: 0                State: Active Adv
  OrigTblID: 0x0             OrigVrf: default-vrf
    TableID: 0xa              OrigAs: 0
      NibID: 0x21000000        LastAs: 0
     AttrID: 0xffffffff       Neighbor: ::
      Flags: 0x10060       OrigNextHop: 10::254
      Label: NULL         RealNextHop: 10::254
    BkLabel: NULL           BkNextHop: N/A
    SRLabel: NULL           BkSRLabel: NULL
  Tunnel ID: Invalid         Interface: Vlan-interface1
BkTunnel ID: Invalid       BkInterface: N/A
   FtnIndex: 0x0          TrafficIndex: N/A
  Connector: N/A               PathID: 0x0
```

コマンド出力は表 1-4 を参照してください。

1.1.10 display ipv6 routing-table prefix-list

Syntax

display ipv6 routing-table 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

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

```
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

```
Summary count : 1

Destination: ::1/128
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x0                 Age: 08h57m19s
      Cost: 0             Preference: 0
     IpPre: N/A           QosLocalID: N/A
       Tag: 0                 State: Active NoAdv
```

```
 OrigTblID: 0x0             OrigVrf: default-vrf
   TableID: 0xa              OrigAs: 0
     NibID: 0x20000000        LastAs: 0
    AttrID: 0xffffffff       Neighbor: ::
     Flags: 0x10004       OrigNextHop: ::1
     Label: NULL         RealNextHop: ::1
   BkLabel: NULL           BkNextHop: N/A
   SRLabel: NULL           BkSRLabel: NULL
 Tunnel ID: Invalid         Interface: InLoopBack0
BkTunnel ID: Invalid       BkInterface: N/A
  FtnIndex: 0x0          TrafficIndex: N/A
 Connector: N/A
```

コマンド出力は表 1-5 を参照してください。

1.1.11 display ipv6 routing-table protocol

Syntax

display ipv6 routing-table 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

protocol: ルーティングプロトコルを指定します。

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

IPv6 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  : InLoop0                                Cost      : 0

Destination: FF00::/8                               Protocol  : Direct
NextHop    : ::                                    Preference: 0
Interface  : NULL0                                  Cost      : 0

Direct Routing table status : <Inactive>
Summary count : 0
```

IPv6 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 : 1

Static Routing table status : <Active>
Summary count : 1

Destination: ::/0                                   Protocol  : Static
NextHop    : 10::254                                Preference: 60
Interface  : Vlan1                                  Cost      : 0

Static Routing table status : <Inactive>
Summary count : 0
```

1.1.12 display ipv6 routing-table statistics

Syntax

display ipv6 routing-table statistics

View

すべての view

定義済みユーザロール

network-admin

network-operator

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。

プロトコルによって指定されたすべてのルート、deleted と記載されたルート、アクティブルート数が含まれます。

例

IPv6 ルートの統計情報を表示します。

<Switch> display ipv6 routing-table statistics

```
Total prefixes: 6      Active prefixes: 6

Proto      Routes      Active      Added       Deleted
DIRECT     5           5           5           0
STATIC     1           1           1           0
RIPng      0           0           0           0
OSPFv3     0           0           0           0
IS-ISv6    0           0           0           0
LISP       0           0           0           0
BGP4+      0           0           0           0
Total      6           6           6           0
```

表 1-6 コマンド出力

フィールド	説明
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。

1.1.13 reset ip routing-table statistics protocol

Syntax

reset ip routing-table statistics protocol { *protocol* | **all** }

View

User view

定義済みユーザロール

network-admin

パラメータ

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。

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

#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

1.1.14 reset ipv6 routing-table statistics protocol

Syntax

reset ipv6 routing-table statistics protocol { *protocol* | **all** }

View

User view

定義済みユーザロール

network-admin

パラメータ

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。

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

#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

目次

このセクションのページは **4-x-x** です。

2 章 デフォルトルート 2-1
2.1 IP ルーティングテーブル設定コマンド 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 2-3
2.2 IPv6 ルーティングテーブル設定コマンド 2-4
2.2.1 delete ipv6 static-routes all 2-4
2.2.2 ipv6 route-static 2-5
2.2.3 ipv6 route-static default-preference 2-6

2章 デフォルトルート

2.1 IPルーティングテーブル設定コマンド

2.1.1 delete static-routes all

Syntax

delete static-routes all

View

System view

定義済みユーザロール

network-admin

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 0.0.0.0 { **0.0.0.0** | **0** } { *interface-type interface-number* [*next-hop-address* [**nexthop-index** *index-string*]] | *next-hop-address* [**nexthop-index** *index-string*] [**permanent**] } [**preference** *preference*] [**description** *text*]

undo ip route-static 0.0.0.0 { **0.0.0.0** | **0** } [*interface-type interface-number* [*next-hop-address*] | *next-hop-address*] [**preference** preference]

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-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。詳細はセクション 4 *ルーティングプロトコル オペレーションマニュアル*を参照してください。

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。詳細はセクション 5 *ルーティングプロトコル オペレーションマニュアル*の“*スタティックルーティング*”を参照してください。

nexthop-index *index-string*: ネクストホップのインデックスを指定します。*index-string* はインデックスを表します。これは、1～93 文字の大文字と小文字を区別しない文字列です。ネクストホップのインデックスを指定しない場合、スタティックルートは、ネクストホップインデックスとしてネクストホップの出力インタフェースと IP アドレスを使用します。同じ宛先へのルートに同じネクストホップインデックスを指定しないでください。

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。

preference *preference*: 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。

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。

QX-S1100G シリーズは宛先アドレスとマスクの両方を 0.0.0.0（あるいは 0）で指定するデフォルトルートのみサポートします。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。

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ポイント-ポイントインタフェースである場合、出力インタフェースのみを指定することができます。対向先のアドレスが変更してもルートの設定を変更する必要がありません。
- 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、装置はネクストホップの MAC アドレスを取得するため、ネクストホップの IP アドレスを使用します。そのため、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。

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*

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: 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を再設定した場合、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

2.2 IPv6ルーティングテーブル設定コマンド

2.2.1 delete ipv6 static-routes all

Syntax

delete ipv6 static-routes all

View

System view

定義済みユーザロール

network-admin

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

2.2.2 ipv6 route-static

Syntax

ipv6 route-static 0:0::0:0 0 { *interface-type interface-number* [*next-hop-address*] [**permanent**] } [**preference** *preference*] [**description** *text*]

undo ipv6 route-static 0:0::0:0 0 [*interface-type interface-number* [*next-hop-address*] | *next-hop-address*] [**preference** *preference*]

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。

next-hop-address: ネクストホップの IPv6 アドレスを指定します。

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。

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。

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。

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。

QX-S1100G シリーズは宛先アドレスを::/0（あるいはプレフィックス長が 0）で指定する IPv6 デフォルトルートのみサポートします。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、ネクストホップアドレス、あるいは両方を指定するとき、以下のガイドラインに従ってください。

関連コマンド

display ipv6 routing-table protocol

2.2.3 ipv6 route-static default-preference

Syntax

ipv6 route-static default-preference *default-preference*

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: 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

QX-S1100G シリーズ Ethernet スイッチ

コマンドマニュアル

5. 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- MLD スヌーピング

目次

このセクションのページは **5-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 1-5
1.1.4 display igmp-snooping static-group 1-7
1.1.5 display igmp-snooping static-router-port 1-8
1.1.6 display igmp-snooping statistics 1-9
1.1.7 display l2-multicast ip forwarding 1-11
1.1.8 display l2-multicast mac forwarding 1-12
1.1.9 display mac-address multicast 1-13
1.1.10 dot1p-priority (IGMP-snooping view) 1-15
1.1.11 entry-limit (IGMP-snooping view) 1-16
1.1.12 fast-leave (IGMP-snooping view) 1-16
1.1.13 group-policy (IGMP-snooping view) 1-17
1.1.14 host-aging-time (IGMP-snooping view) 1-19
1.1.15 igmp-snooping 1-20
1.1.16 igmp-snooping dot1p-priority 1-21
1.1.17 igmp-snooping drop-unknown 1-22
1.1.18 igmp-snooping enable 1-23
1.1.19 igmp-snooping fast-leave 1-24
1.1.20 igmp-snooping general-query source-ip 1-25
1.1.21 igmp-snooping group-limit 1-26
1.1.22 igmp-snooping group-policy 1-27
1.1.23 igmp-snooping host-aging-time 1-29
1.1.24 igmp-snooping host-join 1-31
1.1.25 igmp-snooping last-member-query-interval 1-32
1.1.26 igmp-snooping leave source-ip 1-33
1.1.27 igmp-snooping max-response-time 1-34
1.1.28 igmp-snooping overflow-replace 1-35
1.1.29 igmp-snooping proxy enable 1-37
1.1.30 igmp-snooping querier 1-37
1.1.31 igmp-snooping query-interval 1-38
1.1.32 igmp-snooping report source-ip 1-39
1.1.33 igmp-snooping router-aging-time 1-40
1.1.34 igmp-snooping source-deny 1-42

1.1.35 igmp-snooping special-query source-ip 1-42
1.1.36 igmp-snooping static-group 1-44
1.1.37 igmp-snooping static-router-port 1-45
1.1.38 igmp-snooping version 1-46
1.1.39 last-member-query-interval (IGMP-snooping view) 1-47
1.1.40 mac-address multicast 1-48
1.1.41 max-response-time (IGMP-snooping view) 1-49
1.1.42 overflow-replace (IGMP-snooping view) 1-50
1.1.43 report-aggregation (IGMP-snooping view) 1-51
1.1.44 reset igmp-snooping group 1-52
1.1.45 reset igmp-snooping router-port 1-53
1.1.46 reset igmp-snooping statistics 1-54
1.1.47 router-aging-time (IGMP-snooping view) 1-54
1.1.48 source-deny (IGMP-snooping view) 1-55

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*: 装置のスロット番号を指定します。これは 1 に固定されています。

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)
(1.1.1.1, 224.1.1.1)
  Attribute: local port
  FSM information: dummy
  Host ports (1 in total):
    GE1/0/2                         (00:04:04)
```

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。
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)	このフィールドはサポートしていません。
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。

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*: 装置のスロット番号を指定します。これは 1 に固定されています。

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)
```

#VLAN 2 のダイナミックルータポートの詳細情報を表示します。

<Switch > display igmp-snooping router-port vlan 2 verbose

```
VLAN 2:
  Router slots (0 in total):
  Router ports (2 in total):
    GE1/0/1                       (00:01:30)
    GE1/0/2                       (00:00:23)
```

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)	このフィールドはサポートしていません。
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。

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*: 装置のスロット番号を指定します。これは 1 に固定されています。

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。
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)	このフィールドはサポートしていません。
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*: スロット番号を指定します。*slot-number* は常に 1 となります。

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。
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 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*: 装置のスロット番号を指定します。これは 1 に固定されています。

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 1-7 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。

1.1.8 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*: 装置のスロット番号を指定します。これは 1 に固定されています。

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 1-8 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。

1.1.9 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 1-9 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

1.1.10 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

1.1.11 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

1.1.12 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

1.1.13 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

1.1.14 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

1.1.15 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 5 *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

1.1.16 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**

1.1.17 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。

IGMP snooping の設定については、セクション 5 *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

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

1.1.18 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。

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

1.1.19 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)

1.1.20 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

1.1.21 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

1.1.22 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)

1.1.23 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**

1.1.24 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

1.1.25 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)**

1.1.26 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

1.1.27 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)**

1.1.28 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)

1.1.29 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。

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

1.1.30 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。

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

1.1.31 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**

1.1.32 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

1.1.33 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)**

1.1.34 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** コ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)

1.1.35 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

1.1.36 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

1.1.37 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

1.1.38 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

1.1.39 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

1.1.40 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

1.1.41 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**

1.1.42 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

1.1.43 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

1.1.44 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

1.1.45 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

1.1.46 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

1.1.47 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

1.1.48 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** コ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 **5-x-x** です。

2 章 MLD スヌーピング 2-1
2.1 MLD スヌーピング設定コマンド 2-1
2.1.1 display ipv6 l2-multicast ip forwarding 2-1
2.1.2 display ipv6 l2-multicast mac forwarding 2-2
2.1.3 display mld-snooping 2-3
2.1.4 display mld-snooping group 2-6
2.1.5 display mld-snooping router-port 2-8
2.1.6 display mld-snooping static-group 2-9
2.1.7 display mld-snooping static-router-port 2-10
2.1.8 display mld-snooping statistics 2-11
2.1.9 dot1p-priority (MLD-snooping view) 2-13
2.1.10 enable (MLD-snooping view) 2-14
2.1.11 entry-limit (MLD-snooping view) 2-15
2.1.12 fast-leave (MLD-snooping view) 2-16
2.1.13 group-policy (MLD-snooping view) 2-17
2.1.14 host-aging-time (MLD-snooping view) 2-18
2.1.15 last-listener-query-interval (MLD-snooping view) 2-19
2.1.16 max-response-time (MLD-snooping view) 2-20
2.1.17 mld-snooping 2-22
2.1.18 mld-snooping done source-ip 2-22
2.1.19 mld-snooping dot1p-priority 2-23
2.1.20 mld-snooping drop-unknown 2-25
2.1.21 mld-snooping enable 2-26
2.1.22 mld-snooping fast-leave 2-27
2.1.23 mld-snooping general-query source-ip 2-28
2.1.24 mld-snooping group-limit 2-29
2.1.25 mld-snooping group-policy 2-30
2.1.26 mld-snooping host-aging-time 2-31
2.1.27 mld-snooping host-join 2-33
2.1.28 mld-snooping last-listener-query-interval 2-34
2.1.29 mld-snooping max-response-time 2-35
2.1.30 mld-snooping overflow-replace 2-37
2.1.31 mld-snooping querier 2-38
2.1.32 mld-snooping query-interval 2-39
2.1.33 mld-snooping report source-ip 2-40
2.1.34 mld-snooping router-aging-time 2-41

2.1.35 mld-snooping source-deny 2-42
2.1.36 mld-snooping special-query source-ip 2-43
2.1.37 mld-snooping static-group 2-44
2.1.38 mld-snooping static-router-port 2-45
2.1.39 mld-snooping version 2-46
2.1.40 overflow-replace (MLD-snooping view) 2-47
2.1.41 report-aggregation (MLD-snooping view) 2-48
2.1.42 reset mld-snooping group 2-49
2.1.43 reset mld-snooping router-port 2-50
2.1.44 reset mld-snooping statistics 2-50
2.1.45 router-aging-time (MLD-snooping view) 2-51
2.1.46 source-deny (MLD-snooping view) 2-52
2.1.47 version (MLD-snooping view) 2-53

2章 MLD スヌーピング

2.1 MLDスヌーピング設定コマンド

2.1.1 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*: 装置のスロット番号を指定します。これは 1 に固定されています。

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 2-1 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。

2.1.2 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*: 装置のスロット番号を指定します。これは 1 に固定されています。

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 2-2 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。

2.1.3 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 2-3 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。
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**－有効です。 ● **Disabled**－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。

フィールド	説明
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**－有効です。 ● **Disabled**－無効です。
Proxy Status of IGMP	MLD snooping proxyの状態です。 ● **Enabled**－有効です。 ● **Disabled**－無効です。

2.1.4 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*: 装置のスロット番号を指定します。これは 1 に固定されています。

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 2 entries.

VLAN 2: Total 2 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 2-4 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。
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)	このフィールドはサポートされていません。
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。

関連コマンド

reset mld-snooping group

2.1.5 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*: 装置のスロット番号を指定します。これは 1 に固定されています

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 2-5 コマンド出力

フィールド	説明
VLAN 2	VLAN IDです。
Router slots (0 in total)	このフィールドはサポートされていません。
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。

関連コマンド

reset mld-snooping router-port

2.1.6 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*: 装置のスロット番号を指定します。これは 1 に固定されています

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 2-6 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。
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。
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)	このフィールドはサポートされていません。
Host ports (1 in total)	メンバポートとメンバポートの総数です。

2.1.7 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*: 装置のスロット番号を指定します。これは 1 に固定されています。

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 2-7 コマンド出力

フィールド	説明
VLAN 2	VLAN IDです。
Router slots (0 in total)	このフィールドはサポートされていません。
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。

2.1.8 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 2-8 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

2.1.9 dot1p-priority (MLD-snooping view)

Syntax

dot1p-priority *priority*

undo dot1p-priority

デフォルト

MLD メッセージのグローバルな 802.1p 優先順位は 6 です。

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

2.1.10 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**

2.1.11 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

2.1.12 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

2.1.13 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

2.1.14 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

2.1.15 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

2.1.16 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**

2.1.17 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**

2.1.18 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**

2.1.19 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**

2.1.20 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**

2.1.21 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**

2.1.22 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)

2.1.23 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**

2.1.24 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

2.1.25 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)

2.1.26 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**

2.1.27 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

2.1.28 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**

2.1.29 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**

2.1.30 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)

2.1.31 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。

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**

2.1.32 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**

2.1.33 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**

2.1.34 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)**

2.1.35 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** コ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)

2.1.36 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**

2.1.37 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

2.1.38 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

2.1.39 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)**

2.1.40 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

2.1.41 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

2.1.42 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

2.1.43 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

2.1.44 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

2.1.45 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

2.1.46 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** コ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

2.1.47 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**

QX-S1100G シリーズ Ethernet スイッチ

コマンドマニュアル

6.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-ラインレート
05-輻輳制御
06-タイムレンジ
07-データバッファ

目次

このセクションのページは **6-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 description 1-6
1.1.5 display acl 1-6
1.1.6 display packet-filter 1-8
1.1.7 display packet-filter statistics 1-10
1.1.8 display packet-filter statistics sum 1-13
1.1.9 display packet-filter verbose 1-15
1.1.10 display qos-acl resource 1-18
1.1.11 packet-filter 1-20
1.1.12 reset acl counter 1-22
1.1.13 reset packet-filter statistics 1-22
1.1.14 rule (IPv4 advanced ACL view) 1-24
1.1.15 rule (IPv4 basic ACL view) 1-30
1.1.16 rule (IPv6 advanced ACL view) 1-32
1.1.17 rule (IPv6 basic ACL view) 1-39
1.1.18 rule (Layer 2 ACL view) 1-41
1.1.19 rule comment 1-43
1.1.20 step 1-44

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。

ACL 番号を指定する場合は、以下の規則に従ってください。

- IPv6 ACL を指定するには、ACL 番号と ipv6 キーワードの両方を指定する必要があります。
- レイヤ 2 ACL を指定するには、mac キーワードなしで ACL 番号を指定できます。

IPv6 ACL またはレイヤ 2 ACL を名前で指定するには、ACL 名と **ipv6** または **mac** キーワードの両方を指定する必要があります。

新しい ACL は送信元 ACL と同じプロパティとコンテンツを持っていますが、送信元 ACL とは異なる番号または名前を使用しています

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 の詳細はセクション 10 *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。

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 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

1.1.5 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.
```

#拡張 IPv4 ACL **acl1_L4_IN** の設定と一致する統計情報を表示します。

<Switch > display acl name acl1_L4_IN

```
Advanced IPv4 ACL named acl1_L4_IN, 1 rule,
This is a dynamic advanced IPv4 ACL.
ACL's step is 5, start ID is 0
 rule 0 permit source 1.1.1.1 0
```

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。
rule 5 comment This rule is used on GigabitEthernet 1/0/1.	ACLルール5の説明です。
This is a dynamic advanced IPv4 ACL.	ACLは、アプリケーションモジュールによって動的に追加されます。 このタイプのACLは、アプリケーションモジュールによってのみ追加、変更、または削除でき、CLIコマンドを使用して設定することはできません。

1.1.6 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*: 装置のスロット番号を指定します。これは 1 に固定されています。

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 2001r
  IPv6 ACL 2002 (Failed)
  MAC ACL 4003
```

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。

フィールド	説明
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。
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。

1.1.7 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
Interface: GigabitEthernet1/0/1
 Inbound policy:
  IPv4 ACL 2001, Hardware-count
   From 2011-06-04 10:25:21 to 2011-06-04 10:35:57
   rule 0 permit source 2.2.2.2 0 (2 packets)
   rule 5 permit source 1.1.1.1 0 (Failed)
   Totally 2 packets permitted, 0 packets denied
   Totally 100% permitted, 0% denied
```

```
IPv6 ACL 2000

MAC ACL 4000
 rule 0 permit
```

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

1.1.8 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

1.1.9 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*: 装置のスロット番号を指定します。これは 1 に固定されています。

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)

  IPv6 ACL 2000
   rule 0 permit

  MAC ACL 4000

  IPv4 default action: Deny

  IPv6 default action: Deny, Hardware-count (Failed)

  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。

1.1.10 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*: 装置のスロット番号を指定します。これは 1 に固定されています。

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, XGE1/0/51 to XGE1/0/52 (slot 1)
```

```
------------------------------------------------------------------------
 Type           Total     Reserved   Configured Remaining  Usage
------------------------------------------------------------------------
 TTI ACL        256       0          0          256        0%
 PCL ACL        512       16         0          496        3%
 PCL Counter    656       14         0          642        2%
 IPCL Meter     768       0          0          768        0%
 EPCL Meter     128       0          0          128        0%

Interfaces: GE1/0/25 to GE1/0/48, XGE1/0/49 to XGE1/0/50 (slot 1)
------------------------------------------------------------------------
 Type           Total     Reserved   Configured Remaining  Usage
------------------------------------------------------------------------
 TTI ACL        256       0          0          256        0%
 PCL ACL        512       16         0          496        3%
 PCL Counter    656       14         0          642        2%
 IPCL Meter     768       0          0          768        0%
 EPCL Meter     128       0          0          128        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**–トンネルの終端とインタフェースで使用されるACLのリソースです。 • **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。
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。

1.1.11 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。

acl-number を使用して ACL を指定する場合は、以下のガイドラインに従ってください。

- IPv4 ACL を指定する場合、*acl-number* を直接指定します。
- IPv6 ACL を指定する場合、ipv6 パラメータを指定してから、*acl-number* を指定します。

- レイヤ 2 ACL を指定する場合、mac パラメータは必須ではありません。mac パラメータを指定してから *acl-number* 引数を指定するか、あるいは *acl-number* のみを指定します。

name *acl-name* オプションを使用して ACL を指定する場合は、以下のガイドラインに従ってください。

- IPv4 ACL を指定する場合、**name** *acl-name* オプションを指定します。
- IPv6 またはレイヤ 2 ACL を指定するには、関連キーワードを指定してから、**name** *acl-name* オプションを指定します。

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 IPv6 ACL、1 つの L2 ACL）を適用することができます。

VLAN インタフェースで設定された受信方向のパケットフィルタリングは、VLAN インタフェースで転送されるレイヤ 3 のパケット、VLAN インタフェースに関連付けられた物理ポートによって転送されるレイヤ 2 のパケットを含むすべてのパケットをフィルタします。

VLAN インタフェースで設定された出力方向のパケットフィルタリングはレイヤ 3 で転送されるパケットのみをフィルタします。

🕮 **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**

1.1.12 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

1.1.13 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**

1.1.14 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 port* | { **dscp** *dscp* | { **precedence** *precedence* | **tos** *tos* } * } | **fragment** | **icmp-type** { *icmp-type* [*icmp-code*] | *icmp-message* } | **logging** | **source** { *source-address source-wildcard* | **any** } | **source-port** *operator port* | **time-range** *time-range-name*] *

undo rule *rule-id* [{ { **ack** | **fin** | **psh** | **rst** | **syn** | **urg** } * | **established** } | **counting** | **destination** | **destination-port** | { **dscp** | { **precedence** | **tos** } * | **fragment** | **icmp-type** | **logging** | **source** | **source-port** | **time-range**] *

undo rule { **deny** | **permit** } *protocol* [{ { **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } * | **established** } | **counting** | **destination** { *dest-address dest-wildcard* | **any** } | **destination-port** *operator port* | { **dscp** *dscp* | { **precedence** *precedence* | **tos** *tos* } * | **fragment** | **icmp-type** { *icmp-type* [*icmp-code*] | *icmp-message* } | **logging** | **source** { *source-address source-wildcard* | **any** } | **source-port** *operator port* | **time-range** *time-range-name*] *

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。設定範囲は 0～255 です。表 1-7 に IPv4 で伝送されるプロトコルを示します。

表 1-7 IPv4 で伝送されるプロトコル

番号	キーワード	説明
N/A	**ip**	IPv4パケットと一致します。
1	**icmp**	ICMPパケットと一致します。
2	**igmp**	IGMPパケットと一致します。
4	**ipinip**	IP-in-IPパケットに一致します。
6	**tcp**	TCPパケットに一致
17	**udp**	UDPパケットと一致します。
89	**ospf**	OSPFパケットと一致します。

表 1-8 は、プロトコルの値に関係なく、指定できるパラメータを説明しています。

表 1-8 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。
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。

パラメータ	機能	説明
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の数を指定します。	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、セクション7 *ACL and QoS オペレーションマニュアルの”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 1-9に示します。

表 1-9 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 port*	TCP/UDPの送信元ポート番号を指定します。	*operator*は**eq** (equal to)のみ指定できます。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

パラメータ	機能	説明
destination-port *operator port*	TCP/UDPの宛先ポート番号を指定します。	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)
{ **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 1-10 に示します。

表 1-10 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 1-11に示します。

表 1-11 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
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**

1.1.15 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の数をを指定します。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、セクション *7 ACL and QoS オペレーションマニュアルの”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**

1.1.16 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 port* | **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 port* | **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。設定範囲は 0～255 です。表 1-12 で IPv6 で伝送されるプロトコルを示します。

表 1-12 IPv6 で伝送されるプロトコル

番号	キーワード	説明
N/A	**ipv6**	IPv6パケットと一致します。
1	**icmpv6**	ICMPv6パケットと一致します。
6	**tcp**	TCPパケットと一致します。
17	**udp**	UDPパケットに一致します。
50	**ipv6-esp**	IPv6-ESPパケットに一致
51	**ipv6-ah**	IPv6-AHパケットと一致します。
89	**ospf**	OSPFパケットと一致します。

表 1-13 では、プロトコルの値に関係なく、指定できるパラメータについて説明しています。

表 1-13 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。	*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。

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の数を指定します。	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、セクション7 *ACL and QoS オペレーションマニュアル*の”*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 1-14 に示します。

表 1-14 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 port*	TCP/UDPの送信元ポート番号を指定します。	*operator*は**eq** (equal to)のみ指定できます。*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 port*	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 1-15 に示します。

表 1-15 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 1-16 に示します。

表 1-16 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 1-13 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**::BF5C/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**

1.1.17 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、セクション 7 *ACL and QoS オペレーションマニュアル*の”*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**

1.1.18 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、セクション 7 *ACL and QoS オペレーションマニュアル*の”*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**

1.1.19 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

1.1.20 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 **6-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 display traffic classifier..... 2-1
2.1.2 if-match..... 2-2
2.1.3 traffic classifier..... 2-7
2.2 トラフィック動作設定コマンド..... 2-8
2.2.1 accounting..... 2-8
2.2.2 display traffic behavior..... 2-9
2.2.3 filter..... 2-11
2.2.4 nest top-most..... 2-11
2.2.5 redirect..... 2-12
2.2.6 remark dot1p..... 2-14
2.2.7 remark dscp..... 2-15
2.2.8 remark local-precedence..... 2-16
2.2.9 remark service-vlan-id..... 2-17
2.2.10 traffic behavior..... 2-18
2.3 QoS ポリシー設定コマンド..... 2-19
2.3.1 classifier behavior..... 2-19
2.3.2 display qos policy..... 2-20
2.3.3 display qos policy global..... 2-21
2.3.4 display qos policy interface..... 2-23
2.3.5 display qos vlan-policy..... 2-26
2.3.6 qos apply policy (interface view)..... 2-28
2.3.7 qos apply policy global..... 2-29
2.3.8 qos policy..... 2-29
2.3.9 qos vlan-policy..... 2-30
2.3.10 reset qos policy global..... 2-31
2.3.11 reset qos vlan-policy..... 2-32

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 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*: 装置のスロット番号を指定します。これは 1 に固定されています。

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。

2.1.2 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* [*mac-address-mask*]	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* [*mac-address-mask*]	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

＃発信元 MAC アドレスが 0050-ba27-bed3 で、MAC アドレスマスクが ffff-ffff-0000 のパケットと一致するように、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 destination-mac 0050-ba27-bed3 ffff-ffff-0000

＃トラフィッククラス class2 の一致条件を定義して、発信元 MAC アドレスが 0050-ba27-bed2 および MAC アドレスマスクが ffff-ffff-0000 のパケットを照合します。

<Switch> system-view

[Switch] traffic classifier class2

[Switch-classifier-class2] if-match source-mac 0050-ba27-bed2 ffff-ffff-0000

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

2.1.3 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 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*: 装置のスロット番号を指定します。これは 1 に固定されています。

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


  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。
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。

2.2.3 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。許可されたパケットは、同じ QoS ポリシー内の他のクラスと動作の関連付けによって処理します。

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

2.2.4 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

2.2.5 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、リダイレクト先の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**

2.2.6 remark dot1p

Syntax

remark [**green** | **red** | **yellow**] **dot1p** *dot1p-value*

undo remark [**green** | **red** | **yellow**] **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。

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

2.2.7 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
af41	100010	34

キーワード	DSCP 値（バイナリ）	DSCP 値（10 進数）
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

2.2.8 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

2.2.9 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

2.2.10 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*: 装置のスロット番号を指定します。これは 1 に固定されています。

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
 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*: 装置のスロット番号を指定します。これは 1 に固定されています。

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
 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。

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
```

```
  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

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: b
   Classifier: b
     Operator: AND
     Rule(s) :
      If-match any
     Behavior: b

Interface: GigabitEthernet1/0/4
  Direction: Inbound
  Policy: a
   Classifier: a
     Operator: AND
     Rule(s) :
      If-match any
     Behavior: a
      Mirroring:
        Mirror to the interface: GigabitEthernet1/0/5
```

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。

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 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*: 装置のスロット番号を指定します。これは 1 に固定されています。

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 2-8 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。

2.3.6 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TEST1 を適用します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] qos apply policy TEST1 outbound

2.3.7 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

2.3.8 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 global**
- **qos vlan-policy**

2.3.9 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

2.3.10 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

2.3.11 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 **6-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 プライオリティトラステッドモード設定コマンド 3-4
3.2.1 display qos trust interface 3-4
3.2.2 qos trust 3-5
3.3 ポートプライオリティ設定コマンド 3-6
3.3.1 qos priority 3-6

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 *7 ACL and QoS* の*”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 プライオリティトラステッドモード設定コマンド

3.2.1 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。

3.2.2 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

3.3 ポートプライオリティ設定コマンド

3.3.1 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

目次

このセクションのページは **6-x-x** です。

4 章 ラインレート 4-1
4.1 ラインレート設定コマンド 4-1
4.1.1 display qos lr interface 4-1
4.1.2 qos lr 4-2

4章 ラインレート

4.1 ラインレート設定コマンド

4.1.1 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 4-1 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。
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。

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 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。100 Mbps インタフェースの設定範囲は 8～102400 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 **6-x-x** です。

5 章 輻輳制御 5-1
5.1 SP 設定コマンド 5-1
5.1.1 display qos queue sp interface 5-1
5.1.2 qos sp 5-2
5.2 WRR 設定コマンド 5-2
5.2.1 display qos queue wrr interface 5-2
5.2.2 qos wrr 5-3
5.2.3 qos wrr weight 5-4
5.2.4 qos wrr group sp 5-5
5.3 キューベースアカウンティング設定コマンド 5-7
5.3.1 display qos queue-statistics interface outbound 5-7

5章 輻輳制御

5.1 SP設定コマンド

5.1.1 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 5-1 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。

5.1.2 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

5.2 WRR設定コマンド

5.2.1 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 5-2 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。
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。

5.2.2 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

5.2.3 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 5-3 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**

5.2.4 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 5-3 に示すキーワードで指定します。設定範囲は 0～7 です。

表 5-3 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 キューベースアカウンティング設定コマンド

5.3.1 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 5-4 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。

フィールド	説明
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。

目次

このセクションのページは **6-x-x** です。

6 章 タイムレンジ 6-1
6.1 タイムレンジ設定コマンド 6-1
6.1.1 display time-range 6-1
6.1.2 time-range 6-2

6章 タイムレンジ

6.1 タイムレンジ設定コマンド

6.1.1 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 6-1 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。

6.1.2 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

目次

このセクションのページは **6-x-x** です。

7 章 データバッファ 7-1
7.1 データバッファ設定コマンド 7-1
7.1.1 burst-mode enable 7-1

7章 データバッファ

7.1 データバッファ設定コマンド

7.1.1 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。

バースト機能を有効にすると、デフォルトのデータバッファ設定が変更されます。

例

バースト機能を有効にします。

<Switch> system-view

[Switch] burst-mode enable

QX-S1100G シリーズ Ethernet スイッチ

コマンドマニュアル

7. 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-ポートセキュリティ
05-公開鍵
06-SSH
07-IP ソースガード
08-ARP アタックプロテクション
09-TCP フラグメントアタックプロテクション
10-パスワード管理
11-SSL

目次

このセクションのページは **7-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 1-6
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 1-12
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 1-39
1.2.10 state (local user view) 1-40
1.2.11 user-group 1-41
1.3 RADIUS 設定コマンド 1-42
1.3.1 accounting-on enable 1-42
1.3.2 data-flow-format (RADIUS scheme view) 1-43
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) 1-50
1.3.6 key (RADIUS scheme view) 1-51
1.3.7 nas-ip (RADIUS scheme view) 1-53
1.3.8 primary accounting (RADIUS scheme view) 1-54
1.3.9 primary authentication (RADIUS scheme view) 1-56
1.3.10 radius dscp 1-58
1.3.11 radius nas-ip 1-58
1.3.12 radius scheme 1-60
1.3.13 reauthentication server-select 1-61
1.3.14 reset radius statistics 1-62
1.3.15 reset stop-accounting-buffer (for RADIUS) 1-63
1.3.16 retry 1-64
1.3.17 retry realtime-accounting 1-65
1.3.18 retry stop-accounting (RADIUS scheme view) 1-66
1.3.19 secondary accounting (RADIUS scheme view) 1-67
1.3.20 secondary authentication (RADIUS scheme view) 1-69
1.3.21 snmp-agent trap enable radius 1-71
1.3.22 state primary 1-72
1.3.23 state secondary 1-73
1.3.24 stop-accounting-buffer enable (RADIUS scheme view) 1-75
1.3.25 timer quiet (RADIUS scheme view) 1-76
1.3.26 timer realtime-accounting (RADIUS scheme view) 1-77
1.3.27 timer response-timeout (RADIUS scheme view) 1-78
1.3.28 user-name-format (RADIUS scheme view) 1-80

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。
- 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。
- 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 limit: 4
    MLD access limit: 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 limit: 4
    MLD access limit: 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。
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。

フィールド	説明
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セクション 1 *はじめに コマンドマニュアル*の“*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。

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。このオプションは装置管理および 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
  Password history was last reset: 0 days ago

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
  Password control configurations:
```

```
    Password length:        4 characters

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。
URL	ローカルユーザのリダイレクトURLです。

フィールド	説明
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。
Password history was last reset	履歴パスワードレコードがクリアされた最新の時間です。
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:

ネットワークアクセスユーザ：

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。

装置管理ユーザ：

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、ハッシュ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。

- 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。

装置管理ユーザ：

グローバルパスワード制御が有効になっている場合、装置は装置管理ユーザのパスワードを次のように処理します。

- 履歴レコード内のすべてのパスワードは、ハッシュテキストで保存されます。
- ユーザがプレーンテキストで自分のパスワードを変更すると、システムはユーザに現在のプレーンテキストパスワードの入力を要求します。新しいパスワードは、履歴レコード内のすべてのパスワードおよび現在のパスワードとは異なる必要があります。さらに、新しいパスワードには、現在のパスワードとは異なる最低 4 文字が必要です。
- ユーザが別のユーザのパスワードをプレーンテキストで変更する場合、新しいパスワードは、履歴レコードおよび現在のパスワードの後者のユーザのすべてのパスワードとは異なる必要があります。
- ユーザが自分のパスワードを削除すると、システムは現在のプレーンテキストパスワードの入力をユーザに要求します。
- 上記の状況を除き、システムはユーザに現在の平文パスワードの入力を要求したり、新しいパスワードを履歴レコードのパスワードや現在のパスワードと比較したりしません。

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 123456TESTuser&!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** コマンドの詳細はセクション 1 *はじめに コマンドマニュアルの“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
  Reauthentication server selection       : Reselect
------------------------------------------------------------------
```

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。
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MPLS L3 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。

フィールド	説明
Probe eap-profile	RADIUSサーバのステータス検出で指定されたEAPプロファイルです。 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EAPプロファイルが指定されていない場合、このフィールドは使用できません。
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。
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。 送信するRADIUSパケットにソースインタフェースあるいはソースIPアドレス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。
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。

フィールド	説明
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。
Reauthentication server selection	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。 再認証でのRADIUSサーバ選択モードです。 ● **Inherit**—ユーザの認証を実行したRADIUSサーバを使用して、そのユーザを再認証します。 ● **Reselect**—到達可能なRADIUSサーバを検索してユーザを再認証します。

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。
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。

フィールド	説明
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
Session ID	セッションIDです。属性Acct-Session-Idの値です。
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* | **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }

undo nas-ip [**interface** | **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

interface *interface-type interface-number:* 送信元インタフェースをタイプと番号で指定します。装置は、発信 RADIUS パケットのソース IP アドレスとして、インタフェースのプライマリ IPv4 アドレスあるいは IPv6 アドレスを使用します。

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 パケットのソースインタフェースあるいは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 パケットのソースインタフェースあるいは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 アドレスをチェックします。

- 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 サーバの IPv4 アドレスを指定します。

ipv6 *ipv6-address*: プライマリ RADIUS サーバの IPv6 アドレスを指定します。

port-number: プライマリ 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。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 サーバを指定します。

undo primary authentication コマンドはプライマリ RADIUS サーバの設定を削除します。

プライマリ RADIUS 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 { **interface** *interface-type interface-number* | { *ipv4-address* | **ipv6** *ipv6-address* } }

undo radius nas-ip { **interface** | { *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 IPv4 アドレスがパケットの送信元 IPv6 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

interface *interface-type interface-number:* 送信元インタフェースをタイプと番号で指定します。装置は、発信 RADIUS パケットのソース IP アドレスとして、インタフェースのプライマリ IPv4 アドレスまたは IPv6 アドレスを使用します。

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 パケットの送信元インタフェースあるいは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 パケットの送信元インタフェースあるいは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 アドレスをチェックします。

- 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IP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 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 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。デフォルトは 1812 です。

key: セカンダリ 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

secondary authentication コマンドはセカンダリ RADIUS サーバを指定します。

undo secondary authentication コマンドはセカンダリ RADIUS サーバの設定を削除します。

セカンダリ RADIUS 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 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 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 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 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 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 サーバのデフォルトは 1812 です。セカンダリ RADIUS アカウンティグン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。これを 0 に設定すると、サーバは到達不能な場合にユーザの現在のサーバの状態を変更しません。 ユーザの認証あるいはアカウンティング要求をアクティブ状態の次のサーバに送信します。新しいユーザの認証またはアカウンティング要求の場合、現在のサーバがアクティブ状態にあるため、現在のサーバに要求を送信します。

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

リアルタイムアカウンティング間隔を変更すると、変更前にオンラインであったユーザに以下のルールが適用されます。

- リアルタイムアカウンティング間隔をゼロ以外の値からゼロあるいはゼロからゼロ以外の値に変更した場合、変更はこれらのユーザに反映されません。 これらのユーザは、引き続き古いリアルタイムアカウンティング間隔を使用します。
- リアルタイムアカウンティング間隔をゼロ以外の値から別のゼロ以外の値に変更すると、変更はこれらのユーザにすぐに反映されます。

ユーザが RADIUS 認証と承認ではなく RADIUS アカウンティングを使用する場合、装置は、ユーザの RADIUS アカウンティングスキームで設定されたリアルタイムアカウンティングインターバルのみに基づいて、そのユーザのリアルタイムアカウンティングを実行します。

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 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 **7-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 2-11
2.1.4 dot1x 2-12
2.1.5 dot1x access-user log enable 2-13
2.1.6 dot1x authentication-method 2-13
2.1.7 dot1x auth-fail vlan 2-15
2.1.8 dot1x guest-vlan 2-16
2.1.9 dot1x guest-vlan-delay 2-17
2.1.10 dot1x handshake 2-18
2.1.11 dot1x handshake reply enable 2-19
2.1.12 dot1x mandatory-domain 2-20
2.1.13 dot1x max-user 2-21
2.1.14 dot1x multicast-trigger 2-22
2.1.15 dot1x port-control 2-23
2.1.16 dot1x port-method 2-24
2.1.17 dot1x quiet-period 2-25
2.1.18 dot1x re-authenticate 2-26
2.1.19 dot1x retry 2-27
2.1.20 dot1x timer 2-28
2.1.21 dot1x timer reauth-period 2-30
2.1.22 dot1x unicast-trigger 2-32
2.1.23 reset dot1x guest-vlan 2-33
2.1.24 reset dot1x statistics 2-33
2.1.25 reset dot1x unicast-trigger quiet-mac 2-34

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
  EAP 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
  User aging period for Auth-Fail VLAN : 1000 s
  User aging period for critical VLAN  : 1000 s
  User aging period for guest VLAN     : 1000 s
  EAD assistant function             : Disabled
     URL                           : http://www.dwsoft.com
     Free IP                       : 6.6.6.0       255.255.255.0
     EAD timeout                   : 30 min
  Domain delimiter                  : @
  Max EAP-TLS fragment (to-server)     : 400 bytes
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           : MAC-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
  User aging                    : Enabled
  Server-recovery online-user-sync : Enabled
```

```
Auth-Fail EAPOL                : Disabled
Critical EAPOL                 : Disabled
Discard duplicate EAPOL-Start    : No

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。

フィールド	説明
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。
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。
User aging period for Auth-Fail VLAN	認証を失敗したVLANユーザ秒単位のエージングタイマです。
User aging period for critical VLAN	重要なVLANユーザの秒単位のエージングタイマです。
User aging period for guest VLAN	ゲストVLANユーザの秒単位のエージングタイマです。
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。
Max EAP-TLS fragment (to-server)	認証パケットでサーバに送信されるEAP-TLSフラグメントの最大サイズです。 最大サイズが設定されていない場合、このフィールドにはN / Aが表示されます。
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。

フィールド	説明
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**
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。

フィールド	説明
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。
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。
User aging	ポートでの802.1X非認証ユーザエージングステータスです。 ● **Enabled**–有効です。 ● **Disabled**–無効です。
Server-recovery online-user-sync	802.1Xオンラインユーザ同期のステータスです。 ● **Enabled**–有効です。 ● **Disabled**–無効です。
Auth-Fail EAPOL	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。 このフィールドには、装置がポート上の802.1X Auth-Fail VLANへの割り当て時にEAP-Successパケットを802.1Xクライアントに送信するかどうかが表示されます。
Critical EAPOL	このフィールドは、ポート上の802.1XクリティカルVLANへの割り当て時に、デバイスが802.1XクライアントにEAP-Successパケットを送信するかどうかを表示します。

フィールド	説明
Discard duplicate EAPOL-Start	装置が重複した802.1X EAPOL-Startパケットを破棄するかどうかを表示します。 ● **Yes**—装置は重複した802.1X EAPOL-Startパケットを破棄します。 ● **No**—装置は重複した802.1X EAPOL-Startパケットを破棄しません。
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。
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*: 装置のスロット番号を指定します。これは 1 に固定されています。

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 number/name: 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。
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。 サーバによって承認VLANとしてユーザに割り当てられたVLANは、ユーザアクセスポートで構成されている可能性がありますが、タグ付けモードが異なります。たとえば、サーバはタグ付き属性を使用して許可VLANを割り当てますが、ポートで構成された同じVLANにはタグなし属性があります。 この状況で、ポートのリンクタイプがハイブリッドの場合、ポートで構成されたVLAN設定はユーザに反映されます。詳細については、セクション7 *セキュリティ オペレーションマニュアルの“802.1X”*を参照してください

フィールド	説明
Authorization tagged VLAN list	ユーザに許可されたタグづけVLANです。 サーバによって承認VLANとしてユーザに割り当てられたVLANは、ユーザアクセスポートで構成されている可能性がありますが、タグ付けモードが異なります。たとえば、サーバはタグ付き属性を使用して許可VLANを割り当てますが、ポートで構成された同じVLANにはタグなし属性があります。 この状況で、ポートのリンクタイプがハイブリッドの場合、ポートで構成されたVLAN設定はユーザに反映されます。詳細については、セクション7 *セキュリティ オペレーションマニュアルの "802.1X"* を参照してください。
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 number/name	ユーザに許可されたACLの番号あるいは名前です。 ACLが許可されていない場合、このフィールドには**N / A**が表示されます。 ACL許可が失敗した場合、このフィールドはACL番号または名前の後に**(Not effective)**と表示されます。
Authorization user profile	ユーザに許可されたユーザプロファイルです。
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 Version7.1.13 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－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、セクション 8 *セキュリティ コマンドマニュアル*の“*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**：

Version 7.1.5 を含むそれ以降は、2048 まで認証動作が可能です。
Version 7.1.3 は、2000 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。

ユーザがオンライン同期を待機している間にそのユーザの定期的な再認証がトリガーされると、システムはオンライン同期を実行し、ユーザの再認証は実行しません。

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 { **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* | **user-aging** { **auth-fail-vlan** | **critical-vlan** | **guest-vlan** } *aging-time-value* } }

undo dot1x timer { **handshake-period** | **quiet-period** | **reauth-period** | **server-timeout** | **supp-timeout** | **tx-period** | **unicast-trigger quiet-period** | **user-aging** { **auth-fail-vlan** | **critical-vlan** | **guest-vlan** } }

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
- 802.1X VLAN の該当するすべてのタイプのユーザエージングタイマ：1000 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 Version7.1.13 を含む以降のソフトウェアで 86400 まで設定が可能です。
Version7.1.9 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。

user-aging: 802.1X VLAN タイプのユーザエージングタイマを設定します。

auth-fail-vlan: 802.1X Auth-Fail VLAN を指定します。

critical-vlan: 802.1X クリティカル VLAN を指定します。

guest-vlan: 802.1X ゲスト VLAN を指定します。

aging-time-value: ユーザのエージングタイマを設定します。設定範囲は 60～2147483647 秒です。

🕮 **メモ：**

unicast-trigger quiet-period *quiet-period-value* オプションは Version7.1.13 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。
- **ユーザエージングタイマ（user-aging）**—802.1X 非認証ユーザエージングを有効にすると、Auth-Fail、クリティカル、またはゲスト VLAN ユーザエージングタイマを開始します。802.1X VLAN タイプのユーザエージングタイマは、そのタイプの VLAN にユーザが滞在できる時間を決定します。
  ユーザエージングの動作の詳細については、**dot1x unauthenticated-user aging enable** コマンドの使用ガイドラインを参照してください。
  ユーザエージングタイマをユーザ名要求タイムアウトタイマの倍数に設定しないでください（**dot1x timer tx-period** コマンド）。 その場合、エージングタイマは有効になりません。

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 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

2.1.22 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。

ベストプラクティスとして、ポートベースのアクセス制御を実行するポートでユニキャストトリガを使用しないでください。そのようにすると、ポート上のユーザが正しくオンラインにならない場合があります。

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 port-method**
- **dot1x retry**
- **dot1x timer**

2.1.23 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

2.1.24 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

2.1.25 reset dot1x unicast-trigger quiet-mac

🕮 **メモ**:

display dot1x unicast-trigger quiet-mac コマンドは Version7.1.13 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 dot1x unicast-trigger quiet-mac [**Interface** *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 **7-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 3-9
3.1.4 mac-authentication access-user log enable 3-10
3.1.5 mac-authentication domain 3-11
3.1.6 mac-authentication guest-vlan 3-12
3.1.7 mac-authentication guest-vlan auth-period 3-13
3.1.8 mac-authentication max-user 3-14
3.1.9 mac-authentication offline-detect enable 3-15
3.1.10 mac-authentication parallel-with-dot1x 3-16
3.1.11 mac-authentication timer (interface view) 3-17
3.1.12 mac-authentication timer (system view) 3-18
3.1.13 mac-authentication user-name-format 3-20
3.1.14 reset mac-authentication guest-vlan 3-22
3.1.15 reset mac-authentication statistics 3-23

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
  Authentication method             : PAP
  Username format                  : MAC address in lowercase(xxxxxxxxxxxx)
        Username                  : mac
        Password                  : Not configured
  MAC range accounts                : 2
       MAC address        Mask              Username
       2222-0000-0000     ffff-0000-0000      user1
       4444-0000-0000     ffff-0000-0000      user1
```

```
  Offline detect period            : 300 s
  Quiet period                    : 60 s
  Server timeout                   : 100 s
  Reauth period                   : 3600 s
  User aging period for critical VLAN : 1000 s
  User aging period for guest VLAN    : 1000 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 reauthentication     : Enabled
    Guest VLAN auth-period       : 150 s
  Critical VLAN                 : Not configured
  Critical voice VLAN            : Disabled
  Host mode                     : Multiple VLAN
  Offline detection              : Enabled
  Authentication order           : Parallel
  User aging                    : Enabled
  Server-recovery online-user-sync : Enabled

  Auto-tag feature              : Disabled
  VLAN tag configuration ignoring  : Disabled
  Max online users              : 4294967295
  Authentication attempts         : successful 2, failed 3
  Current online users           : 1
       MAC address      Auth state
       0001-0000-0000    Authenticated
       0001-0000-0001    Unauthenticated
```

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。
Authentication method	MAC認証方法はCHAPあるいはPAPです。
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。 ● 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。
MAC range accounts	MACアドレス範囲に固有のMAC認証ユーザアカウントです。
MAC address	MACアドレスです。
Mask	MACアドレスマスクです。 MACアドレスとマスクはともにMACアドレス範囲を指定します
Username	MACアドレス範囲内のユーザ名です。
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。

フィールド	説明
User aging period for critical VLAN	重要なVLANユーザの秒単位のエージングタイマーです。
User aging period for guest VLAN	ゲストVLANユーザの秒単位のエージングタイマーです。
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。
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	ポートのMAC認証のステータスです。 ● **Enabled**－有効です。 ● **Enabled** (but NOT effective)－有効（ただし無効）です。 この値は、装置に使用可能なACLリソースがないときにMAC認証が有効になっている場合に表示されます。 ● **Disabled**－無効です。
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。

フィールド	説明
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 reauthentication	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。 MAC認証でのゲストVLAN再認証のステータスです。有効あるいは無効です。
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。
Host mode	ポート上の1つのVLANから別のVLANに移動するユーザのMAC認証VLANモードです。 ● **Single VLAN**—シングルVLANモードです。 ● **Multiple VLAN**—マルチVLANモードです。
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。
User aging	ポート上の認証されていないMAC認証ユーザのエージング機能のステータスです。 ● **Enabled**－有効です。 ● **Disabled**－無効です。

フィールド	説明
Server-recovery online-user-sync	ポートでのMAC認証のオンラインユーザ同期のステータスです。 • **Enabled**－有効です。 • **Disabled**－無効です。
Guest VSI reauthentication	ポートで設定されたMACアドレス認証ゲストVSIです。有効あるいは無効です。
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*: 装置のスロット番号を指定します。これは 1 に固定されています。

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 number/name: 3001
Authorization user profile: N/A
Termination action: Radius-request
Session timeout period: 2 sec
Offline detection: 100 sec (server-assigned)
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。

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	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 number/name	ユーザに許可されたACLの番号あるいは名前です。 ユーザにACLが許可されていない場合、このフィールドには**N / A**が表示されます。 ACL許可が失敗した場合、このフィールドはACL番号または名前の後に**(Not effective)**と表示されます。
Authorization user profile	ユーザに許可されたユーザプロファイルです。
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。

フィールド	説明
Offline detection	ユーザのオフライン検出設定です。 • **Ignore (command-configured)**—装置はユーザのオフライン検出を実行しません。 設定はCLIから構成されます。 • **timer (command-configured)**— オフライン検出タイマを表示します。 タイマはCLIから設定されます。 • **Ignore (server-assigned)**—装置はユーザのオフライン検出を実行しません。 設定はRADIUSサーバによって割り当てられます。 • **timer (server-assigned)**—オフライン検出タイマを表示します。 タイマはRADIUSサーバによって割り当てられます。
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、セクション 8 *セキュリティ オペレーションマニュアル*の”*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：**

Version 7.1.5 を含むそれ以降は、2048 まで認証動作が可能です。
Vesion 7.1.3 では、2000 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。

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 コマンドはポートで MAC アドレス認証と 802.1X 認証の並列処理を無効にします。

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 コマンドの詳細はセクション 8 *セキュリティ コマンドマニュアル*の“*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セクション 8 *セキュリティ オペレーションマニュアル*の“*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 timer (interface view)

Syntax

mac-authentication timer auth-delay *auth-delay-time*

undo mac-authentication timer auth-delay

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。

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、セクション 8 *セキュリティ コマンドマニュアルの”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**

3.1.12 mac-authentication timer (system view)

Syntax

mac-authentication timer { **offline-detect** *offline-detect-value* | **quiet** *quiet-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** | **server-timeout** | **temporary-user-aging** | **user-aging** { **critical-vlan** | **guest-vlan** } }

デフォルト

offline detect timer は 300 秒、quiet timer は 60 秒、server timeout timer は 100 秒、User aging timer は 1000 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。

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。

user-aging: MAC 認証 VLAN のタイプにユーザエージングタイマを設定します。

critical-vlan: MAC 認証クリティカル VLAN を設定します。

guest-vlan: MAC 認証ゲスト VLAN を設定します。

aging-time-value: ユーザエージングタイマを設定します。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。
- **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。
- **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。

RADIUS パケット送信の最大試行回数と RADIUS サーバの応答タイムアウトタイマの設定については、*セクション7 セキュリティ オペレーションマニュアル*の“*AAA*”を参照してください。

- **User aging timer (user-aging)**— MAC 認証 VLAN のタイプにユーザエージングタイマを設定します。
  未認証の MAC 認証ユーザのユーザエージングを有効にすると、MAC 認証のクリティカルまたはゲスト VLAN のユーザエージングタイマを設定できます。あるタイプの MAC 認証 VLAN のユーザエージングタイマは、ユーザがそのタイプの VLAN に留まることができる期間を決定します。

MAC 認証ゲスト VLAN のユーザのユーザエージングタイマを、それらのユーザの認証間隔の倍数に設定しないでください。その場合、エージングタイマは有効になりません。ゲスト VLAN の MAC 認証ユーザの認証間隔は、**mac-authentication guest-vlan auth-period** コマンドで設定できます。

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 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。MAC ベースのユーザアカウントのパスワードを指定しない場合、装置は指定された形式の各ユーザの MAC アドレスをパスワードとして使用します。共有アカウントのパスワードを指定しない場合、共有アカウントにはパスワードがありません。

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。

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 アドレスを MAC 認証のユーザ名とパスワードの両方として使用します。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

3.1.14 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**

3.1.15 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 **7-x-x** です。

4章 ポートセキュリティ 4-1
4.1 ポートセキュリティ設定コマンド 4-1
4.1.1 display port-security 4-1
4.1.2 display port-security mac-address block 4-5
4.1.3 display port-security mac-address security 4-6
4.1.4 port-security access-user log enable 4-8
4.1.5 port-security authorization ignore 4-9
4.1.6 port-security enable 4-10
4.1.7 port-security intrusion-mode 4-11
4.1.8 port-security mac-address security 4-12
4.1.9 port-security mac-move permit 4-14
4.1.10 port-security max-mac-count 4-16
4.1.11 port-security ntk-mode 4-17
4.1.12 port-security oui 4-18
4.1.13 port-security port-mode 4-19
4.1.14 port-security timer autolearn aging 4-23
4.1.15 port-security timer disableport 4-25
4.1.16 snmp-agent trap enable port-security 4-26

4章 ポートセキュリティ

4.1 ポートセキュリティ設定コマンド

4.1.1 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
   Blockmac timeout       : 180 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
  MAC-move VLAN check bypass    : Disabled
```

表 4-1 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。
Blockmac timeout	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。 ブロックされたMACアドレスリスト内のMACアドレスのブロックタイマです。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。

フィールド	説明
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。
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セクション8 *セキュリティオペレーションマニュアル*の“*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転送します。 ● **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転送します。 ● **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転送します。 ● **NeedToKnowAuto**—ポートにオンラインユーザがいる場合のみ、認証された宛先MACアドレスのブロードキャストパケット、マルチキャストパケット、およびユニキャストフレームを転送します。 ● **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。
MAC-move VLAN check bypass	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。 他のポートからポートに移動するユーザに対してVLANチェックバイパス機能を有効にするかどうかを示します。

4.1.2 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 4-2 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

4.1.3 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 4-3 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残り時間です。 • 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

4.1.4 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を記録します。

mac-learning: MAC アドレスの学習イベントを記録します。

violation: 侵入防御イベントを記録します。

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 (セクション 11 *システム管理 コマンドマニュアル*)

4.1.5 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

4.1.6 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**

4.1.7 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**

4.1.8 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**

4.1.9 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。

ポートセキュリティ MAC の移動は、以下のシナリオで有効になります。

- **Port move on a device**—802.1X あるいは MAC 認証を通じて認証されたオンラインユーザは、装置上のポート間を移動します。ユーザ VLAN あるいは認証方法は、移動後に変更されるか、変更されないままになる場合があります。

- **VLAN move on a port**—802.1X あるいは MAC 認証を通じて認証されたオンラインユーザは、トランクあるいはハイブリッドポート上の VLAN 間を移動します。さらに、認証をトリガーするパケットには VLAN タグがあります。

ポートセキュリティ MAC 移動により、あるポートあるいは VLAN で 802.1X あるいは MAC 認証を通じて認証されたオンラインユーザを再認証し、最初にオフラインにならずに別のポートあるいは VLAN でオンラインにすることができます。ユーザが新しいポートあるいは VLAN で認証を渡すと、システムは元のポートまたは VLAN でユーザの認証セッションを削除します。

🕮 **メモ：**

MAC 認証の場合、MAC 移動機能は、MAC 認証シングル VLAN モードが使用されている場合にのみ適用されます。 MAC 移動機能は、MAC 認証マルチ VLAN モードが有効になっているポート上の VLAN 間を移動する MAC 認証ユーザには適用されません。

この機能が無効になっている場合、802.1X あるいは MAC で認証されたユーザは、新しいポートまたは VLAN で正常に再認証されてオンラインになる前に、オフラインにする必要があります。

802.1X または MAC 認証されたユーザは、認証サーバ上のオンラインユーザの最大数に達した場合、装置上のポート間またはポート上の VLAN 間を移動できません。

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

4.1.10 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

4.1.11 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

4.1.12 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

4.1.13 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 Version7.1.13 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	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、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、ダイナミックMACアドレスとしてMACアドレステーブルには追加されません。**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**モードに変更され未登録のMACアドレスを破棄します。
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	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	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。 ● 802.1Xフレームを受信した場合、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。 ● それ以外のフレームを受信した場合、MACアドレス認証のみを実行します。

キーワード	セキュリティモード	説明
mac-else-userlogin-secure-ext	macAddressElseUserLoginSecureExt	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	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
userlogin	userLogin	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	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	複数のユーザに対して802.1X認証を実行することを除き、**userLoginSecure**モードと同じです。

キーワード	セキュリティモード	説明
userlogin-secure-or-mac	macAddressOrUserLoginSecure	**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。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。 下記の2つの設定がある場合、認証していない不明なMACアドレスのパケットを受信すると、ポートは802.1X認証を開始するため、不明なMACアドレス宛にユニキャストEAP-Request/Identityパケットを送信します。送信後、ポートは802.1X認証の結果を待つことなく即座にMACアドレス認証の処理を行います。 ● MACアドレス認証と802.1X認証の並列処理（**mac-authentication parallel-with-dot1x**）が有効 ● 802.1Xユニキャストトリガ（**dot1x unicast-trigger**）が有効
userlogin-secure-or-mac-ext	macAddressOrUserLoginSecureExt	複数の802.1X認証およびMACアドレス認証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、セクション 8 *セキュリティ コマンドマニュアルの”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**

4.1.14 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**

4.1.15 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**

4.1.16 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、セクション 10 *システム管理 オペレーションマニュアル*の“*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 **7-x-x** です。

5 章 公開鍵 5-1
5.1 公開鍵設定コマンド 5-1
5.1.1 display public-key local public 5-1
5.1.2 display public-key peer 5-4
5.1.3 peer-public-key end 5-6
5.1.4 public-key local create 5-7
5.1.5 public-key local destroy 5-10
5.1.6 public-key local export dsa 5-11
5.1.7 public-key local export rsa 5-14
5.1.8 public-key peer 5-16
5.1.9 public-key peer import sshkey 5-17

5章 公開鍵

5.1 公開鍵設定コマンド

5.1.1 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
  585DA7F42519718CC9B09EEF038184000218041912CE34D12BCD2157E7AB1C2F03B3EF395
  100F3DB4A9E2FDFE860C1BD663D676438F7DA40A9406D61CA9079AF13E330489F1C76785DE
  52DA649AC8BC04B6D39CD7C52CD0A14F75F7491A91D31D6AC22340B5981B27A915CDEC4F09
  887E541EC1E5302D500F68E7AC29A084463C60F9EE266985A502FC92193E1CF4D265C4BA
==========================================
Key name: dsa1
```

```
Key type: DSA
Time when key pair created: 15:35:42 2011/05/12
Key code:
  308201B83082012C06072A8648CE3804013082011F02818100D757262C4584C44C211F18BD
  96E5F061C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE65BE6C265854889DC1E
  DBD13EC8B274DA9F75BA26CCB987723602787E922BA84421F22C3C89CB9B06FD60FE01941D
  DD77FE6B12893DA76EEBC1D128D97F0678D7722B5341C8506F358214B16A2FAC4B36895038
  7811C7DA33021500C773218C737EC8EE993B4F2DED30F48EDACE915F0281810082269009E1
  4EC474BAF2932E69D3B1F18517AD9594184CCDFCEAE96EC4D5EF93133E84B47093C52B20CD
  35D02492B3959EC6499625BC4FA5082E22C5B374E16DD00132CE71B020217091AC717B6123
  91C76C1FB2E88317C1BD8171D41ECB83E210C03CC9B32E810561C21621C73D6DAAC028F4B1
  585DA7F42519718CC9B09EEF0381850002818100A1E456C8DA2AD1BB83B1BDF2A1A6B5A6E8
  3642B460402445DA7E4036715F468F76655E114D460B7112F57143EE020AEF4A5BFAD07B74
  0FBCB1C64DA8A2BCE619283421445EEC77D3CF0D11866E9656AD6511F4926F8376967B0AB7
  15F9FB7B514BC1174155DD6E073B1FCB3A2749E6C5FEA81003E16729497D0EAD9105E3E76A
```

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
  7811C7DA33021500C773218C737EC8EE993B4F2DED30F48EDACE915F0281810082269009E1
  4EC474BAF2932E69D3B1F18517AD9594184CCDFCEAE96EC4D5EF93133E84B47093C52B20CD
  35D02492B3959EC6499625BC4FA5082E22C5B374E16DD00132CE71B020217091AC717B6123
  91C76C1FB2E88317C1BD8171D41ECB83E210C03CC9B32E810561C21621C73D6DAAC028F4B1
  585DA7F42519718CC9B09EEF0381850002818100A1E456C8DA2AD1BB83B1BDF2A1A6B5A6E8
  3642B460402445DA7E4036715F468F76655E114D460B7112F57143EE020AEF4A5BFAD07B74
  0FBCB1C64DA8A2BCE619283421445EEC77D3CF0D11866E9656AD6511F4926F8376967B0AB7
  15F9FB7B514BC1174155DD6E073B1FCB3A2749E6C5FEA81003E16729497D0EAD9105E3E76A
```

表 5-1 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

5.1.2 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 5-2 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 5-3 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**

5.1.3 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**

5.1.4 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 5-4 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 5-5 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 5-5 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**

5.1.5 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セクション 8 *セキュリティ オペレーションマニュアル*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

5.1.6 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セクション 1 *はじめに オペレーションマニュアルの”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 の詳細はセクション 1 *はじめに オペレーションマニュアルの“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**

5.1.7 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セクション 1 *はじめに オペレーションマニュアルの”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 の詳細はセクション 1 *はじめに オペレーションマニュアルの*“*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**

5.1.8 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**

5.1.9 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セクション 1 *はじめに オペレーションマニュアルの" 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 **7-x-x** です。

6 章 SSH 6-1
6.1 SSH サーバ設定コマンド 6-1
6.1.1 display ssh server 6-1
6.1.2 display ssh user-information 6-3
6.1.3 sftp server enable 6-4
6.1.4 sftp server idle-timeout 6-5
6.1.5 ssh server acl 6-6
6.1.6 ssh server authentication-retries 6-7
6.1.7 ssh server authentication-timeout 6-8
6.1.8 ssh server compatible-ssh1x enable 6-9
6.1.9 ssh server dscp 6-10
6.1.10 ssh server enable 6-11
6.1.11 ssh server ipv6 acl 6-11
6.1.12 ssh server ipv6 dscp 6-13
6.1.13 ssh server rekey-interval 6-13
6.1.14 ssh user 6-15
6.2 SSH クライアント設定コマンド 6-17
6.2.1 bye 6-17
6.2.2 cd 6-18
6.2.3 cdup 6-19
6.2.4 delete 6-19
6.2.5 dir 6-20
6.2.6 display sftp client source 6-21
6.2.7 display ssh client source 6-22
6.2.8 exit 6-22
6.2.9 get 6-23
6.2.10 help 6-24
6.2.11 ls 6-25
6.2.12 mkdir 6-26
6.2.13 put 6-26
6.2.14 pwd 6-27
6.2.15 quit 6-27
6.2.16 remove 6-28
6.2.17 rename 6-29
6.2.18 rmdir 6-29
6.2.19 sftp 6-30

6.2.20 sftp client ipv6 source 6-32
6.2.21 sftp client source 6-33
6.2.22 sftp ipv6 6-34
6.2.23 ssh client ipv6 source 6-36
6.2.24 ssh client source 6-37
6.2.25 ssh2 6-39
6.2.26 ssh2 ipv6 6-41

6章 SSH

6.1 SSHサーバ設定コマンド

6.1.1 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 6-1 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 6-2 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。

6.1.2 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 6-3 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

6.1.3 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

6.1.4 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

6.1.5 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

6.1.6 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

6.1.7 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

6.1.8 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

6.1.9 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

6.1.10 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

6.1.11 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

6.1.12 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

6.1.13 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

6.1.14 ssh user

Syntax

ssh user *username* **service-type** { **all** | **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 ISP ドメイン名が含まれる場合、*pureusername@domain* の形式になります。*pureusername* の設定範囲は 1～55 文字です。*domain* の設定範囲は 1～24 文字です。

service-type: SSH ユーザのサービスタイプを指定します。

- **all**: Stelnet、SFTP 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**: キーボードインタラクティブ認証、パスワード認証あるいは公開鍵認証を指定します。
- **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 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**

6.2 SSHクライアント設定コマンド

6.2.1 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>
```

6.2.2 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>
```

6.2.3 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>
```

6.2.4 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
```

6.2.5 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
```

6.2.6 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**

6.2.7 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**

6.2.8 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>
```

6.2.9 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
```

6.2.10 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
```

6.2.11 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
```

6.2.12 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

6.2.13 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
```

6.2.14 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.
```

6.2.15 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>

6.2.16 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
```

6.2.17 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
```

6.2.18 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

6.2.19 sftp

Syntax

sftp *server* [*port-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* | **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。

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 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。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 IPv4 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 SFP 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

6.2.20 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

6.2.21 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

6.2.22 sftp ipv6

Syntax

sftp ipv6 *server* [*port-number*] [**-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。

-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

6.2.23 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

6.2.24 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

6.2.25 ssh2

Syntax

ssh2 *server* [*port-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* | **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。

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 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。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 IPv4 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 $

6.2.26 ssh2 ipv6

Syntax

ssh2 ipv6 *server* [*port-number*] [**-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。

-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 **7-x-x** です。

7 章 IP ソースガード 7-1
7.1 IP ソースガード設定コマンド 7-1
7.1.1 display ip source binding 7-1
7.1.2 display ipv6 source binding 7-3
7.1.3 ip source binding (interface view) 7-5
7.1.4 ip verify source 7-7
7.1.5 ipv6 source binding (interface view) 7-8
7.1.6 ipv6 verify source 7-9

7章 IP ソースガード

7.1 IPソースガード設定コマンド

7.1.1 display ip source binding

Syntax

display ip source binding [**static** | [**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。

dhcp-server: DHCP サーバをもとに生成される IPv4SG バインディングを表示します。

dhcp-snooping: DHCP スヌーピングをもとに生成される IPv4SG バインディングを表示します。

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表示します。

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表示します。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 IPv4 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*: 装置のスロット番号を指定します。これは 1 に固定されています。

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
10.1.0.9        040a-0000-2000 GE1/0/2               N/A  Static
```

表 7-1 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IPSGで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。 • **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 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**

7.1.2 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*: 装置のスロット番号を指定します。これは 1 に固定されています。

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 7-2 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。
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。

フィールド	説明
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**

7.1.3 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

7.1.4 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

Layer 3 aggregate subinterface 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。

インタフェースで IPv4SG を複数回設定できます。最新の設定が有効になります。

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

7.1.5 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

Layer 3 aggregate subinterface 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

7.1.6 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

Layer 3 aggregate subinterface 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。

インタフェースで IPv6SG を複数回設定でき、最新の設定が有効になります。

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 **7-x-x** です。

8 章 ARP アタックプロテクション 8-1
8.1 宛先不明の IP アタックプロテクション設定コマンド 8-1
8.1.1 arp resolving-route enable 8-1
8.1.2 arp resolving-route probe-count 8-2
8.1.3 arp resolving-route probe-interval 8-2
8.1.4 arp source-suppression enable 8-3
8.1.5 arp source-suppression limit 8-4
8.1.6 display arp source-suppression 8-5
8.2 ARP パケットレートリミット設定コマンド 8-6
8.2.1 arp rate-limit 8-6
8.3 送信元 MAC ベース ARP アタック detection 設定コマンド 8-6
8.3.1 arp source-mac 8-6
8.3.2 arp source-mac aging-time 8-7
8.3.3 arp source-mac exclude-mac 8-8
8.3.4 arp source-mac threshold 8-9
8.3.5 display arp source-mac 8-10
8.4 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 8-11
8.4.1 arp valid-check enable 8-11
8.5 ARP 確認応答設定コマンド 8-12
8.5.1 arp active-ack enable 8-12
8.6 ARP アタック検出設定コマンド 8-12
8.6.1 arp detection enable 8-12
8.6.2 arp detection log enable 8-13
8.6.3 arp detection trust 8-14
8.6.4 arp detection validate 8-15
8.6.5 arp restricted-forwarding enable 8-16
8.6.6 display arp detection 8-16
8.6.7 display arp detection statistics attack-source 8-17
8.6.8 display arp detection statistics packet-drop 8-18
8.6.9 reset arp detection statistics attack-source 8-19
8.6.10 reset arp detection statistics packet-drop 8-20
8.7 ARP ゲートウェイプロテクション設定コマンド 8-21
8.7.1 arp filter source 8-21
8.8 ARP フィルタリング設定コマンド 8-22
8.8.1 arp filter binding 8-22

8章 ARP アタックプロテクション

8.1 宛先不明のIPアタックプロテクション設定コマンド

8.1.1 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**

8.1.2 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**

8.1.3 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**

8.1.4 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

8.1.5 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

8.1.6 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 8-1 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。

8.2 ARPパケットレートリミット設定コマンド

8.2.1 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

8.3 送信元MACベースARPアタックdetection設定コマンド

8.3.1 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

8.3.2 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

8.3.3 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。

このコマンドを繰り返して、送信元 MAC ベースの ARP 攻撃 detection から除外される最大 64 個の MAC アドレスを設定できます。

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

8.3.4 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

8.3.5 display arp source-mac

Syntax

display arp source-mac { **interface** *interface-type interface-number* [**slot** *slot-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*: 装置のスロット番号を指定します。これは 1 に固定されています。

slot *slot-number* 装置のスロット番号を指定します。これは 1 に固定されています。

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。

slot *slot-number* オプションは、**interface** *interface-type interface-number* オプションで仮想インタフェースが指定されている場合にのみサポートされます。

仮想インタフェースは、レイヤ 2 集約インタフェースのみです。

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/VSI name    Interface             Aging-time (sec)
23f3-1122-3344   4094           GE1/0/1               10
```

8.4 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

8.4.1 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

8.5 ARP確認応答設定コマンド

8.5.1 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

8.6 ARPアタック検出設定コマンド

8.6.1 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

8.6.2 arp detection log enable

Syntax

arp detection log enable [**interval** *interval* | **number** *number*]

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。

number *number*: 各ログ出力の ARP 攻撃検出ログの最大数を指定します。*number* は 1～128 の範囲で指定が可能です。デフォルトは 128 です。

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。

ログ数が多すぎると、装置のパフォーマンスに影響するだけでなく、特定のイベントログを見つけることが難しくなります。この問題を解決するために、ログ出力ごとに ARP 攻撃検出ログの最大数を調整します。制限数を超えるログ出力は表示されません。

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

8.6.3 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

8.6.4 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

8.6.5 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

8.6.6 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
```

表 8-2 コマンド出力

フィールド	説明
ARP detection is enabled in the following VLANs:	ARP攻撃detectionが有効なVLANです。VLANでARP攻撃detectionが有効になっていない場合、このフィールドには、どのVLANでもARP検出が有効になっていないことを表示します。

関連コマンド

arp detection enable

8.6.7 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*: 装置のスロット番号を指定します。これは 1 に固定されています。

説明

display arp detection statistics attack-source コマンドは ARP 攻撃ソースの統計情報を表示します。

例

スロット 1 の ARP 攻撃ソースの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 8-3 コマンド出力

フィールド	説明
Interface	ARP攻撃パケットの受信インタフェースです。
VLAN	ARP攻撃パケットが属するVLANです。
MAC address	ARP攻撃パケットの送信MACアドレスです。
IP address	ARP攻撃パケットの送信IPアドレスです。
Number	ARP攻撃detectionによって廃棄されたARP攻撃パケットの数です。
Time	ARP攻撃detectionがARP攻撃パケットを廃棄した最新の時刻です。

関連コマンド

arp detection enable

8.6.8 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*: タイプと番号でインタフェースを指定します。指定しない場合、すべてのインタフェースのドロップされたパケットの統計情報を表示します

説明

display arp detection statistics packet-drop コマンドは ARP アタック検出の統計情報を表示します。

例

ARP 攻撃 detection によってドロップされたパケットの統計を表示します。

<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 8-4 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**—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 packet-drop

8.6.9 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*: 装置のスロット番号を指定します。これは 1 に固定されています。

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

ARP 攻撃ソースの統計をクリアします。

<Switch> reset arp detection statistics attack-source

関連コマンド

- **arp detection enable**
- **display arp detection statistics attack-source**

8.6.10 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*: タイプと番号でインタフェースを指定します。指定しない場合、すべてのインタフェースのドロップされたパケットの統計情報を削除します。

説明

reset arp detection statistics コマンドは ARP アタック検出によってドロップされたパケットの統計情報を削除します。

例

ARP 攻撃 detection によってドロップ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

8.7 ARPゲートウェイプロテクション設定コマンド

8.7.1 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

8.8 ARPフィルタリング設定コマンド

8.8.1 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 **7-x-x** です。

9 章 TCP フラグメントアタックプロテクション 9-1
9.1 TCP フラグメントアタックプロテクション設定コマンド 9-1
9.1.1 attack-defense tcp fragment enable 9-1

9章 TCP フラグメントアタックプロテクション

9.1 TCPフラグメントアタックプロテクション設定コマンド

9.1.1 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 **7-x-x** です。

10 章 パスワード管理.....10-1
10.1 パスワード管理設定コマンド.....10-1
10.1.1 display password-control.....10-1
10.1.2 display password-control blacklist.....10-3
10.1.3 password-control { aging | composition | history | length } enable.....10-4
10.1.4 password-control aging.....10-6
10.1.5 password-control alert-before-expire.....10-7
10.1.6 password-control change-password first-login enable.....10-8
10.1.7 password-control complexity.....10-9
10.1.8 password-control composition.....10-10
10.1.9 password-control enable.....10-12
10.1.10 password-control expired-user-login.....10-13
10.1.11 password-control history.....10-14
10.1.12 password-control length.....10-15
10.1.13 password-control login idle-time.....10-17
10.1.14 password-control login-attempt.....10-18
10.1.15 password-control super aging.....10-21
10.1.16 password-control super composition.....10-22
10.1.17 password-control super length.....10-23
10.1.18 password-control update-interval.....10-23
10.1.19 reset password-control blacklist.....10-24
10.1.20 reset password-control history-record.....10-25

10章 パスワード管理

🕮 **メモ:**

本機能は Version 7.1.5 を含む以降のソフトウェアからサポートしています。

10.1 パスワード管理設定コマンド

10.1.1 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 10-1 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。

フィールド	説明
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。

10.1.2 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 10-2 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。

10.1.3 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**

10.1.4 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**

10.1.5 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

10.1.6 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**

10.1.7 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**

10.1.8 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**

10.1.9 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**

10.1.10 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

10.1.11 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**

10.1.12 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**

10.1.13 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

10.1.14 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**

10.1.15 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**

10.1.16 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**

10.1.17 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**

10.1.18 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

10.1.19 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

10.1.20 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 **7-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

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-S1100G 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

QX-S1100G シリーズ Ethernet スイッチ

コマンドマニュアル

8. 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-DLDP

02-Smart Link

03-Monitor Link

04-Track

目次

このセクションのページは **8-x-x** です。

1 章 DLDP 1-1
1.1 DLDP 設定コマンド 1-1
1.1.1 display dldp 1-1
1.1.2 display dldp statistics 1-3
1.1.3 dldp authentication-mode 1-5
1.1.4 dldp authentication-password 1-6
1.1.5 dldp delaydown-timer 1-7
1.1.6 dldp enable 1-8
1.1.7 dldp global enable 1-9
1.1.8 dldp interval 1-9
1.1.9 dldp unidirectional-shutdown 1-10
1.1.10 reset dldp statistics 1-11

1章 DLDP

1.1 DLDP設定コマンド

1.1.1 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 initial-unidirectional-delay: 100s
 Number of the port's neighbors: 1
  Neighbor MAC address: 0023-8956-3600
  Neighbor port index: 79
```

```
  Neighbor state: Confirmed
  Neighbor aged time: 13s
  Neighbor echo time: -

Interface GigabitEthernet1/0/2
 DLDP port state: Inactive
DLDP initial-unidirectional-delay: 100s
 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
 Number of the port’s neighbors: 1
DLDP initial-unidirectional-delay: 100s
  Neighbor MAC address: 0023-8956-3600
  Neighbor port index: 79
  Neighbor state: Confirmed
  Neighbor aged time: 13s
  Neighbor echo time: -
```

表 1-1 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 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
DLDP initial-unidirectional-delay	初期から単方向への状態遷移時にDLDPがインタフェースをブロックする遅延時間（秒）です。
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。
Neighbor echo time	エコータイマが期限切れになるまでの残りの秒数です。 エコータイマは、エントリタイマが切れると開始します。 エコータイマが期限切れになると、ネイバ情報が削除されます。ハイフン（-）は、エコータイマが開始されていないことを示します。

1.1.2 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 1-2 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

1.1.3 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**

1.1.4 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**

1.1.5 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

1.1.6 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

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**

1.1.7 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**

1.1.8 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

1.1.9 dldp unidirectional-shutdown

Syntax

dldp unidirectional-shutdown { **auto** | **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。

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

1.1.10 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 **8-x-x** です。

2 章 Smart Link 2-1
2.1 Smart Link 設定コマンド 2-1
2.1.1 display smart-link flush 2-1
2.1.2 display smart-link group 2-2
2.1.3 flush enable 2-3
2.1.4 port 2-4
2.1.5 port smart-link group 2-6
2.1.6 preemption delay 2-7
2.1.7 preemption mode 2-8
2.1.8 protected-vlan 2-9
2.1.9 reset smart-link statistics 2-10
2.1.10 smart-link flush enable 2-11
2.1.11 smart-link group 2-12

2章 Smart Link

2.1 Smart Link設定コマンド

2.1.1 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 2-1 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

2.1.2 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 2-2 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。）

2.1.3 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

2.1.4 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

2.1.5 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

2.1.6 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

2.1.7 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

2.1.8 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**（セクション 3 *アクセス コマンドマニュアル*の“*STP*”）
- **smart-link group**

2.1.9 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

2.1.10 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

2.1.11 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 **8-x-x** です。

3 章 Monitor Link 3-1
3.1 Monitor Link 設定コマンド 3-1
3.1.1 display monitor-link group 3-1
3.1.2 monitor-link group 3-2
3.1.3 port 3-3
3.1.4 port monitor-link group 3-4

3章 Monitor Link

3.1 Monitor Link設定コマンド

3.1.1 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 3-1 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。 ● **DOWN**－downしています。 ● **DOWN (Monitor Link)**― メンバリンクはモニタリンクによってシャットダウンされます。 ● **UP**－upしています。

3.1.2 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]

3.1.3 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

3.1.4 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

Loopback 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 **8-x-x** です。

4 章 Track 4-1
4.1 Track 設定コマンド 4-1
4.1.1 display track 4-1
4.1.2 track interface 4-3
4.1.3 track interface protocol 4-4
4.1.4 track nqa 4-6

4章 Track

4.1 Track設定コマンド

4.1.1 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
  Tracked object type: NQA
  Notification delay: Positive 20, Negative 30 (in seconds)
  Tracked object:
    NQA entry: admin test
    Reaction: 10
    Remote IP/URL: 2.2.2.2
    Local IP: 1.1.1.1
```

```
    Interface: Vlan-interface1
Track ID: 3
  State: Negative
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Tracked object type: Interface
  Notification delay: Positive 20, Negative 30 (in seconds)
  Tracked object:
    Interface:  Vlan-interface3
    Protocol: IPv4
```

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 4-1 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。
Type	追跡されるオブジェクトタイプです。 ● **Interface** ● **Route** ● **NQA** ● **LLDP** このフィールドは、**track brief brief**コマンドが実行された場合にのみ表示されます。
Tracked object type	追跡されるオブジェクトタイプです。 ● **Interface** ● **Route** ● **LLDP** ● **NQA**

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。
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。

関連コマンド

- **track interface**
- **track interface protocol**
- **track nqa**

4.1.2 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、トラック View あるいは既存のトラックエントリの View に入ります。

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。

track エントリを作成したのち、遅延時間の設定を修正する場合、**track interface delay** コマンドのみを使用することができます。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。

トラックエントリを作成するには、このコマンドのインタフェースであるトラッキング対象オブジェクトタイプを指定する必要があります。

既存のトラックエントリの View に入るには、**track** *track-entry-number* コマンドを使用します。 追跡されるオブジェクトタイプは必要ありません。

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

[Switch-track-1]

関連コマンド

- **display ip interface brief (セクション 4 IP サービス コマンドマニュアル)**
- **display track**

4.1.3 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

トラックエントリを作成するには、**interface protocol** コマンドでインタフェースプロトコルであるトラッキング対象オブジェクトタイプを指定する必要があります。

既存のトラックエントリの View に入るには、**track** *track-entry-number* コマンドを使用します。 追跡されるオブジェクトタイプは必要ありません。

トラックエントリ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てから、**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

[Switch-track-1]

関連コマンド

- **display ip interface brief (Layer 3—IP Services Command Reference)**
- **display track**

4.1.4 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

トラックエントリを作成するには、nqa コマンドでトラッキング対象オブジェクトタイプを指定する必要があります。

既存のトラックエントリの View に入るには、**track** *track-entry-number* コマンドを使用します。追跡されるオブジェクトタイプは必要ありません。

トラックエントリ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てから、**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

[Switch-track-1]

関連コマンド

- **delay**
- **display track**

QX-S1100G シリーズ Ethernet スイッチ

コマンドマニュアル

9. 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-NTP

03-Information Center

04-SNMP

05-RMON

06-NQA

07-ポートミラーリング

08-トラフィックミラーリング

09-プロセスモニタリングとメンテナンス

10-PoE

11-NetMeister

目次

このセクションのページは **9-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 1-2
1.1.4 ping ipv6 1-6
1.1.5 tracert 1-8
1.1.6 tracert ipv6 1-10

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 の詳細はセクション 10 *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。

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**] * *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。

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。
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。

フィールド	説明
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**] * *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）

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。
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* | **-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。

-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 操作を開始する前に、送信元と宛先の間の中間装置で ICMP 宛先到達不能メッセージの送信を有効にする必要があります。以下の ICMP 宛先到達不能メッセージのいずれかを受信すると、tracert 操作が停止します。

- **!N**—ネットワークに到達できません。
- **!H**—宛先ホストに到達できません。
- **!P**—プロトコルに到達できません。プロトコル番号は不明です。
- **!F**—断片化が必要です。このメッセージは、パケットの断片化が必要であるが、DF ビットが直接の装置に設定されていることを示しています。
- **!W**—宛先ホストが不明です。
- **!Q**—ToS のネットワークに到達できません。
- **!T**—ToS に到達できないホスト。

- **!X**—フィルタリングポリシーにより管理上禁止されている通信。
- **!V**—ホストの優先順位違反です。
- **!C**—優先カットオフが有効です。

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。
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* | **-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。

-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。）

IPv6 tracert 操作を開始する前に、送信元と宛先の間の中間装置で ICMPv6 宛先到達不能メッセージの送信を有効にする必要があります。以下の ICMPv6 宛先到達不能メッセージのいずれかが受信されると、IPv6 tracert 操作は停止します。

- **!N**—宛先へのルートはありません。
- **!P**—フィルタリングポリシーにより管理上禁止されている宛先との通信です。
- **!A**—アドレスに到達できません。到達不能の理由は不明です。
- **!S**—送信元アドレスの範囲を超えています。このメッセージは、プローブパケットにリンクローカルの送信元アドレスと非リンクローカルの宛先アドレスがある場合に表示されます。このようなパケットは、送信元アドレスのスコープを離れることなく宛先に配信できません。

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 **9-x-x** です。

2 章 NTP 2-1
2.1 NTP 設定コマンド 2-1
2.1.1 display ntp-service sessions 2-1
2.1.2 display ntp-service status 2-7
2.1.3 display ntp-service trace 2-10
2.1.4 ntp-service acl 2-11
2.1.5 ntp-service authentication enable 2-13
2.1.6 ntp-service authentication-keyid 2-14
2.1.7 ntp-service broadcast-client 2-15
2.1.8 ntp-service broadcast-server 2-16
2.1.9 ntp-service dscp 2-17
2.1.10 ntp-service enable 2-18
2.1.11 ntp-service inbound enable 2-18
2.1.12 ntp-service max-dynamic-sessions 2-19
2.1.13 ntp-service multicast-client 2-20
2.1.14 ntp-service reliable authentication-keyid 2-21
2.1.15 ntp-service source 2-22
2.1.16 ntp-service unicast-peer 2-24
2.1.17 ntp-service unicast-server 2-25

2章 NTP

2.1 NTP設定コマンド

2.1.1 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 2-1 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、stratumフィールドに関連した値が表示されます。 • 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。 • 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。
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 2-2 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NTPサーバです。 • **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NTPサーバ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-S1100G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。

2.1.2 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 2-3 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NTPサーバ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NTPサーバ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。

2.1.3 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 NTP サーバ間の 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 NTP サーバ間の 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 2-4 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NTPサーバの識別子です。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**

2.1.4 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**

2.1.5 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**

2.1.6 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**

2.1.7 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

2.1.8 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

2.1.9 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

2.1.10 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

2.1.11 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

2.1.12 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

2.1.13 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。IP アドレスは 224.0.1.0/24 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 NTP マルチキャストクライアント設定を削除します。

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、NTP マルチキャストクライアント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

2.1.14 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**

2.1.15 ntp-service source

Syntax

ntp-service source { *interface-type interface-number* | *ipv4-address* **}**

undo ntp-service source

デフォルト

NTP メッセージの送信元 IPv4 アドレ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 IPv4 アドレスとして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-type interface-number: インタフェースのタイプと番号を指定します。NTP メッセージの送信元インタフェースを指定すると、装置は指定された送信元インタフェースのプライマリ IPv4 アドレスをソースアドレスとして使用して、NTP メッセージを送信します。受信装置は、このアドレスを NTP 応答メッセージの宛先アドレスとして使用します

ip-address: NTP メッセージのソース IPv4 アドレスを指定します。

説明

ntp-service source コマンドは NTP メッセージの送信元 IPv4 アドレスを指定します。

undo ntp-service source コマンドはデフォルトに戻します。

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。

ntp-service unicast-server あるいは **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、指定されたインタフェースの IPv4 アドレスが NTP メッセージのソース IPv4 アドレスとして使用されます。

インタフェース View で **ntp-service broadcast-server** あるいは **ntp-service multicast-server** コマンドを設定している場合、インタフェースの IPv4 アドレスがブロードキャストまたはマルチキャスト NTP メッセージの送信元 IPv4 アドレスとして使用されます。

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 IPv4 アドレスとして 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

2.1.16 ntp-service unicast-peer

Syntax

ntp-service unicast-peer { *peer-name* | *ip-address* } [**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* }

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。

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**

2.1.17 ntp-service unicast-server

Syntax

ntp-service unicast-server { *server-name* | *ip-address* } [**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* }

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。

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 **9-x-x** です。

3 章 Information Center 3-1
3.1 Information Center 設定コマンド 3-1
3.1.1 display info-center 3-1
3.1.2 display logbuffer 3-2
3.1.3 display logbuffer summary 3-4
3.1.4 display logfile summary 3-5
3.1.5 enable log updown 3-6
3.1.6 info-center enable 3-6
3.1.7 info-center logbuffer 3-7
3.1.8 info-center logbuffer size 3-8
3.1.9 info-center loghost 3-9
3.1.10 info-center loghost source 3-10
3.1.11 info-center source 3-11
3.1.12 info-center synchronous 3-13
3.1.13 info-center syslog min-age 3-14
3.1.14 info-center timestamp 3-15
3.1.15 info-center timestamp loghost 3-16
3.1.16 logfile save 3-17
3.1.17 reset logbuffer 3-18
3.1.18 snmp-agent trap enable syslog 3-18
3.1.19 terminal debugging 3-19
3.1.20 terminal logging level 3-20
3.1.21 terminal monitor 3-21

3章 Information Center

3.1 Information Center設定コマンド

3.1.1 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, log output filter: loghost1,
   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
```

3.1.2 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 3-1 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*: 装置のスロット番号を指定します。これは 1 に固定されています。

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 3-2 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**

3.1.3 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 3-1 を参照してください。

slot *slot-number*: 装置のスロット番号を指定します。これは 1 に固定されています。

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 3-3 コマンド出力

フィールド	説明
EMERG	emergencyを示します。詳細は表 3-1を参照してください。
ALERT	alertを示します。詳細は表 3-1を参照してください。
CRIT	criticalを示します。詳細は表 3-1を参照してください。
ERROR	errorを示します。詳細は表 3-1を参照してください。
WARN	warningを示します。詳細は表 3-1を参照してください。
NOTIF	notificationを示します。詳細は表 3-1を参照してください。
INFO	informationalを示します。詳細は表 3-1を参照してください。

フィールド	説明
DEBUG	debugを示します。詳細は表 3-1を参照してください。

3.1.4 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: 2 MB
Log file directory: flash:/logfile
Writing frequency: 24 hour 0 min 10 sec
```

表 3-4 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。

3.1.5 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

3.1.6 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.
```

3.1.7 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。

info-center logbuffer コマンドは、ログソースモジュールに基づいてログバッファへのログ出力を有効にします。

- 個別のログバッファを持つモジュールによって生成されたログは、それぞれのログバッファに保存されます。
  たとえば、セッションログはセッションログバッファに保存されます。
- 他のモジュールによって生成されたログは、一般的なログバッファに保存されます。

ログバッファ情報とバッファされたログを表示するには、**display logbuffer** コマンドを使用します。

ログバッファサイズを設定するには、**info-center logbuffer size** コマンドを使用します。

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**

3.1.8 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。

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**

3.1.9 info-center loghost

Syntax

info-center loghost { *hostname* | *ipv4-address* | **ipv6** *ipv6-address* } [**port** *port-number*] [**facility** *local-number*] [**filter** *filter-name*]

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。

filter *filter-name*: ログホストへのログ出力を制御するログ出力フィルタを指定します。filter-name は、1～8 文字の大文字と小文字を区別しない文字列であるフィルタ名を表示します。ログ出力フィルタを指定しない場合、ログホストの宛先に **info-center source** コマンドを使用して構成されたログ出力ルールが使用されます。

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

関連コマンド

info-center source

3.1.10 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

3.1.11 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 3-5 にデフォルトのログ出力ルールを示します。

表 3-5 デフォルト出力ルール

宛先	送信元モジュール	出力スイッチ	セキュリティ
コンソール	サポートされるすべてのモジュールです。	Enabled	デバッグ
モニタ端末	サポートされるすべてのモジュールです。	Disabled	デバッグ
ログホスト	サポートされるすべてのモジュールです。	Enabled	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。	Enabled	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。	Enabled	Informational

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 3-1 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

3.1.12 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 Sysname SHELL/5/SHELL_LOGIN: VTY logged in 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 Sysname SHELL/5/SHELL_LOGIN: VTY logged in 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。

3.1.13 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

#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

3.1.14 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

3.1.15 info-center timestamp loghost

Syntax

info-center timestamp loghost { **date** [**with-milliseconds**] | **iso** [**with-milliseconds**] * | **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。

with-milliseconds: 日付あるいは ISO 8601 形式のログホストに出力されるログタイムスタンプをミリ秒単位で正確に設定します。 ミリ秒の値は、区切り文字としてドットを使用して、タイムスタンプの時間情報に追加されます。 このキーワードを指定しない場合、日付あるいは ISO 8601 形式のタイムスタンプは秒単位で正確です。

- ミリ秒精度の日付形式のタイムスタンプの例は Dec 8 10：12：21.708 2018 です。
- ミリ秒精度の ISO 8601 形式のタイムスタンプの例は 2018-09-21T15：32：55.708 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

3.1.16 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.
```

3.1.17 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

3.1.18 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、セクション 10 *システム管理 オペレーションマニュアル*の“*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

3.1.19 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 logs.
```

関連コマンド

- **terminal logging level**
- **terminal monitor**

3.1.20 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

3.1.21 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 **9-x-x** です。

4 章 SNMP 4-1
4.1 SNMP 設定コマンド 4-1
4.1.1 display snmp-agent community 4-1
4.1.2 display snmp-agent group 4-3
4.1.3 display snmp-agent local-engineid 4-5
4.1.4 display snmp-agent mib-view 4-6
4.1.5 display snmp-agent statistics 4-8
4.1.6 display snmp-agent sys-info 4-10
4.1.7 display snmp-agent trap queue 4-11
4.1.8 display snmp-agent trap-list 4-11
4.1.9 display snmp-agent usm-user 4-12
4.1.10 enable snmp trap updown 4-15
4.1.11 snmp-agent 4-16
4.1.12 snmp-agent { inform | trap } source 4-17
4.1.13 snmp-agent calculate-password 4-18
4.1.14 snmp-agent community 4-20
4.1.15 snmp-agent group 4-23
4.1.16 snmp-agent local-engineid 4-26
4.1.17 snmp-agent log 4-27
4.1.18 snmp-agent mib-view 4-28
4.1.19 snmp-agent packet max-size 4-29
4.1.20 snmp-agent packet response dscp 4-30
4.1.21 snmp-agent sys-info contact 4-31
4.1.22 snmp-agent sys-info location 4-32
4.1.23 snmp-agent sys-info version 4-33
4.1.24 snmp-agent target-host 4-34
4.1.25 snmp-agent trap enable 4-36
4.1.26 snmp-agent trap if-mib link extended 4-37
4.1.27 snmp-agent trap life 4-38
4.1.28 snmp-agent trap log 4-39
4.1.29 snmp-agent trap queue-size 4-39
4.1.30 snmp-agent usm-user { v1 | v2c } 4-40
4.1.31 snmp-agent usm-user v3 4-43

4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。

4.1 SNMP設定コマンド

4.1.1 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 4-1 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 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。
IPV6 ACL	IPv6 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。

フィールド	説明
IPV6 ACL name	IPv6 ACL名です。 このフィールドはSNMPv1あるいはSNMPv2cコミュニティにACLが指定されときにのみ表示されます。
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 }**

4.1.2 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 4-2 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 4-1を参照してください。）
ACL	IPv4 ACL番号です。 このフィールドはSNMPグループで、IPv4ACLが指定されたときのみ表示されます。

フィールド	説明
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。
IPv6 ACL	IPv6 ACL番号です。 このフィールドは、SNMPグループにIPv6 ACLが指定されたときのみ表示されます。
IPV6 ACL name	IPv6 ACL名です。 このフィールドは、SNMPグループにIPv6 ACLが指定されたときのみ表示されます。

関連コマンド

snmp-agent group

4.1.3 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

4.1.4 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 4-3 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 4-1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

4.1.5 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 4-4 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。
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。

フィールド	説明
forwarded Confirmed Class PDUs dropped silently	廃棄された転送パケットの数です。

4.1.6 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

4.1.7 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**

4.1.8 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

4.1.9 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 4-5 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 4-1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 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。
IPV6 ACL	IPv6 ACL番号です。 このフィールドは、SNMPv3ユーザにACLが指定されたときのみ表示されます。

フィールド	説明
IPV6 ACL name	IPv6 ACL名です。 このフィールドは、SNMPv3ユーザにACLが指定されたときのみ表示されます。

関連コマンド

snmp-agent usm-user v3

4.1.10 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**

4.1.11 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

4.1.12 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**

4.1.13 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**

4.1.14 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 の詳細はセクション *7 ACL and QoS オペレーションマニュアルの“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 コミュニティを亜 S く制します。

display snmp-agent community コマンドは、プレーンテキスト形式で作成および保存されたコミュニティに関する情報のみを表示します。

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**

4.1.15 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 4-6 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 4-6 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。
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 の詳細はセクション 7 *ACL and QoS オペレーションマニュアル*の“*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**

4.1.16 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**

4.1.17 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

4.1.18 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**

4.1.19 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

4.1.20 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

4.1.21 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

4.1.22 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

4.1.23 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。

IPv6 で SNMP 通知を使用するには、SNMPv2c あるいは SNMPv3 を有効にします。

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

4.1.24 snmp-agent target-host

Syntax

snmp-agent target-host inform address udp-domain { *ipv4- target-host* | **ipv6** *ipv6-target-host* } [**udp-port** *port-number*] **params securityname** *security-string* { **v2c** | **v3** [**authentication** | **privacy**] }

snmp-agent target-host trap address udp-domain { *ipv4- target-host* | **ipv6** *ipv6-target-host* } [**udp-port** *port-number*] **params securityname** *security-string* [**v1** | **v2c** | **v3** [**authentication** | **privacy**]]

undo snmp-agent target-host { **trap** | **inform** } **address udp-domain** { *ipv4- target-host* | **ipv6** *ipv6- target-host* } **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- target-host: 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- target-host*: 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**

4.1.25 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 4-7 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 sys-info version**
- **snmp-agent target-host**

4.1.26 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

4.1.27 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**

4.1.28 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

4.1.29 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。

キューのサイズを変更して、キュー内の通知の数がキューのサイズを超えるとき、最も古い通知が新しい通知のために廃棄されます。

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**

4.1.30 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 の詳細はセクション *7 ACL and QoS オペレーションマニュアル*の“*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**

4.1.31 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: 暗号化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 の詳細はセクション 7 *ACL and QoS オペレーションマニュアル*の“*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 **9-x-x** です。

5 章 RMON 5-1
5.1 RMON 設定コマンド 5-1
5.1.1 display rmon alarm 5-1
5.1.2 display rmon event 5-3
5.1.3 display rmon eventlog 5-4
5.1.4 display rmon history 5-6
5.1.5 display rmon prialarm 5-9
5.1.6 display rmon statistics 5-11
5.1.7 rmon alarm 5-14
5.1.8 rmon event 5-17
5.1.9 rmon history 5-18
5.1.10 rmon prialarm 5-20
5.1.11 rmon statistics 5-22

5章 RMON

5.1 RMON設定コマンド

5.1.1 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 5-1 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

5.1.2 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 5-2 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

5.1.3 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 5-3 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

5.1.4 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 5-4 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。 過大サイズパケットは、**jumboframe enable**コマンドで指定された最大フレーム長（フレーミングビットを除き、FCSオクテットを含む）を超えるパケットです。
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

5.1.5 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 5-5 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

5.1.6 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 5-6 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。 過大サイズパケットは、**jumboframe enable**コマンドで指定された最大フレーム長（フレーミングビットを除き、FCSオクテットを含む）を超えるパケットです。
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。

フィールド	説明
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。
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

5.1.7 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 5-7 の 1 つを使用します。

表 5-7 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**

5.1.8 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、セクション 10 *システム管理 オペレーションマニュアル* の”*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**

5.1.9 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

5.1.10 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**

5.1.11 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。

RMON 統計エントリのインデックスは、グローバルに一意である必要があります。インデックスが別のインタフェースで使用されている場合、作成操作は失敗します。

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 **9-x-x** です。

6 章 NQA 6-1
6.1 NQA クライアント設定コマンド 6-1
6.1.1 advantage-factor 6-1
6.1.2 codec-type 6-2
6.1.3 data-fill 6-2
6.1.4 data-size 6-4
6.1.5 description 6-5
6.1.6 destination ip 6-6
6.1.7 destination port 6-7
6.1.8 display nqa history 6-7
6.1.9 display nqa result 6-9
6.1.10 display nqa statistics 6-15
6.1.11 filename 6-23
6.1.12 frequency 6-23
6.1.13 history-record enable 6-24
6.1.14 history-record keep-time 6-25
6.1.15 history-record number 6-26
6.1.16 next-hop ip 6-27
6.1.17 nqa 6-28
6.1.18 nqa agent enable 6-29
6.1.19 nqa schedule 6-29
6.1.20 operation (FTP operation view) 6-31
6.1.21 operation (HTTP operation view) 6-32
6.1.22 password 6-33
6.1.23 probe count 6-34
6.1.24 probe packet-interval 6-35
6.1.25 probe packet-number 6-36
6.1.26 probe packet-timeout 6-37
6.1.27 probe timeout 6-37
6.1.28 reaction checked-element probe-fail (for trap) 6-38
6.1.29 reaction trap 6-40
6.1.30 resolve-target 6-41
6.1.31 route-option bypass-route 6-42
6.1.32 source interface (ICMP echo operation view) 6-43
6.1.33 source ip 6-44
6.1.34 source port 6-45

6.1.35 statistics hold-time 6-46
6.1.36 statistics interval 6-46
6.1.37 statistics max-group 6-47
6.1.38 tos 6-48
6.1.39 ttl 6-49
6.1.40 type 6-50
6.1.41 url 6-51
6.1.42 username 6-52
6.1.43 version 6-53
6.2 NQA サーバ設定コマンド 6-54
6.2.1 display nqa server 6-54
6.2.2 nqa server enable 6-55
6.2.3 nqa server tcp-connect 6-56
6.2.4 nqa server udp-echo 6-57

6章 NQA

6.1 NQAクライアント設定コマンド

6.1.1 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

6.1.2 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

6.1.3 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

6.1.4 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 6-1 に示します。

表 6-1 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

6.1.5 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

6.1.6 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

6.1.7 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

6.1.8 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 6-2 コマンド出力

フィールド	説明
Index	履歴記録のIDです。
TTL	ルーティングテーブルバイパス機能が操作で有効になっていないとき、このフィールドにはプローブパケットのTTL値が表示されます。 ルーティングテーブルバイパス機能が有効なとき、このフィールド値は**init-ttl**コマンドによって異なります。ただし、プローブパケットの実際のTTL値は1に固定されています。
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。

6.1.9 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
   SD average: 14                    DS average: 14
 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
    SD average: 0                      DS average: 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 6-3 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
SD average	送信元から宛先へのジッタの平均値です。
DS average	宛先から送信元へのジッタの平均値です。
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。
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	ルーティングテーブルバイパス機能が操作で有効になっていないとき、このフィールドにはプローブパケットのTTL値が表示されます。 ルーティングテーブルバイパス機能が有効な場合、このフィールド値は**init-ttl**コマンドによって異なります。ただし、プローブパケットの実際のTTL値は1に固定されています。

フィールド	説明
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。

6.1.10 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 6-4 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。

フィールド	説明
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。
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。

フィールド	説明
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。
SD average	送信元から宛先へのジッタの平均値です。
DS average	宛先から送信元へのジッタの平均値です。
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。

フィールド	説明
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。
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 6-5 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 6-5 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

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-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 6-5 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 6-6 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

6.1.11 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

6.1.12 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

6.1.13 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

6.1.14 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

6.1.15 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

6.1.16 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

6.1.17 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]

6.1.18 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

6.1.19 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**（セクション 1 *はじめに オペレーションマニュアルの“装置管理”*）
- **type**

6.1.20 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**

6.1.21 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**

6.1.22 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**

6.1.23 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

6.1.24 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

6.1.25 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

6.1.26 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

6.1.27 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

6.1.28 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

6.1.29 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

6.1.30 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

6.1.31 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

6.1.32 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

6.1.33 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 IPv4 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 IPv4 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

6.1.34 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

6.1.35 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

6.1.36 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

6.1.37 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

6.1.38 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

6.1.39 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

6.1.40 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]

6.1.41 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、セクション1 *はじめに オペレーションマニュアルの”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

6.1.42 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**

6.1.43 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

6.2 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。

6.2.1 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 6-7 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。 ToSの値は、NQAサーバでTCPまたはUDPリスニングサービスを構成するときに指定できます。ToSの値が指定されていないとき、次の規則が適用されます。 このフィールドには、ハイフン（-）が表示されます。 TCPリスニングサービスの応答パケットのToSの値は0です。 UDPリスニングサービスの応答パケットのToSの値は、要求パケットから取得されます。
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**

6.2.2 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**

6.2.3 nqa server tcp-connect

Syntax

nqa server tcp-connect *ip-address port-number* [**tos** *tos*]

undo nqa server tcp-connect *ip-address port-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

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。

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**

6.2.4 nqa server udp-echo

Syntax

nqa server udp-echo *ip-address port-number* [**tos** *tos*]

undo nqa server udp-echo *ip-address port-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

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。

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 **9-x-x** です。

7 章 ポートミラーリング 7-1
7.1 ポートミラーリング設定コマンド 7-1
7.1.1 display mirroring-group 7-1
7.1.2 mirroring-group 7-2
7.1.3 mirroring-group mirroring-port (interface view) 7-3
7.1.4 mirroring-group mirroring-port (system view) 7-4
7.1.5 mirroring-group monitor-egress 7-6
7.1.6 mirroring-group monitor-port (interface view) 7-8
7.1.7 mirroring-group monitor-port (system view) 7-9
7.1.8 mirroring-group reflector-port 7-10
7.1.9 mirroring-group remote-probe vlan 7-12

7章 ポートミラーリング

7.1 ポートミラーリング設定コマンド

7.1.1 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 7-1 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。

7.1.2 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

7.1.3 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

7.1.4 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

7.1.5 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

7.1.6 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

7.1.7 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

7.1.8 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。

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

7.1.9 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。

装置は 1 つのリモートプローブ VLAN のみをサポートします。

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 **9-x-x** です。

8 章 トラフィックミラーリング 8-1
8.1 トラフィックミラーリング設定コマンド 8-1
8.1.1 mirror-to interface 8-1

8章 トラフィックミラーリング

8.1 トラフィックミラーリング設定コマンド

8.1.1 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 *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 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 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。

mirror-to コマンドは受信インタフェースに適用できます。

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 **9-x-x** です。

9 章 プロセスモニタリングとメンテナンス 9-1
9.1 プロセスモニタリングとメンテナンス設定コマンド 9-1
9.1.1 display exception context 9-1
9.1.2 display exception filepath 9-6
9.1.3 exception filepath 9-7
9.1.4 process core 9-8
9.1.5 reset exception context 9-9

9章 プロセスモニタリングとメンテナンス

9.1 プロセスモニタリングとメンテナンス設定コマンド

9.1.1 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*: 装置のスロット番号を指定します。これは 1 に固定されています。

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、コアダンプ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:0x000000000400fff3      lo:0xdf3b645a1cac08c9
       hi:0x000000000000007f     bad:0x000000555589ba84
    cause:0x0000000000800020      pc:0x0000005555a3bcb4
```

表 9-1 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	コアダンプ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

9.1.2 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*: 装置のスロット番号を指定します。これは 1 に固定されています。

説明

display exception filepath コマンドはコアダンプファイルのディレクトリを表示します。

例

コアダンプ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:.
```

9.1.3 exception filepath

Syntax

exception filepath *directory*

undo exception filepath *directory*

デフォルト

コアダンプファイルを保存するディレクトリは、デフォルトのファイルシステムのルートディレクトリです。デフォルトのファイルシステムの詳細については、セクション 1 *はじめに オペレーションマニュアル*の“*ファイルシステム管理*”を参照してください。

View

User view

定義済みユーザロール

network-admin

パラメータ

directory: コアダンプファイルを保存するディレクトリを指定します。ディレクトリは、ファイルシステムのルートディレクトリである必要があります。

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

コアダンプ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**

9.1.4 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ダンプファイルを作成し、続く例外のコアダンプ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: コアダンプファイルの作成を無効にします。

maxcore *value*: コアダンプ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*: 装置のスロット番号を指定します。これは 1 に固定されています。

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、コアダンプ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、コアダンプファイルを作成することを有効にします。コアダンプファイルは例外情報を記録します。

コアダンプ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ダンプ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** のコアダンプ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** のコアダンプ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**

9.1.5 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*: 装置のスロット番号を指定します。これは 1 に固定されています。

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

目次

このセクションのページは **9-x-x** です。

10 章 PoE 10-1
10.1 PoE 設定コマンド 10-1
10.1.1 apply poe-profile 10-1
10.1.2 apply poe-profile interface 10-2
10.1.3 display poe device 10-3
10.1.4 display poe interface 10-4
10.1.5 display poe interface power 10-8
10.1.6 display poe pse 10-10
10.1.7 display poe pse interface 10-12
10.1.8 display poe pse interface power 10-14
10.1.9 display poe-profile 10-16
10.1.10 display poe-profile interface 10-17
10.1.11 poe enable 10-18
10.1.12 poe high-inrush enable 10-20
10.1.13 poe max-power 10-23
10.1.14 poe pd-description 10-23
10.1.15 poe pd-policy priority 10-24
10.1.16 poe priority 10-25
10.1.17 poe update 10-26
10.1.18 poe utilization-threshold 10-27
10.1.19 poe-profile 10-28
10.1.20 poe track 10-29

10章 PoE

PoE 機能は QX-S1108GT-2G-PW、QX-S1116GT-4G-PW、QX-S1124GT-4G-PW でサポートしています。

10.1 PoE設定コマンド

10.1.1 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**

10.1.2 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**

10.1.3 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*: 装置のスロット番号を指定します。これは 1 に固定されています。

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 10-1 コマンド出力

フィールド	説明
PSE ID	PSEのIDです。

フィールド	説明
Slot No.	PSEのスロット番号です。
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。

10.1.4 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
Legacy PD Detection            : Disabled
```

表 10-2 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	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	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	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	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	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	平均電力です。
Peak Power	ピーク電力です。
Max Power	供給可能な最大電力です。
Electric Current	供給電流です。
Voltage	供給電圧です。
PD Description	PI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 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。
PoE	PoEの状態です。 ● **Enabled**－有効です。 ● **Disabled**－無効です。
Priority	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	現在の供給電力です。
Oper	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	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	（動的な電力割り当てをサポートする装置です。）最大電力で構成されたすべてのPSEの残りの電力の合計です。 最大電力で構成されたPSEがない場合、このフィールドには0が表示されます（すべてのPSEが動的電力割り当てに参加します）。 （動的な電力割り当てをサポートしない装置です。）すべてのPSEの合計残り電力です。

10.1.5 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 10-4 コマンド出力

フィールド	説明
Interface	インタフェース名です。
CurPower	現在の供給電力です。
PeakPower	ピーク電力です。
MaxPower	供給可能な最大電力です。
PD Description	PII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。

フィールド	説明
Used	現在のPIの消費電力です。
Remaining	（動的な電力割り当てをサポートする装置です。）最大電力で構成されたすべてのPSEの残りの電力の合計です。 最大電力で構成されたPSEがない場合、このフィールドには0が表示されます（すべてのPSEが動的電力割り当てに参加します）。 （動的な電力割り当てをサポートしない装置です。）すべてのPSEの合計残り電力です。

10.1.6 display poe pse

Syntax

display poe { **pse | 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 10-5 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。
PSE Fast Power Supply	PSE高速電源装置の有効化ステータスです。 ● **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。
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。

フィールド	説明
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。
PD High Inrush	PD高突入が有効かどうか表示します。 ● **Enabled**ー有効です。 ● **Disabled**ー無効です。

10.1.7 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 10-6 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。動的な電力割り当てに参加するPSEのとき、このフィールドには0が表示されます。

10.1.8 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。

<Sysname> 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 10-7 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。
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。
Remaining	PSEの余力電力です。動的な電力割り当てに参加するPSEのとき、このフィールドには0が表示されます。

10.1.9 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 10-8 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。

10.1.10 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 10-5 を参照してください。

10.1.11 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**

10.1.12 poe high-inrush enable

🕮 **メモ:**

S1100X 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**

10.1.13 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

10.1.14 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

10.1.15 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

10.1.16 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

10.1.17 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、すべての 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

10.1.18 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。詳細はセクション 10 *システム管理 オペレーションマニュアル*の”*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

10.1.19 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**

10.1.20 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

目次

このセクションのページは **9-x-x** です。

11 章 NetMeister 11-1
11.1 Netmeister 設定コマンド 11-1
11.1.1 display netmeister 11-1
11.1.2 netmeister account 11-3
11.1.3 netmeister alarm enable notice 11-5
11.1.4 netmeister enable 11-6
11.1.5 netmeister mode 11-6
11.1.6 netmeister parent ip 11-7
11.1.7 netmeister parent-mode mqtt port 11-9
11.1.8 netmeister parent-mode sitename 11-10
11.1.9 netmeister proxy 11-10
11.1.10 netmeister update 11-12

11章 NetMeister

11.1 Netmeister設定コマンド

11.1.1 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

親機モードの装置で NetMeisetr との接続情報を表示します。

<Switch> display netmeister

```
NetMeister state                              : Enabled
Mode                                          : Parent
Connection state with NetMeister              : Connected
Account name                                  : nec
Proxy information:
State                                         :  --
Parent information:
Site name                                     : test
Interval                                      : 3600 sec
MQTT interval                                 : 60 sec
MQTT status                                   : Connected
```

NetMeisetr 及び親機との接続情報を表示します。

<Switch> 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                                : 444
  Connection state                           : Connected
```

表 11-1 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
Mode	NetMeisterへの接続モードです。 ● **Parent** —親機モード ● **Child** —子機モード
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。
State	プロキシサーバへの接続状態です。 ● **Connected.**—接続 ● **Disconnected.**—切断 ● **"--"** —プロキシサーバを設定していない場合に表示されます。
URL	プロキシサーバのURL。形式はhttp :// <domain>:<ポート>です。 domainはプロキシサーバのWebアドレスまたはIPアドレス、portはポート番号です。 プロキシサーバが構成されていない場合、このフィールドは表示されません。
IP address	親機のIPアドレスです。 子機モード時のみ表示されます。

フィールド	説明
Port number	親機のポート番号です。 子機モード時のみ表示されます。
Connection state	NetMeister機能による親機への接続状態です。 • **Connected.**—接続 • **Disconnected.**—切断 子機モード時のみ表示されます。
Site name	拠点名です。 親機モード時のみ表示されます。
Interval	親機の更新情報の送信間隔です。 親機モード時のみ表示されます。
MQTT interval	MQTTプロトコルの送信間隔です。 親機モード時のみ表示されます。
MQTT status	MQTTプロトコルの接続状態です。 • **Connected.**—接続 • **Disconnected.**—切断 • **"--"** —接続が成功しなかった場合に表示されます。 親機モード時のみ表示されます。

関連コマンド

- **netmeister account**
- **netmeister enable**

11.1.2 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。

password: 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。

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。

<Switch> system-view

[Switch] netmeister account nec password simple nec1234

関連コマンド

- **netmeister enable**
- **display netmeister**

11.1.3 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

11.1.4 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。

<Switch> system-view

[Switch] netmeister enable

11.1.5 netmeister mode

🕮 **メモ:**

netmeister mode コマンドは Version 7.1.16 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

11.1.6 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。

<Switch> system-view

[Switch] 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。

<Switch> system-view

[Switch] netmeister parent ip 192.168.1.254

関連コマンド

- **netmeister enable**
- **display netmeister**

11.1.7 netmeister parent-mode mqtt port

🕮 **メモ:**

netmeister parent-mode mqtt port コマンドは Version 7.1.16 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**

11.1.8 netmeister parent-mode sitename

🕮 **メモ:**

netmeister parent-mode sitename コマンドは Version 7.1.16 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**

11.1.9 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 proxy 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**

11.1.10 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